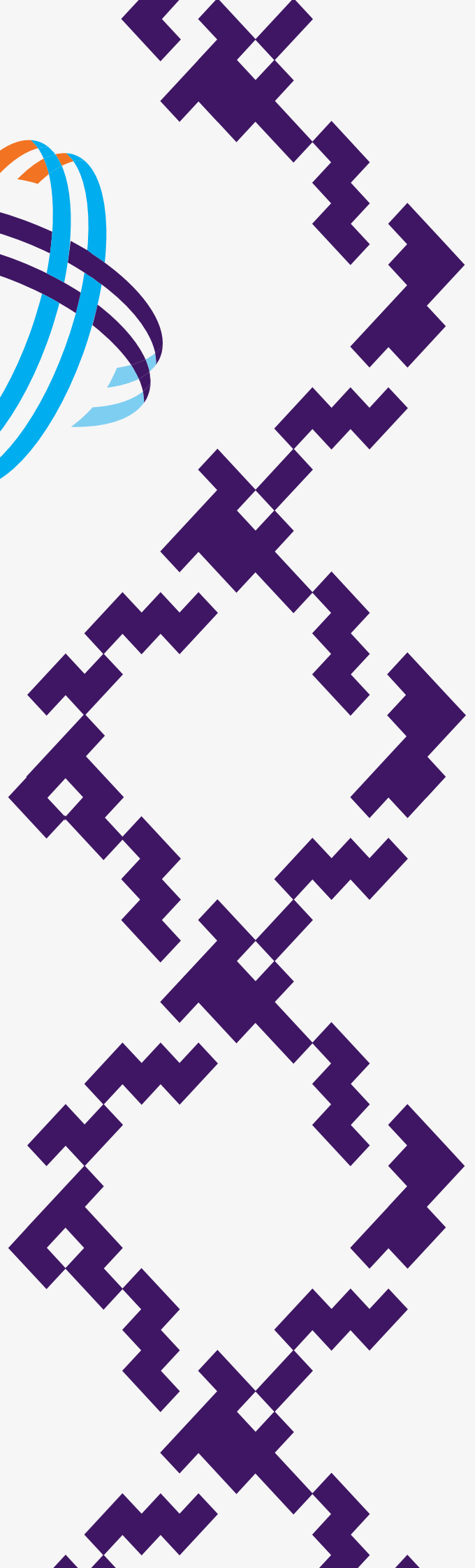




**GFCE
WORKING
GROUPS**

| ANNUAL REPORT 2020

**GLOBAL
FORUM ON
CYBER
EXPERTISE**



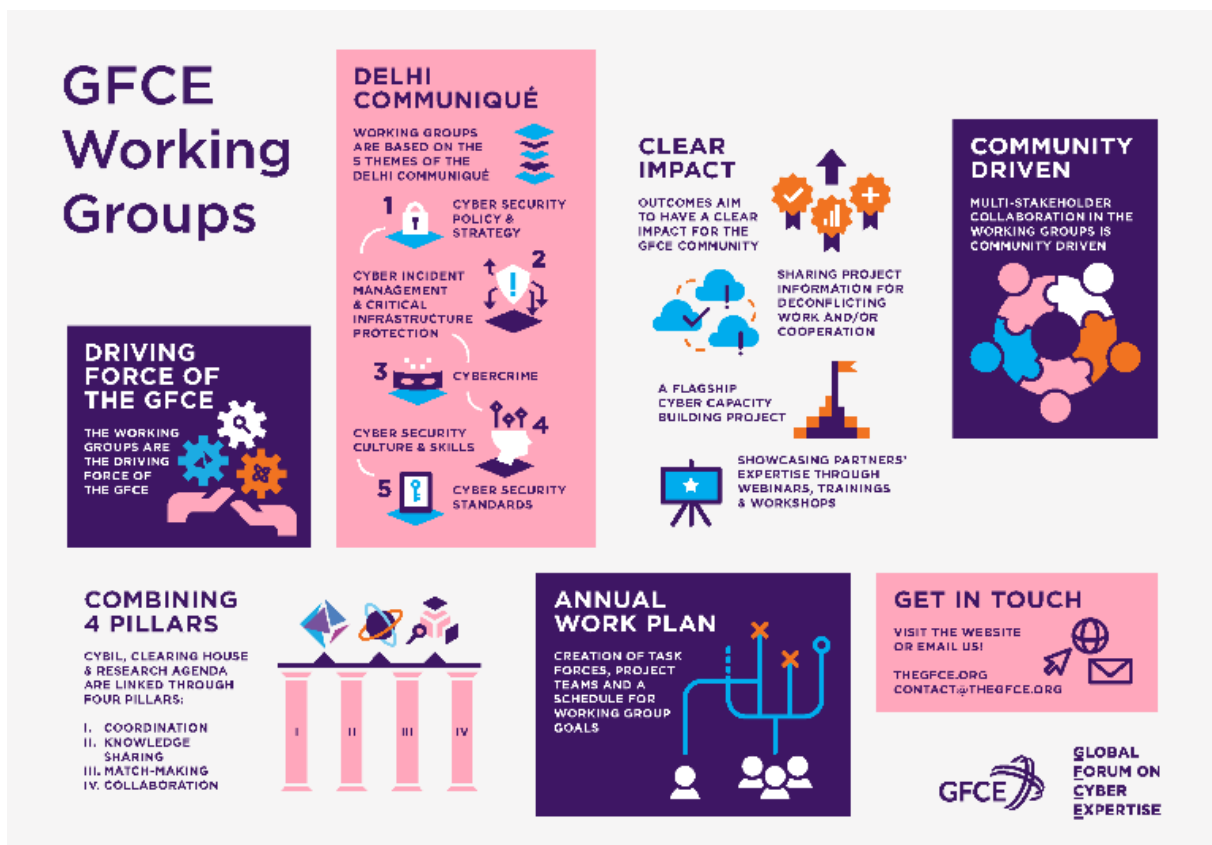
GFCE Working Groups

The Global Forum on Cyber Expertise (GFCE) Working Groups were established in 2018, following the GFCE Community's endorsement of the [Delhi Communiqué](#) on a Global Agenda for Cyber Capacity Building.

The Working Groups are the GFCE's driving force to coordinate and improve global cyber capacity building efforts. Based on the thematic priorities identified in the Delhi Communiqué, the GFCE Working Groups are organized along the listed themes:

- A. Cyber Security Policy and Strategy;
- B. Cyber Incident Management and Critical Information Infrastructure Protection;
- C. Cybercrime;
- D. Cyber Security Culture and Skills.

The GFCE Members and Partners collaborate with each other through the Working Groups and over 85% of the community is involved in at least one group. For coherence and synergy, the activities of Working Groups are divided across common goals of avoiding duplication of efforts (**Coordination**), improving the efficiency and effectiveness of CCB projects and filling knowledge gaps (**Knowledge Sharing**), filling capacity gaps (**Match Making**) and collaborating on new projects within the GFCE community (**Collaboration**).



GFCE Working Groups

DELHI COMMUNIQUÉ
WORKING GROUPS ARE BASED ON THE 5 THEMES OF THE DELHI COMMUNIQUÉ

1. CYBER SECURITY POLICY & STRATEGY
2. CYBER INCIDENT MANAGEMENT & CRITICAL INFRASTRUCTURE PROTECTION
3. CYBERCRIME
4. CYBER SECURITY CULTURE & SKILLS
5. CYBER SECURITY STANDARDS

DRIVING FORCE OF THE GFCE
THE WORKING GROUPS ARE THE DRIVING FORCE OF THE GFCE

CLEAR IMPACT
OUTCOMES AIM TO HAVE A CLEAR IMPACT FOR THE GFCE COMMUNITY

SHARING PROJECT INFORMATION FOR DECONFLICTING WORK AND/OR COOPERATION

A FLAGSHIP CYBER CAPACITY BUILDING PROJECT

SHOWCASING PARTNERS' EXPERTISE THROUGH WEBINARS, TRAININGS & WORKSHOPS

COMMUNITY DRIVEN
MULTI-STAKEHOLDER COLLABORATION IN THE WORKING GROUPS IS COMMUNITY DRIVEN

COMBINING 4 PILLARS
CYBIL, CLEARING HOUSE & RESEARCH AGENDA ARE LINKED THROUGH FOUR PILLARS:

- I. COORDINATION
- II. KNOWLEDGE SHARING
- III. MATCH-MAKING
- IV. COLLABORATION

ANNUAL WORK PLAN
CREATION OF TASK FORCES, PROJECT TEAMS AND A SCHEDULE FOR WORKING GROUP GOALS

GET IN TOUCH
VISIT THE WEBSITE OR EMAIL US!

THEGFCE.ORG
CONTACT@THEGFCE.ORG

GFCE GLOBAL FORUM ON CYBER EXPERTISE



In 2020, based on lessons learnt from the past two years and discussions within the Working Groups and the GFCE Community, the GFCE Secretariat has revised [the GFCE Working Groups Terms of Reference \(TOR\)](#) and has put together a [GFCE Working Groups Outcomes 2021](#) document. The revised Terms of Reference provides more clarity on the mandate of the Working Groups and the roles and responsibilities, while the Outcomes 2021 document provides concrete targets for the GFCE Working Groups for 2021 in line with the ambitions of the GFCE.

The focus of the GFCE Working Groups in 2020 has been given to further strengthen cooperation on cyber capacity building through the development of common deliverables and projects. The Working Groups and Task Forces have demonstrated their added value through the members' involvement, engagement and active participation in Working Group calls, meetings and during the V-Meeting online sessions in April and May 2020.

Contents

Report Working Group A – Cyber Security Policy & Strategy	3 -5
Report Working Group B – Cyber Incident Management & Critical Infrastructure Protection	6 – 8
Report Working Group C – Cybercrime	9 – 11
Report Working Group D – Cyber Security Culture & Skills	12 - 14

Working Group A - Cyber Security Policy & Strategy

Introduction

Working Group A is chaired by Ian Wallace and its divided into two Task Forces (TF):

1. TF Strategy and Assessments (co-Leads Lea Kaspar and Carolin Weisser)
2. TF CBMs, Norms Implementation and Cyber Diplomacy (co-Leads Kaja Ciglic and Szilvia Toth)

The Policy & Strategy theme may be understood as the ‘foundation’ for the other identified themes in the Delhi Communiqué. The aim of the group is to help countries and other stakeholders improve their policy and strategy making capacity. Recognizing the importance of the ongoing international cyber negotiations and the need for greater cyber diplomacy capacity, the Working Group split into two Task Forces during an informal meeting at the Internet Governance Forum (IGF) in 2018; one focusing on National Cyber Security Strategy and National Assessments, and the other focusing on CBMs, Norms Implementation and Cyber Diplomacy. Members of Working Group A could therefore decide if they wanted to participate in one or both Task Forces, depending on their interest.

In 2019, the Task Forces focused on mapping existing initiatives and available tools related to their respective topics. During the GFCE Annual Meeting 2019 in Addis Ababa, both Task Forces also organized workshops for the beneficiary community. Towards 2021, the Strategy & Assessments Task Force aims to build on the work of the ‘catalogue’ and ‘assessments overview’ developed in 2020, while the other Task Force aims to demonstrate its added value in supporting the implementation of outcomes from international cyber stability discussions. Additionally, the two other things both Task Forces aim to build on in 2021 is getting more materials available in languages other than English and in leveraging the outputs of the new research agenda.

I. Coordination

GFCE members have submitted information on **76** ongoing projects that are relevant to the strategy/policy process, national assessments, CBMs and norms, and/or cyber diplomacy. This can be found at www.CybilPortal.org.

In October 2019, the Strategy & Assessments Task Force used the GFCE Annual Meeting to help coordinate strategy support projects in West Africa, in partnership with ECOWAS. Following this meeting, in Jan 2020, Global Partners Digital shared its Terms of Reference for a planned strategy consultancy activity in Sierra Leone and invited expressions of interest in delivering the work from suitable consultants.

During Task Force meetings, members are invited to share updates and information on ongoing or finished projects. By facilitating such discussion, members can draw on each other’s experiences and expertise, de-conflict projects to avoid duplication and discover new opportunities for collaboration.

II. Knowledge Sharing

The Strategy and Assessments Task Force has identified **38** tools and publications to help members, which can be found at www.CybilPortal.org. These cover support to national cyber security capacity assessments and capacity building for the strategy/policy setting process.



The CBMs, Norms Implementation and Cyber Diplomacy Task Force has similarly identified **38** tools and publications on the relevant topics and identified key stakeholders, actors, and events in this space. The Task Force has also developed **a [whitepaper on Cyber Diplomacy](#)** in 2019 and an **[introduction paper on CBMs as they relate to cyberspace in 2020](#)** (available in English and Spanish).

During the GFCE V-Meetings in April and May 2020, the CBMs, Norms Implementation and Cyber Diplomacy Task Force organized a session on [Capacity Building and UN Processes](#); which saw the participation of the Chairs of the UN GGE and OEWG. The aim of the session was to provide an update on the UN OEWG and GGE processes, and to elaborate on the role of capacity building in implementing the outcomes of such discussions. The Strategy & Assessments Task Force organized a session on [Cyber Capacity Assessments](#) with the objective to raise awareness on different assessment tools and underline the utility of assessment tools in informing cyber capacity building efforts.

In 2020, the Task Forces submitted a total of **6 research ideas** for the Draft Global Cyber Capacity Building Research Agenda 2021.

III. Match Making

The Strategy & Assessments Task Force has **1 active Clearing House case**, Sierra Leone. At the GFCE Annual Meeting 2019, Minister Swarray met with 17 donor and implementer organisations to discuss Sierra Leone's priorities and how the international community could support them. Some examples of follow-on actions from this meeting: the US helped Sierra Leone join STOP.THINK.CONNECT and materials from this supported a local awareness campaign; The Council of Europe is helping review draft legislation; and Global Partners Digital have extended their national strategy support project.

To help countries know what types of support activity are available for the National Cybersecurity Strategy cycle, and to help programme managers design projects, the Strategy & Assessments Task Force has developed a 'catalogue' of examples. **A draft of the catalogue has been prepared ahead of the GFCE Annual Meeting 2020 and will be finalized for circulation by early 2021.** The Task Force would like to thank the following organizations for their comments or contributions on the catalogue: Africa Cybersecurity and Digital Rights Organisation (ACDRO), Cybersecurity Capacity Centre for Southern Africa (C3SA), Commonwealth Telecommunications Organization (CTO), Cyber4Dev, CyberGreen, CYSIAM, DiploFoundation, Global Cybersecurity Capacity Centre (GCSCC), George C. Marshall European Centre for Security Studies, Global Partners Digital (GPD), International Telecommunications Union (ITU), the MITRE Corporation, Organization of American States (OAS), Oceania Cyber Security Centre (OCSC) and the UK Home Office.

The CBMs, Norms Implementation and Cyber Diplomacy Task Force has not received a formal request for support. In 2020, the Task Force developed an overview of Cyber diplomacy initiatives living document.

IV. Collaboration

The GFCE V-Meeting session on Cyber Capacity Assessments confirmed the assumption that there is a need in the GFCE community to learn more about the different tools and their methodologies, outputs and impact. Therefore, in September 2020, members of the Strategy & Assessments Task Force came together to form a project team to **develop an overview of the existing tools to assess cyber capacity of countries.** The project will be finalized in February/March 2021 and aims to:



- i) Provide an overview document which describes the existing tools and their characteristics to facilitate beneficiaries, funders and implementers to better understand the approach, benefits and outputs of each tool and support their decision-making processes.
- ii) Provide GFCE members (and potentially non-members) a platform to showcase their assessment tool, including its USP and benefits, and to get in contact with potential beneficiaries in and outside the GFCE community.

This project would not have been possible without the contributions of GCSCC, OCSC, ITU, Potomac Institute for Policy Studies (PIPS), e-Governance Academy (eGA), OAS, World Bank, the Australian Strategic Policy Institute (ASPI), and the MITRE Corporation.

Working Group A Deliverables

GFCE Objective	Working Group Agenda Element	Achievements by Annual Meeting 2020	Work Plan in 2021
1. Coordination	i.e. Mapping Projects	76 ongoing projects on Cybil	Cybil platform updated regularly with relevant projects and events
	i.e. Support coordination of projects	Members share updates on projects, deconflict work and coordinate (Ongoing) Coordinate strategy support in West Africa with ECOWAS (2019)	TF members provided with platform to explore ways to build synergies and coordinate on projects where necessary
2. Knowledge Sharing	Identifying tools/publications	73 tools/publications on Cybil	Cybil platform updated regularly with relevant tools and publications
	Knowledge products	Cyberdiplomacy paper (2019) CBMs paper (2020)	Standard support package is developed
	Workshops	2 Workshops (AM 2019) 2 V-Meeting sessions (2020)	Organize a table-top exercise on norms (tbd)
	Research Agenda	6 ideas submitted for the Draft Research Agenda 2021	At least 2 ideas submitted for each Task Force for the Research Agenda 2022
3. Match Making	Clearing House	Sierra Leone request (2019) Tunisia request (2019)	Existing Clearing House cases followed up on; new / incoming clearing house requests fielded by TF
	Offers for support	Overview of existing cyber diplomacy initiatives (2020) Catalogue of project options (2020)	Catalogue is finalized and published; plan to operationalise Catalogue developed.
4. Collaboration	Projects	Assessments overview project (2020)	Overview of CNI frameworks project in cooperation with WG B. Impact of COVID-19 travel restrictions on cyber capacity building activities project. Deliver a coordinated message at OEWG in March project. Norms and Capacity Building project.

Working Group B - Cyber Incident Management & Critical Infrastructure Protection

Introduction

Working Group B is chaired by Abdul-Hakeem Ajjola and its divided into two Task Forces (TF):

3. TF Cyber Incident Management (TF CIM) - TF Lead Maarten van Horenbeeck
4. TF Critical Information Infrastructure Protection (TF CIIP) – TF Lead Marc Henauer

Cyber Capacity Building (CCB) on incident management and infrastructure protection aims to improve capacities that allow nations to respond to and recover from cyber incidents in a timely and efficient manner. Monitoring, response and mitigation capacities enhances infrastructures continuity and can improve communication and cooperation between national and international entities and stakeholders. In turn these activities can support the overall cyber resilience of cyberspace much beyond a particular country. This particular theme is quite broad, and therefore the Working Group split into two Task Forces during the GFCE Annual Meeting 2018 in Singapore.

Throughout 2019, the TF CIM worked on Global CSIRT Maturity Framework whilst the TF CIIP worked on a CIIP Capacity Framework. During the GFCE Annual Meeting 2019 in Addis Ababa, both Task Forces organized workshops with an African focus for the beneficiary community.

In 2020, the TF CIM started working in three project teams on separate deliverables: 1) National CSIRT Career Path; 2) Phase 0 CERT; and 3) Next phase for the CSIRT Maturity Framework. The TF CIIP worked in 2020 on assisting Senegal with its clearing house request for support on their CIIP and is additionally looking for ways to cooperate closely with the Meridian community (a CIIP community).

I. Coordination

GFCE members have submitted information on **65 ongoing projects** that are relevant to the theme Cyber Incident Management & Critical Infrastructure Protection. An overview of these projects can be found at www.CybilPortal.org.

During Task Force meetings, members are invited to share updates and information on ongoing or finished projects. By facilitating such discussion, members can draw on each other's experiences and expertise, de-conflict projects to avoid duplication and discover new opportunities for collaboration.

II. Knowledge Sharing

WG B has identified **18 tools** and **19 publications** to help members, which can be found at www.CybilPortal.org. These cover support with National Computer Security Incident Response, Incident Capture and Analysis, Cyber Security Exercises, and Critical Information Infrastructure Protection.

In 2020, the Task Forces submitted a total of **5 research ideas** for the Draft Global Cyber Capacity Building Research Agenda 2021. One of the research proposals was selected as a pilot project to support the efforts of the project team on a National CSIRT Career Path. This research proposal aims to Identify



a menu of practical, feasible and affordable individual, team, and group training options that increase the maturity and capabilities of national CSIRTs in low- income countries. The other two research proposals that the TF CIM put forward focus on 1) a framework on how to manage the relationship between national CSIRTs and sectoral CSIRTs, and 2) the role of the private sector in CSIRT capacity building. The TF CIIP submitted two ideas for the research agenda on:

- 1) Identifying important contextual factors that shape and drive different national approaches to CIIP - A foundational study of the different aspects of how nations develop and implement CIIP policies and programs around the world to address the question of what are the design factors and set of best practices for the development and implementation of CIIP policies and programs given certain key factors; and
- 2) Identifying indicators of CIIP maturity - An initial study that identifies probable indicators of CIIP maturity by identifying how developed countries have implemented CIIP strategies and policies to identify best practices for implementation and measuring success.

III. Match Making

The Critical Infrastructure Protection Task Force has **1 active Clearing House case**, Senegal. In 2019, Senegal requested support with their national Critical Infrastructure Information Protection. The aim was to organize a national combined with a regional workshop in collaboration with ECOWAS and other West-African states in June 2020. However, due to COVID-19 this workshop had to be postponed. In October 2020, Senegal organized a virtual workshop on CIIP and invited experts from the GFCE community to be on the panel.

The Cyber Incident Management Task Force has not received a formal request for support yet. To help countries know what types of support activity is available within both Task Forces of WG B, in 2021, the Task Forces will develop an overview of offers for support.

IV. Collaboration

The Cyber Incident Management Task Force created three project teams at the start of 2020 based on project ideas from its Task Force members. Two of the project teams are led by The Netherlands and TNO and leverage the expertise of the Task Force members. The first project team focuses on **Phase 0 CERT**, which aims to develop a guideline for newcomers who are at the start of setting up of a national CSIRT. The second project team is on the **Next phase of the CSIRT Maturity Framework**. The aim of the project is to improve the profiles that the framework was built on since its three years old in close cooperation with ENISA and the Open CSIRT Foundation. Both of these projects will be finalized in the beginning of 2021. The third project is focused on developing a **National CSIRT career path**, which to make an offer to low income countries national CSIRTs where they offer a paid training certification pathway for their CSIRT staff. The idea is to have a mix between remote learning and receiving mentoring and coaching. The initiative is led by FIRST.

The Task Force on Critical Infrastructure Information Protection has been focusing in 2020 to formalize ways to collaborate more closely with the Meridian community and will start a project team in 2021.



Working Group B Deliverables

WG B – Cyber Incident Management & Critical Infrastructure Protection			
GFCE Objective	Working Group Agenda Element	Achievements by Annual Meeting 2020	Work Plan in 2021
I. Coordination	i.e. Mapping Projects	65 Ongoing projects on Cybil	Cybil platform updated regularly with relevant projects and events
	i.e. Support coordination of projects	Linking actors to deconflict projects and explore new areas for collaboration (Ongoing)	TF members provided with platform to explore ways to build synergies and coordinate on projects where necessary
II. Knowledge Sharing	Identifying tools/publications	37 tools/publications on Cybil	Cybil platform updated regularly with relevant tools and publications
	Workshops	Workshop (2019) V-Meeting session 2020	TF CIIP – Webinars with Meridian community (TBD)
	Research Agenda	5 ideas submitted for the Draft Research Agenda 2021	At least 2 ideas submitted for each Task Force for the Research Agenda 2022
III. Match Making	Clearing House	Senegal (2020)	Existing Clearing House cases followed up on; new / incoming clearing house requests fielded by TF
	Overview of offers for support		Overview of WG B offers for support
IV. Collaboration	Projects	TF CIM – National CSIRT Career Path (2021) TF CIM – Phase 0 CERT (2021) TF CIM – Next phase CSIRT Maturity Framework (2021) TF CIIP – Infographic Identifying CIIP (2021)	

Working Group C - Cybercrime

Introduction

Working Group C brings together governments, industry and experts focused on coordination of capacity building efforts relating to cybercrime. Through the Working Group, GFCE Members and Partners discuss capacity building and cybercrime issues such as development and implementation of legal frameworks, strengthening criminal justice and law enforcement responses to cybercrime, as well as the development of formal and informal frameworks for cooperation.

The Working Group is also a place for those involved in the prevention, response and assessment of cybercrime to engage with each other and share knowledge and expertise that leads to impactful capacity building projects and initiatives, helping countries to develop their own capacity to deal with the challenges presented by cybercrime and to identify best practices which can lead to innovative solutions.

Structure of Working Group C

Working Group C is chaired by [Joyce Hakmeh](#), Senior Research Fellow of the International Security Programme and Co-Editor of the Journal of Cyber Policy at Chatham House. Prior to the GFCE open call for applications to Working Group Chair positions in October 2020, the chairpersonship of Working Group C was the shared responsibility of Co-Chairs Joyce Hakmeh and Zahid Jamil.

As of October 2020, Working Group C comprises 51 GFCE Members and Partners the vast majority of which have been active in the Working Group since its establishment in 2018.

I. Coordination

WG-C contributions to Cybil Knowledge Portal

Working Group C members have submitted information on over **130 projects to Cybil**. Enhancing coordination between activities of Working Group C members was a clear goal identified in 2019 and the submissions of Working Group members to the Cybil portal go some way towards achieving that objective.

Cybil is considered an important tool for mapping existing capacity building activities and for identifying knowledge gaps. Developing the portal, for example by having a means of regularly obtaining updates on projects, whilst improving awareness and understanding of members on the benefits of Cybil through regularly providing contributors with analytics on the ways information is accessed and downloaded by users were highlighted by the group as potential ways of encouraging others to continue to provide and upload information.

In the upcoming year, the group intends to implement additional means of improving coordination and communication amongst members, including setting up a mailing list and newsletter. Implementation of these ideas within the group is currently under discussion.

Asia-Pacific Cybercrime Capacity Building Hub (APC Hub)

In 2019 the GFCE signed a Memorandum of Understanding with the Supreme Prosecutors' Office of the Republic of Korea (KSPO) and World Bank on the establishment of an APC Hub. The role of the GFCE is to provide advice and support to the Hub in developing and providing targeted training to countries and organizations in the Asia Pacific region. Such trainings will be based on assessments conducted for



the subject country or organization. An assessment tool will also be developed and customized for target countries.

GFCE Working Group C has been acting as a sounding board for proposed activities for the Hub. Once the Hub is operational, the intention is that Working Group C will be a critical source of resources and support for the coordination of the outreach activities of the Hub, whereas Working Group C members experience and know-how can contribute to avoiding duplication of existing capacity building activities in the region. It is expected that the Hub will also contribute to and draw knowledge from GFCE's Cybil platform.

II. Knowledge Sharing

There are currently **20 tools** and **21 publications** on Cybil tagged with the cybercrime indicator. Tools on Cybil refer to a collection of resources to help design and deliver international cyber capacity building projects. Publications refers to lessons learnt, outcomes and research for and about international cyber capacity building, in this case on the specific topic of countering cybercrime.

III. Match Making

Updates on The Gambia clearing house request

The Friends of the Gambia group was launched in September 2019 following the official Letter of Request from The Gambia. The Gambia's request builds on its National Cybersecurity Strategy and Action Plan (2016) and key priority areas of its National Development Plan (2018-21). The request was first introduced in the GFCE through Working Group C.

Following a brainstorm session in November 2019, the Working Group began mapping the current project activity in order to identify areas where further support could be provided. In January 2020 The Gambia provided further information on activities under the request.

An updated outline of the request was distributed to all GFCE Working Groups, asking members to provide feedback, and indicated where they could support. During a [meeting in May 2020](#), The Gambia along with Expertise France and Council of Europe described the progress that has been made on the request. Updates include:

- 1) The Gambia updating its Draft Cybersecurity Strategy & Action Plan
- 2) Drafting and approving the Data Protection Law
- 3) Drafting and approving (pending) the draft Cybercrime Bill
- 4) Establishing the gmCSIRT (staff recruited and operational. installation of equipment and other engagements pending)
- 5) ECOWAS / OCWAR-C has offered The Gambia to establish/renovate a Digital Forensic laboratory for the national police force

IV. Collaboration

The Working Group has convened in two full meetings in 2020, once in July and once in November. In addition, a virtual session was held during the GFCE April V-meetings on the topic of capacity building and countering cybercrime.

This session aimed to get a better picture of what has been happening in this space considering the recent pandemic and what effect this might have had for a concurrent rise in cyberattacks and

ANNUAL MEETING 2020

GFCE WORKING GROUPS | REPORT



GLOBAL
FORUM ON
CYBER
EXPERTISE

cybercrime. The session was structured around a series of presentations and interventions from representatives of Council of Europe, United Nations Office on Drugs and Crime (UNODC), Europol, FireEye Mandiant and the Global Cyber Alliance. A report on the session can be found [here](#).



Working Group D - Cyber Security Culture & Skills

Introduction

Working Group D on Cyber Security Culture & Skills focusses on the following two topics:

1. Cyber Security Awareness
2. Education and Training, with a focus on Cyber Security Workforce Development

The Working Group is chaired by Tereza Horejsova for the coming two-year 2020 – 2022, for the period from 2018 to 2020, it was chaired by Deborah Housen-Couriel.

The theme Cyber Security Culture and Skills has been endorsed by the GFCE community in the [Delhi Communiqué](#) as one of the five prioritized themes for cyber capacity building to

- a. Promote comprehensive awareness across all stakeholders of cyber-related threats and vulnerabilities and empower them with the knowledge, skills and sense of shared responsibility to practice safe and informed behaviors in the use of ICTs, and to
- b. Involve all stakeholders to create a workforce with a set of cyber security skills and knowledge employers require.

Since the establishment of the Working Groups, the focus of Working Group D is dual: leverage cyber security awareness and promote foundational understandings of cyber threats, risk and cyber hygiene and bring together stakeholders and collaborate on generating a skilled cybersecurity workforce through education and training opportunities. Working Group D members should aim to provide best practices, tools and materials for cybersecurity programs. In 2018, the Working group split into two Task Forces; one focusing on Cyber Security Awareness and the other one on Cybersecurity Professional Training and Development. The two Task Forces were dissolved in late 2019.

In 2018, the Working Group's participants identified the need for more information on existing programs for cybersecurity awareness and professional education and training. In 2019, the Task Forces carried on this project and focused on mapping existing initiatives for promoting cybersecurity awareness, education, professional training and development. In 2020, regarding the component of education and training, the Working Group made a [written submission](#) providing views and recommendations in relation to the request for comments by NIST for the update to the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181. Regarding the Working Group's component on Cyber Security Awareness, the participants have focused on the development of a GFCE Cyber Security Awareness Campaigns Toolkit.

Towards 2021, the Working group aims to demonstrate its added value in supporting cyber security awareness and workforce development among all stakeholders.

I. Coordination

To support the coordination of resources and expertise, the Working Group mapped existing initiatives and facilitated dialogue between actors within the group to foster synergies, to identify the needs and



priorities and to avoid duplication of efforts. In 2019, a [questionnaire](#) was developed for WG D members to provide input pertaining to current initiatives for promoting cybersecurity awareness, education, professional training and development. GFCE members have submitted information on **97 projects** that are relevant to cyber security awareness, education & training and workforce development. These can be found at on [Cybil Knowledge Portal](#). The Working Group will continue the mapping exercise on relevant projects.

II. Knowledge sharing

The Working Group has identified **27 publications** and **17 tools**, related to Cyber Security Culture and Skills which have been uploaded on Cybil Knowledge Portal under the [theme of Cyber Security Culture and Skills](#). In 2019, The Working Group authored two white papers outlining good practices on [cyber security professional training & development](#) and [cyber security awareness](#). During the GFCE Annual Meeting 2019 in Addis Ababa, Working Group D held two workshops, one on Regional Cybersecurity Awareness Campaigns and one on Workforce Development Frameworks – The NICE Framework. In May 2020, a session on Cyber Security Awareness Campaigns took place as part of the GFCE V-Meeting.

III. Match Making

One of the goals of the Working Group in 2020 is to proactively and reactively help countries find partners to help them strengthen their cyber capacity building on the topic cyber security awareness and education and training. The Working Group has received no formal requests to date but is currently working on a document outlining the needs and interests of involved stakeholders. Towards 2021, the Working Group also aims to create an [Offers for Support](#) Package on Awareness and Workforce Development.

IV. Collaboration

To support the collaboration on new projects within the GFCE Community and the need to learn more about Cyber Security Awareness Campaigns, the Working Group formed, in September 2020, a **Project Team on Cyber Awareness**. The team has focused its work on the development of a [GFCE WG D Awareness Campaigns Standard Toolkit for SMEs](#). The project will be finalized in 2021. The aim is to map existing cybersecurity awareness activities focused on SMEs and analyse how the local context is defined by different organisations. The Working Group has also identified other potential deliverables on the field of education, training and workforce development.

Working Group D Deliverables

GFCE Objective	Working Group Agenda Element	Achievements by Annual Meeting 2020	Work Plan 2021
I. Coordination	i.e. Mapping Projects	97 Ongoing projects on Cybil	Continue identifying relevant projects (Ongoing)
	i.e. Support coordination of projects	Questionnaire (2019)	Continue the mapping exercise on projects (Ongoing)
II. Knowledge Sharing	Identifying tools/publications	44 tools & publications on Cybil	Continue identifying relevant tools/publication (Ongoing)
	Research Agenda	Two Research Ideas (2020)	
	Workshops	Workshop in GFCE Annual Meeting (2019) V-Meeting Session (2020)	
III. Match Making	Catalogue of Offers for Support		Identify Offers for Support on Cyber Security Awareness, Education and Workforce Development
IV. Collaboration	Projects	White Paper on Cyber Security Awareness (2019) White Paper on Cyber Security Professional Training, Education & Workforce Development (2019)	Project Team on Cyber Awareness – Development of a CyberSecurity Awareness Campaigns Toolkit