GFCE Working Groups Annual Report | 2021

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 Communique, the five GFCE Working Groups are organized into the following themes:

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

Towards 2022, three general Working Group objectives have been identified (see Annex):

1. Knowledge and expertise sharing through regular engagement opportunities
2. Support contributions to and use of the GFCE tools through regular updates and review
3. Provide a platform for GFCE members and partners to showcase expertise, to enable better understanding of cyber capacities as they apply in African countries (AU-GFCE Project)

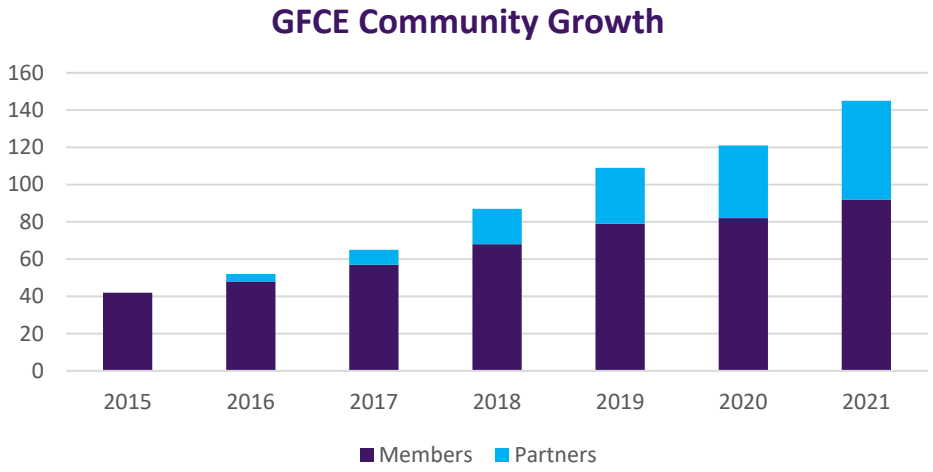
Key Achievements 2021

The GFCE Working Groups provide a communal space for Members and Partners to discuss thematic CCB issues, share knowledge and updates with each other, exchange best practices, and deconflict CCB efforts. They play a strong role in keeping the community connected and bringing new stakeholders into the GFCE. Some key achievements of the Working Groups in 2021 are presented below:

1.	Published the Global Overview of Existing Cyber Capacity Assessment Tools (GOAT) in English, French, Spanish, Russian and Arabic
2.	Published the Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle in English and Spanish
3.	Created and updated an internal database tracker on National Cybersecurity Strategy and Assessments
4.	Provided input and review on research projects commissioned through the Research Agenda mechanism: • Putting Cyber Norms into Practice • Improving the Practice of Cyberdiplomacy: Gaps Analysis on Trainings • Cyber Incident Management in Low-income Countries • Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people
5.	Initiated a joint collaborative project on developing a Guide for the Process of Identifying Critical National Infrastructures (CNI)
6.	Published an updated Global CSIRT Maturity Framework (GCMF)
7.	Published the Getting Started with a National CSIRT Guide
8.	Developed the GFCE CIIP Capacity Framework
9.	Launched a multi-part Cybercrime Series
10.	Initiated a new project on developing Cyber Security as a Profession
11.	Launched the GFCE Community Showcase, with 22 initiatives presented. To be expanded in 2022

GFCE Community in Numbers

In 2021, the GFCE welcomed **28 new stakeholders to the Community**: 11 Members and 17 Partners.



New Members: Ghana | Ethiopia | Papua New Guinea | ESET | Capgemini | ACBF | AFRIPOL | AUDA-NEPAD | Smart Africa | Luxembourg | Somalia

New Partners: AfricaCERT | ACSIS | IFES | Insight | Registry Africa | INCIBE | ZA Central Registry | CREST | InFuture Foundation | LCCPMA | ASD | ORF | Open CSIRTs Foundation | CCU | PGI | WACREN

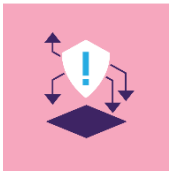
Working Group A
Cyber Security Policy & Strategy

The main objective of Working Group A is to help countries and other stakeholders strengthen their policy and strategy making capacity, and to create a space for multi-stakeholders to share expertise on relevant topics and learn from one another. The Working Group is chaired by Ian Wallace and is organized into two Task Forces (TF):
1. TF Strategy and Assessments
2. TF CBMs/Norms Implementation and Cyberdiplomacy

The Strategy & Assessments TF continues to be led by Carolin Weisser-Harris and Lea Kaspar. In 2021, the TF finalized and published the Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle and the Global Overview of Existing Cyber Capacity Assessment Tools (GOAT). The GOAT is available in four languages and the Catalog is currently available in two languages, with two more on the way in 2022. The Catalog will also be turned into an interactive web-based tool in 2022, supported by the US State Department. In the spirit of knowledge sharing and coordination, the TF has developed an internal database tracker on National Cybersecurity Strategy and Assessments, facilitating the tracking and sharing of updates raised during TF meetings. Another highlight of 2021 is the initiation of a joint collaborative project with Working Group B TF CIIP on developing a Guide for the Process of Identifying Critical National Infrastructures (CNI). The TF presented its work during the GFCE Showcase Meeting in September and identified three research topics for the Global CCB Research Agenda 2022.

The leadership of TF CBMs/Norms Implementation and Cyberdiplomacy changed in 2021 as Kaja Ciglic stepped down and Nikolas Ott joined Szilvia Toth as TF lead in November. In 2021, two research ideas that were identified by the TF as knowledge gaps were commissioned as research projects through the Global CCB Research Agenda mechanism. TF members engaged in the research by providing input and comments on the research reports during feedback cycles, participating as interview respondents to share their experiences and participating in validation exercises. The researchers also participated in TF meetings to explain the project, share their findings, and answer questions. This also created opportunities for TF members to share their experiences and have open discussions on the topics of norms implementation and cyberdiplomacy. The TF identified two research topics for the Global CCB Research Agenda 2022.

For 2022, both TFs are focused on maintaining an overview and creating awareness on relevant efforts, increasing the visibility and accessibility of products, continue building upon work already done and pooling TF members' knowledge and expertise to demonstrate its added value. More information on the group's ambitions for 2022 is detailed in the Working Groups Workplan in Annex.



Working Group B
Cyber Incident Management & Critical Infrastructure Protection

Cyber Capacity Building (CCB) on incident management and infrastructure protection aims to strengthen capacities that allow nations to respond to and recover from cyber incidents in a timely and efficient manner.

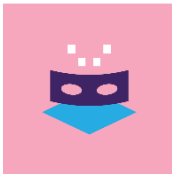
Working Group B is chaired by Abdul-Hakeem Ajijola and it is divided into two Task Forces (TF):
1. TF Cyber Incident Management (TF CIM) - TF Lead Maarten van Horenbeeck (succeeded by Vilius Benetis since November 2021)
2. TF Critical Information Infrastructure Protection (TF CIIP) – TF Lead Marc Henauer

The Task Force on Cyber Incident Management (CIM) has concentrated its efforts in developing two key deliverables. It has updated the Global CSIRT Maturity Framework (GCMF) with the aim of stimulating the development and maturity enhancement of national CSIRTs. The GCMF combines previous models that are widely recognised and adopted, in particular, the Open CSIRT Foundation SIM3 model and the European Union Network and Information Security Agency (ENISA) three-tier maturity approach. This new updated version includes more in-depth information and explanation about the relevance of different parameters of the maturity model for national CSIRTs. It has also completed the Getting Started with a National CSIRT Guide. This guide is meant for anyone who wants to learn more about setting up a national CSIRT (nCSIRT). It includes seven different modules that document experiences from experts across the world, drawing from their experiences with the aim to guide the reader through the planning, development and initial stages of nCSIRT capacity building.

The Task Force on Critical Information Infrastructure Protection (CIIP) has focused on developing three major deliverables in 2021. First the joint project between the Task Force on Strategy & Assessments from Working Group A and the Task Force on Critical Information Infrastructure Protection (CIIP) on Developing a **Guide for the Process of Identifying Critical National Infrastructures (CNI) and Critical Information Infrastructures (CIIP).** The aim of this project is to provide GFCE Community with a tool to support them in their National Cybersecurity Strategy (NCS) lifecycle. This guide will include examples that illustrate several different Critical National Infrastructures identification aspects of the NCS development and implementation lifecycle.

Second, the Task Force is also helping develop the **GFCE and the Meridian Cooperation Project.** This project aims to bring together the GFCE and the Meridian communities, particularly in contributing expertise and experience on Critical Information Infrastructure Protection. This project has 3 main objectives that range from: (i) Aligning Meridian community topics with the GFCE Task Force on CIIP (including invitation for the Meridian community to join the CIIP Task Force, share and discuss issues of common concern as well as good practices related to CIIP, support the realization of specific CIIP deliverables; (ii) Virtual meeting opportunities in-between the annual Meridian conference (Support from the GFCE Secretariat to the Chair and the Meridian community in organizing online events that lead to the next Meridian conference; (iii) Identifying research needs linked to CIIP and cyber capacity building.

Third, with the aid of The Netherlands and TNO the Task Force developed the GFCE CIIP Capacity Framework**.** This framework supports the discussion on CIIP and the exchange of good practices by specifying the capacities that may be part of a CIIP approach, while at the same time provides knowledge to policymakers on how to establish and maintain sustainable and efficient efforts to protect CII by outlining the required capacities. It also describes CIIP capacities in a general way to allow for the adjustment of capacities to national conditions.



Working Group C
Cybercrime

Working Group C brings together governments, industry and experts focused on the coordination of efforts relating to legal frameworks, criminal justice, as well as formal and informal cooperation frameworks in the field of cybercrime.

Working Group C is chaired by Joyce Hakmeh, Senior Research Fellow International Security Programme & Co-Editor of the Journal of Cyber Policy at Chatham House.

Cybercrime Series
In 2021 the Working Group started a new initiative, aimed at sharing knowledge and expertise on cybercrime topics with the community in a structured way. With the Working Group identifying the topics to be discussed, the Cybercrime Series is also considered a soft agenda-setting exercise within the group.

The first session looked at cybercrime trends and developments, painting a picture of what cybercrime looks like from various perspectives, how it is evolving, and what the main challenges are for policymakers and other stakeholders. The second section looked at what needs to be done, with a strong focus on how capacity building can help address these issues. Speakers included UNODC, FireEye Mandiant, Europol, Global Cyber Alliance and INTERPOL. The Series will be continued into 2022, with one session planned per quarter.

Research Agenda 2022
The Working Group identified 9 research topics. Working Group members voted on the 9 topics, with the chosen topic to be included in the Research Agenda 2022. All draft topics received votes, so they will be included in the Annex of the Research Agenda as a reference of the knowledge gaps identified by the Working Group. The final Agenda, with chosen topics of each Working Group, will be presented during the Annual Meeting. The chosen topics will be put to an RFP in 2022 and supported with a request for funding.

Participation in international and industry events
The GFCE and Working Group C members also participated in a number of other industry meetings and events. These include contributions to the GFCE Community Showcase, Council of Europe 2nd Africa Forum, GFCE Consultation Meeting, OSCE Cybercrime Briefing, Council of Europe Octopus Conference and the World Bank Cyber Resilience Series, following discussions such as those in the United Nations Open-Ended Intergovernmental Expert Group, UN Ad-Hoc Committee, the EU ISS Paths for Multi-stakeholder Engagement in the Fight Against Cybercrime, and participation in a briefing on ransomware to diplomats from the Netherlands.

Working Group D
Cyber Security Culture & Skills

Working Group D is chaired by Tereza Horejsova (DiploFoundation). 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 sharedresponsibility to practice safe and informed behaviors in the use of ICTs (Cyber Security Awareness)
B. Involve all stakeholders to create a workforce with a set of cyber security skills and knowledge employers require (Education, Training & Workforce Development).

Working Group D hosted several virtual meetings during which participants had the opportunity to discuss the Working Group's activities included in the Work Plan 2021, promote knowledge-sharing, exchange best practices and share updates on cyber capacity building topics.

With regards to the Global CCB Research Agenda 2021, Working Group D submitted a **research idea on "Developing cyber skills amongst the young"** which received funding and was developed by a research team from the University of Kent. The aim of the project is to understand how cyber security skills development is currently covered in pre-university curricula in different countries and regions, technical and non-technical approaches used to develop cyber security skills for different age groups up to 18, and the role of different stakeholders in such skills development activities.

To support the collaboration on new projects, a project team was formed in 2021 to develop and work on a new initiative proposed by the United Kingdom, on **developing 'Cyber Security as a Profession'**. The team identified that there is an increasing demand globally for cyber security skills and increasing the number of qualified cyber professionals is a global challenge that is likely to become more acute over the coming years. In many countries, the current qualification and certification landscape for cyber security is difficult to navigate and that brings many challenges. For this reason, the project team created a survey to raise awareness and gather international views on developing cyber security as a profession. The survey explores how we can cement professional standards and quality assurance in the profession without adding unnecessary barriers to entry and progression, how we can ensure we are attracting the next generation of cyber security professionals, and how we can ensure employers are able to recruit the right people.

To participate in the survey, use this link. After the survey, the team will analyze the responses and publish a short report setting out the key messages and next steps.

General Ongoing Activities – GFCE Working Groups 2022

Activity	Actions	Lead	Timeframe	Comments
General WG Objective 1 : Knowledge and expertise sharing through regular engagement opportunities				
GFCE Community Showcases	Submit proposals for a showcase	WG/TF members	March 2022 June 2022 September 2022	GFCE Secretariat to host and handle logistics.
	Participate in showcase events	WG/TF members		
Working Group [Town Hall] Meetings	Submit suggestions for agenda	WG/TF members	At least twice a year	Secretariat to host. In addition to other meetings (e.g. GFCE global events, project team meetings, brainstorm sessions, etc)
	Participate in discussions	WG/TF members		
Sharing information on events	Inform the Secretariat / Working Group of relevant events (training, networking, workshops etc)	WG/TF members	Ongoing; prior and during meetings	Secretariat to consolidate information and update Cybil https://cybilportal.org/events/
General WG Objective 2: Support contributions to and use of the GFCE Tools through regular updates and reviews				
GFCE Research Agenda	Submit/review ideas for the Research Agenda	WG/TF members	Prior to the Annual Meeting 2022	GFCE Research Committee & Secretariat to support.
	Provide comments on research proposals/drafts			
Cybil Portal	Members contribute to Cybil, sharing updates on projects/resources	WG/TF members	Ongoing	GFCE Cybil Steering Committee & Secretariat to Support.
	Members review own profiles			
General WG Objective 3: Provide a platform for GFCE members and partners to showcase expertise, to enable better understanding of cyber capacities as they apply in African countries (AU-GFCE Project)				
AU-GFCE Knowledge Modules	Engage in the deployment of the KMs by participating in the in-person or virtual events	WG/TF members (with DiploFoundation)	Between February 2022 - July 2022	GFCE Secretariat to support.

GFCE WG A TF Strategy & Assessments Work Plan 2022

Project/activity	Actions	Lead	Timeframe	Comments
Objective 1: Maintain an overview of the NCS and Assessments landscape, in the spirit of coordination and knowledge sharing				
Internal tracker on the NCS and Assessments	Provide updates on any new, planned, started or completed Assessments or Strategies.	All TF members	Ongoing	
	Update internal tracker and make available to TF. Notify NCS repository-owners when new NCS are published.	GFCE Secretariat (Kathleen)	Ongoing	
Quarterly Task Force Newsletter	Development and dissemination of the Newsletter: updates on the internal tracker, workplan updates and upcoming events.	GFCE Secretariat & TF Leaders, with contributions from the TF.	Quarterly	
Quarterly Cybil Review	Presentation to raise awareness on recently added projects/resources on the Cybil Portal that is relevant to NCS or Assessments	Presentation by TF Leaders.	Quarterly.	TF members expected to update and contribute to Cybil regularly, see General Activities in Annex.
Objective 2: Increase accessibility and reach of the NCS Catalog				
The NCS Catalog will be converted to a web-based tool and made accessible in 3 languages.	Test and provide comments on the Beta version of the web-tool.	Looking for volunteers – will be shared with the whole TF.	First half 2022	The development of the Catalog into a web-based tool is kindly supported by US State Department.
	Identify (public) events to promote the NCS Catalog more widely, develop a plan with a timetable on promoting the tool.	Looking for volunteers	By September 2022	TF might be interested to convene a side meeting at a relevant event.
Objective 3: Develop (free) resources to support countries in their NCS journey by pooling TF members' expertise and knowledge				
NCS Interview series, covering different aspects: i) Communicating new NCS ii) Strengthening cross-government coordination iii) New NCS in 2021 iv) Receiving NCS Support in 2021	Identify potential interview respondents, draft interview questions, and circulate questions with respondents.	Project Team • Looking for volunteers!	Project to conclude by September 2022	The interview series will be an update to the WG's 2018 National Strategies Interviews behind the cover.
	Consolidate responses into one document, format/edit document for publication on the Cybil Portal.			Budget may be necessary to edit/translate document – looking for in-kind support from TF.
Standard Support Package	Develop a Standard Support Package to highlight the most useful resources and initiatives available to actors when designing, delivering, assessing or seeking Support.	GFCE Secretariat + contributions from the TF.	First half 2022	

GFCE WG A TF CBMs/Norms & Cyberdiplomacy Work Plan 2022

Project/activity	Actions	Lead	Timeframe	Comments
Objective 1: Create awareness and increase reach of the 2 concluded research projects: Cyberdiplomacy & Norms Implementation				
Disseminating the outcomes of the 2 research projects that were requested by the TF.	Identify (public) events to promote the findings of the research projects more widely, develop a plan with a timetable on its promotion.	TF Leaders	By March 2022	
Objective 2: Support countries that require assistance with building up Cyberdiplomacy capacity in their MFA				
Good practice guide/ recommendations for countries that want to develop Cyberdiplomacy capacity in their MFA … OR… Interview series with cyber diplomats	Determine potential topics/areas to be covered, identify cyberdiplomacy practitioners to contribute tips, expertise and share lessons learned.	Project Team Looking for volunteers!	First half 2022	Note existing podcast 'Inside Cyber Diplomacy', how can the TF build upon this?
Standard Support Package	Maintain an overview of cyberdiplomacy trainings and highlight useful resources and existing expertise within the TF. Create a plan to increase awareness of available trainings and resources.	GFCE Secretariat, with contributions from the TF.	Ongoing	Finding from Cyberdiplomacy research project: lack of awareness on diplomacy trainings & suspicions of biased trainings
Objective 3: Create awareness and support for multi-stakeholder engagement in international cybersecurity negotiations (e.g. at the UN)				
Actively support the implementation of CCB-related outcomes from the OEWG/GGE reports.	Pick 1-2 topics where the GFCE Community can contribute meaningfully to support implementation efforts.	Project Team Looking for volunteers!	Sep 2022	
	Develop statements and participate in discussions on the role of multi-stakeholder actors and the GFCE on CCB elements in the OEWG/PoA.			
	External engagement to promote the TF and support GFCE leadership in 1:1 meetings with governments on how the group can help and hearing on what they would like to see		Twice monthly	
	Identify core group of countries and work with them on implementation.		First quarter 2022	

GFCE WG B TF Cyber Incident Management Work Plan 2022

Project/activity	Actions	Lead	Timeframe	Comments
Objective 1: Foster trust and better cooperation in in the incident response community				
Developing a framework or guide on how national CSIRTs can cooperate with sectorial CSIRTS	Prepare a concept note that defines background information, aim/ purpose of the guide and work schedule,	Vilius Benetis (NRD), Abdul-Hakeem Ajijola (WG B Chair), Mark Zajicek (SEI), Sanjay Bahl (India), Marwan Ben Rached (ITU), Klee Aiken and Richard Harris (MITRE).	February 2022	Budget may be necessary to edit/translate document – looking for in-kind support from TF.
	Develop the guide for cooperation among nCSIRTs and sCSIRTs	Project team	February-May 2022	
	Publish the guide	Project team + GFCE Secretariat	June 2022	
Objective 2: Aid in preventing further incidents and reducing the harm from said cyber incidents				
Proactive communications and information in Cyber Incidents	Prepare a concept note that defines background information, aim/ purpose of the guide and work schedule	Maarten Van Horenbeeck (WG B CIM Taskforce Leader), Richard Harris (MITRE), Abdul-Hakeem Ajijola (WG B Chair), Mark Zajicek (SEI), Vilius Benetis (NRD), Sanjay Bahl (India), Marwan Ben Rached (ITU), Hadyn Green, Klee Aiken and Andy Purdy (Huawei).	First half 2022	Has been proposed a research topic for the 2022 Global Research Agenda
	Develop the guide for countries to establish a crisis management plan	Looking for volunteers	By September 2022	
	Publish the guide	Project team + GFCE Secretariat	BY November 2022	
Objective 3: Developing a training and educational framework for CSIRTs.				
Continuation of the CSIRTS Training framework for Low-Income Countries initiative	Create a strategic level framework for CSIRTs in low income countries to train, and retain qualified personnel	Sanjay Bahl (India), Mark Zajicek (SEI), Klee Aiken and Hanneke Duijnhoven (TNO).	First half 2022	Budget may be necessary to edit/translate document – looking for in-kind support from TF.
	Publish the framework	Project team + GFCE Secretariat	By September 2022	

GFCE WG B TF Critical Information Infrastructure Protection Work Plan 2022

Project/activity	Actions	Lead	Timeframe	Comments
Objective 1: Ensure a rapid and adequate response to cyber incidents in Critical Information Infrastructures				
Develop a guide for countries to establish a crisis management plan	Prepare a concept note that defines background information, aim/ purpose of the guide and work schedule,	A Vilius Benetis (NRD), Hanneke Duijnhoven (TNO), Richard Harris (MITRE), Sanjay Bahl (India), and Mark Zajicek (SEI).	February 2022	Budget may be necessary to edit/translate document – looking for in-kind support from TF.
	Develop the guide for countries to establish a crisis management plan	Project team	February-July 2022	
	Publish the guide	Project team + GFCE Secretariat	June 2022	
Objective 2: Enhance understanding of key issues associated with a focused cyber-attack, including coordination and information sharing in response to such an attack.				
Guide for carrying out Cybersecurity Table-top exercises (TTX).	Prepare a concept note that defines background information, aim/ purpose of the guide and work schedule,	Hanneke Duijnhoven (TNO), Sanjay Bahl (India), and Mark Zajicek (SEI).	February 2022	Budget may be necessary to edit/translate document – looking for in-kind support from TF.
	Develop the guide for carrying out Cybersecurity Table-top exercises (TTX).	Project team	February-July 2022	
	Publish the guide	Project team + GFCE Secretariat	By September 2022	
Objective 3: Aid in strengthening the internet infrastructure				
Develop a guide on securing National Internet Infrastructure.	Develop a guide on securing National Internet Infrastructure.	A Vilius Benetis (NRD), Hanneke Duijnhoven (TNO), Richard Harris (MITRE), Sanjay Bahl (India), and Mark Zajicek (SEI).	First half 2022	Has been proposed a research topic for the 2022 Global Research Agenda
	Publish the framework	Project team + GFCE Secretariat	By September 2022	

GFCE WG C Cybercrime Work Plan 2022

Activity	Actions	Timeframe	Comments
Objective 1: Raising awareness and understanding on key cybercrime issues and topics			
1.A. GFCE Cybercrime Series	Provide suggestions & input for discussion topics, session format & speaker(s) of upcoming session(s)	Quarterly	GFCE Secretariat to coordinate input opportunities, sharing takeaways & gathering feedback Next session Jan 2022 (TBC)
	Participate in sessions		
	Follow up on key takeaways (e.g. updates in WG discussions, suggesting new project ideas)		
Objective 2: Develop and maintain an overview of the international cybercrime landscape			
2.A. Mapping competent cybercrime institutions & authorities at national, regional & international levels	Contribute to mapping exercise within Working Group C, providing information on relevant institutions/authorities (including competence and focus areas)	By May 2022	
	Expand mapping to collect information on external institutions & authorities, as well as existing tools or trackers	Mid Q2-Q4	
	Collate all information in common overview/database	By GFCE AM22	
2.B. Quarterly Working Group Newsletter	Provide updates on projects, publications, tools, relevant for the Working Group	Continuous; Prior to release of Quarterly newsletter	Secretariat to coordinate & compile and share newsletter with Working Group
Objective 3: Create awareness and support for multi-stakeholder engagement in international negotiations, such as the UN			
3.A. Connect the Working Group and its members with international discussions on cybercrime	Discussion within Working Group on UN processes (agenda, outcomes and timeline) & areas of alignment	By end Q1	
	Provide input & updates to Working Group on participation in discussions on role of multi-stakeholder actors with regards to the UN processes	Regular/ continuous	

GFCE WG D Cybersecurity Culture & Skills Work Plan 2022

Project/activity	Actions	Responsibility	Timeframe	Comments
Objective 1: Maintaining an overview of the Cybersecurity Awareness, Education and Workforce landscape, in the spirit of coordination and knowledge sharing				
Quarterly Working Group Newsletter	Development and dissemination of the Newsletter: updates on workplan, upcoming activities and events	GFCE Secretariat & WG Chair, with contributions from the WG.	Quarterly	
Quarterly Cybil Review	Presentation to raise awareness on recently added projects/resources on the Cybil Portal that is relevant to awareness, education and workforce	GFCE Secretariat & WG Chair	Quarterly	WG members expected to update and contribute to Cybil regularly, see General Activities in Annex
Objective 2: Raise awareness on developing cybersecurity as a profession				
Project on developing 'Cyber Security as a Profession'	Develop the survey and translate in French and Spanish	Project Team (support from GFCE Secretariat)	By November 2021	
	Circulate the survey within and outside the GFCE Community	GFCE Secretariat & Project Team, with support from the WG.	By January 2022	
	Analyze responses and write the report	Project Team	By February 2022	
Objective 3: Develop resources to support knowledge sharing by pooling WG members' expertise and knowledge				
Standard Support Package	Develop a Standard Support Package to highlight the most useful resources and initiatives available to actors when designing, delivering, assessing or seeking Support.	GFCE Secretariat + contributions from the WG.	First half 2022	
Guide on cybersecurity skills/education/trainings for professionals	Actions for idea TBD	WG for volunteers	NA	