Contribution by the Global Forum on Cyber Expertise (GFCE)

to facilitate the preparation of the report requested by the Secretariat for the seventh session of the OEWG, scheduled from 4-8 March 2024

On behalf of the Global Forum on Cyber Expertise (GFCE) Foundation Board and at the request of the UN Office for Disarmament Affairs (UNODA) to invite stakeholders views on the landscape of information and communications technologies capacity-building programmes and initiatives within and outside the United Nations, the GFCE Secretariat submits the following overview of the global cyber capacity building (CCB) landscape. In this contribution, the GFCE's initiatives and efforts on cyber capacity building will be reiterated. A short analysis of ongoing capacity building projects on the knowledge portal – Cybil[1] (CybilPortal.org) – and its utility in mapping and gathering information on ongoing CCB programmes and initiatives will be presented thereafter.

Background Context

Many countries still lack the technical, institutional and policy capability to respond to malicious cyber events, including the capability to cooperate internationally, and lack the ability or expertise to fully participate in the many international debates that are shaping the future of cyberspace. A substantial answer to both preparing countries to deal with cyber threats and ensuring they can more fully participate in policy implementation is cyber capacity building. We therefore **welcome and support the continued emphasis on capacity building**, as well as the request to map existing initiatives and efforts. We hope that the upcoming sessions will recognize and promote leveraging existing capacity building efforts from regional and international institutions, and multistakeholder platforms, including the GFCE (for further reading, please see recommendations made in the GFCE's Contribution to the second substantive session of the OEWG).

GFCE Efforts

The GFCE is an apolitical multistakeholder community of over 190 members and partners including member states, international and regional organizations, private sector, civil society and academia, dedicated to the global coordination and promotion of cyber capacity building. The Forum holds a **unique position** as it is already playing a key role in facilitating and coordinating capacity building efforts, made possible by its neutrality, multi-stakeholder community, and bottom-up approach.

[1] The Cybil Portal was launched in 2019 as an initiative of the GFCE together with several knowledge partners, and it is overseen by the GFCE Advisory Board consisting of civil society and technical community representatives.

The GFCE has developed and maintained a flexible and diverse ecosystem that is geared towards the needs of the community and that mobilizes multistakeholder engagement by design. Since 2015, the GFCE has been harnessing and **consolidating existing capacity building** efforts, making capacity building more effective, through its ecosystem to strengthen coordination, facilitate knowledge sharing, and connect assistance requests with support or resources. The ecosystem includes tools such as the GFCE's Research Agenda, the Cybil Portal and Clearing House mechanism, as well as structures such as the GFCE Working Groups and Regional Hubs.

The Working Groups have been leveraged by the community to **identify knowledge gaps** and prioritize them, resulting in the development of an annual Global Capacity Building Research Agenda. Four research projects have already been concluded through this mechanism, effectively engaging the broader Academic Community to address cyber capacity knowledge gaps. Of relevance to discussions on responsible state behavior in cyberspace is, for example, the research project on cyber norms implementation (Putting Cyber Norms in Practice) which looks at national examples from across the world to illustrate how norms can be implemented in various national contexts and formats. The academic community, as authors of the research reports and as members of the GFCE Research Committee, supports capacity building in this regard by providing data, evidence, analysis and research generated through the organization's mechanism to seek and support informed practical and policy capacity solutions.

The Clearing House is a GFCE Tool which aims to **facilitate matchmaking** between GFCE Members who have cyber capacity needs with GFCE Partners and Implementers that can, in turn, offer cyber capacity support. With an effective global clearing house mechanism, the GFCE hopes to improve efficiency on a global level in the delivery of capacity building programs through coordination and knowledge sharing. 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, each Clearing House request received is unique, and therefore a tailor-made approach is utilized to evaluate each case. The GFCE has supported several member countries build cyber capacity through the Clearing House mechanism including Tunisia and Sierra Leone with the drafting of their National Cyber Security Strategy, Senegal with setting up a CSIRT and their national CIIP framework, and The Gambia with cybercrime legislation.

On the other hand, Cybil contributes to stronger global cyber security and cybercrime capacity by helping capacity building projects be more effective – through **enhancing accessibility on information and improving transparency**. The Cybil Portal catalogues expertise, tools, publications, and CCB projects from all corners of the globe. It is **a global, open and free knowledge repository** with information on close to 900 projects, 400 tools and publications, and 895 active actors. As a multistakeholder knowledge-sharing platform, Cybil adds value by allowing actors to map and gain a baseline understanding of capacity building projects that often involve actors across sectors. Users can discover projects, tools, and actors, by filtering diverse contributions along various lines. Information and updates for the Portal is primarily provided by the multistakeholder GFCE Community. They also provide feedback for improvement and suggest the addition of new features. The contributions of the multistakeholder community include updates on projects that they are implementing or supporting (ranging from the establishment of CERTs to delivering cybercrime training), new tools or reports that they have developed, and webinars or events they are organizing.

Lastly, to realize a demand driven approach to capacity building and to empower local capacity building communities, the GFCE started to build regional nodes and further increase its regional focus over the last three years. A regional approach is favorable because States tend to share similarities in priorities and are able to reach a common understanding, agreement or way forward more easily than in other multilateral fora. As capacity building requires trust between implementers and the beneficiary community to ensure sustainable and long-term impact, the GFCE is **committed to connecting and collaborating with regional organizations**/centers and key leaders to bolster regional efforts. The establishment of GFCE regional hubs and liaisons in five regions (Americas, Pacific, Southeast Asia, Pacific, and Africa) will support needs analysis, regional coordination and delivery of capacity building support from the GFCE community in a unique manner.

Past mapping exercises

Through and beyond regional programs, the GFCE has been conducting foundational mapping exercises of existing projects as well as resources and policy landscapes (see the GFCE's Overview of existing Confidence Building Measures (CBMs), submitted to the OEWG in 2022). The latest mapping efforts leverage the GFCE's strong partnerships with regional organizations such as the Organization of American States (OAS), Organization of Security and Cooperation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN) alongside their respective Member States, with improved regional coordination and information sharing one of the key benefits and objectives of the partnership with OAS as the GFCE Hub in the Americas.

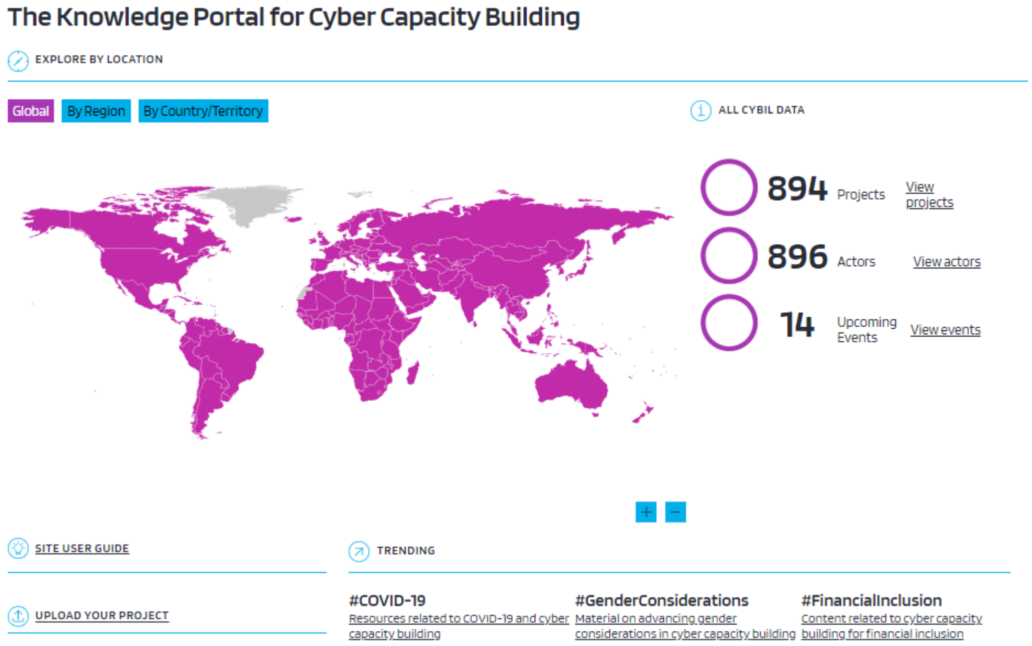
However, to expand mapping efforts and support the Community, the GFCE recognizes that more needs to be done to increase high-level awareness and commitment to widen the pool of resources available. Over the years, the Cybil Portal has grown to host a significant number of projects from around the world. The Portal is a growing comprehensive source of basic project information and is a good starting point for setting a baseline for mapping activities globally. It has been used by researchers to inform on trends in cyber capacity building, or by implementors to gain initial understanding of recipient countries capacity building contexts, and has been leveraged as a tool by academics in creating indicators for cyber capacity power (see the GFCE's Submission to the fifth substantive session of the OEWG for more information on Cybil).

Guiding principles

With reference to principles contained in para. 56 of the final substantive report of the 2019-2021 OEWG, the Cybil Portal contributes to increasing recognition that capacity-building initiatives have the greatest impact when projects are sustainable, nationally-owned, non-discriminatory and contribute to an open, secure, stable, accessible and peaceful ICT environment. Projects catalogued on Cybil reflect these principles while additionally illuminating multistakeholder and triangular cooperation efforts that contribute to national capacity development. As stakeholder engagement in CCB constitutes an integral part of confidence-building, Cybil contributes a unique multistakeholder catalogue and knowledge portal that covers these various efforts.

Mapping Cyber Capacity Building

The Portal maintains an initial overview on existing and past cyber capacity building projects and programs by ascribing characteristics to activities (region, theme, actor type, status, resource type, and data related chart information). Content is categorized along five key capacity-building themes prioritized and endorsed by the Community through the Delhi Communique in 2017. While not an exhaustive list of capabilities that a country or organization might implement to achieve a desired level of cyber resilience, the GFCE identified these capacity building themes as a baseline reference for good cyber practices. Additionally, while logged projects are often either received, funded or implemented by national actors (such as ministries of telecommunication), actors from other sectors are linked and tagged on project pages. To that end, users can filter results along different sectors (civil society, knowledge institution, private sector, and government).



The Knowledge Portal for Cyber Capacity Building

EXPLORE BY LOCATION

Global | By Region | By Country/Territory

ALL CYBIL DATA

894 Projects View projects

896 Actors View actors

14 Upcoming Events View events

SITE USER GUIDE

UPLOAD YOUR PROJECT

TRENDING

#COVID-19
Resources related to COVID-19 and cyber capacity building

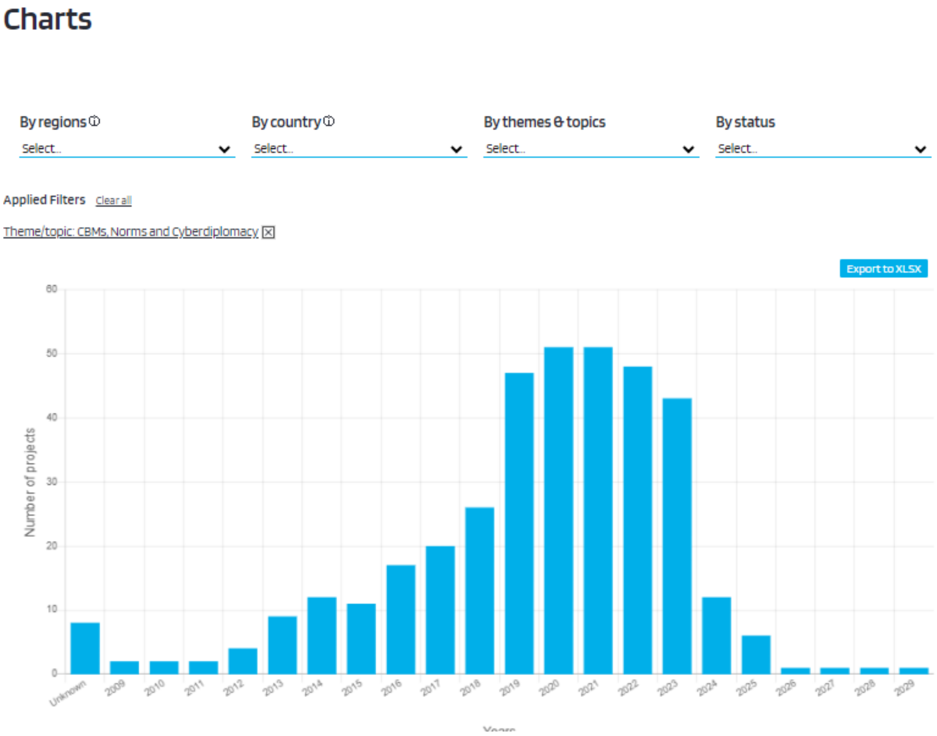
#GenderConsiderations
Material on advancing gender considerations in cyber capacity building

#FinancialInclusion
Content related to cyber capacity building for financial inclusion

Figure 1. The Cybil Portal Homepage (CybilPortal.org)

Charting growth: 2013 to 2023

In 2021, Cybil introduced a new function which synthesizes data and illustrate trends visually through bar charts. The bar chart represents the number of projects active per year using the information uploaded to the Cybil Portal, providing an overview of projects beginning as early as 1999. When applying *CBMs, Norms and Cyberdiplomacy* as a thematic filter, for example, a visual demonstration of projects by year is made available for initial mapping purposes, as illustrated in the figure below. The bar charts enable users to gain a quick impression of when the first projects on *CBMs, Norms and Cyberdiplomacy* were initiated – two of which were active as of 2009. The chart also indicates that 12 projects or activities on *CBMs, Norms and Cyberdiplomacy* are currently logged on Cybil as ongoing and will be completed in 2023.[2]



Charts

By regions ⓘ: Select...

By country ⓘ: Select...

By themes & topics: Select...

By status: Select...

Applied Filters Clear all

Theme/topic: CBMs, Norms and Cyberdiplomacy ☒

Figure 2. This Bar Chart shows active capacity building projects by year, with the thematic filter *CBMs, Norms and Cyberdiplomacy* applied.

[2] **Note**: It is up to submitting organizations to choose how they divide their activities into projects for the purpose of sharing information about them through the Portal. This results in a wide variety of project sizes and durations reflecting different uses of the term project across organizations and different decisions on how best to communicate capacity building activities. We advise considering these caveats when working with the chart data.

Ongoing projects on the Cybil Portal

The following section provides **a snapshot of ongoing projects** that are available on the Cybil Portal. These cases illustrate the multistakeholder and layered process of capacity building that include not only States, but also other involved actors. The portal also exemplifies south-south and triangular cooperation projects and activities.

Regional

As of the end of October 2023, there are **156 ongoing projects** catalogued on Cybil. Of these, **32 are ongoing in Asia** (encompassing Central, South, and Southeast Asia). Prominent projects include the Singapore Cybersecurity Centre for Excellence, running since 2019 and funded as well as implemented by Singapore, with ASEAN member state beneficiaries and private sector as well as academic institutional partners involved in the project. Activities of the project target three of the GFCE's identified CCB topics (Cyber Security Policy and Strategy, Cyber Incident Management & Critical Information Protection, Cybercrime). Another prominent project is Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World (2021-2023) (as part of Cyber Security Culture & Skills), convened in the Asia-Pacific region for women-led cybersecurity reform and leadership in the region, and implemented by UN Women.

In Pacific Oceania,16 ongoing projects are currently documented. One of which is the New Zealand Cyber Security Capacity Building in the Pacific Programme, initiated and funded by the New Zealand ministry of Foreign Affairs and Trade as well as the New Zealand Computer Emergency Response Team. The project focuses on supporting Pacific partners to develop national cyber security strategies, strong security standards and frameworks, effective CERTs, and other capacity, for the long-term longevity and resilience of their cyber systems.

In Europe, there are 23 ongoing projects catalogued in the Portal. One of which is the facilitation of the development and implementation of National Cyber Incident Severity Scales (NCISS) and related measures to protect critical infrastructures among European, Central Asian, and other countries. The project focuses on Confidence Building Measures (CBMs), such as crisis communication and management procedures, as well as incident classification methods. The Organization for Security Co-Operation in Europe (OSCE) is the implementor of this project, while beneficiaries are OSCE participating States. Further, an ongoing partnership-project Enhancing Security Cooperation In and With Asia, funded by the European Union and implemented by German and French government development agencies, is a cross-regional effort to promote greater convergence between Europe and Asia on policies, practices, and general awareness of responsible state behavior in cyberspace. Lastly, the Good Governance in Cybersecurity in the Western Balkans project, funded by the United Kingdom, and implemented by the Geneva Centre for Security Sector

Governance (DCAF), supports cybersecurity policy making in the Western Balkans and equips the region with good governance training.

In Latin America, the Caribbean and North America, there are 28 ongoing projects. Most notably the Latin America and Caribbean Cyber Competence Centre, which trains regional ministries with cyber competence skills such as incident response methods, strategy implementation, and national risk assessment. Further, the OAS Cybersecurity Program is an ongoing effort to build technical and policy-level cybersecurity capacities among OAS member states. It supports regional capacity building by enhancing cooperation, coordination, and information sharing among cybersecurity stakeholders at the national, regional, and international level.

In Africa, there are 24 ongoing projects, **and 8 in the Middle East & North Africa**. Her Cyber Tracks is active in both regions. It offers targeted cyber capacity building activities for women involved in national and international cybersecurity policy processes. On the other hand, the Horn of Africa Digital Governance and Cybersecurity Initiative promotes cyber and digital resilience through the strengthening of policy and institutional frameworks that increase cybersecurity awareness and cyber incident response capacity of government officials and IT professionals.

Global

Many initiatives go beyond regional boundaries and extend to benefit States and ministries around the world. **There are 42 ongoing projects catalogued with near-to global reach**, such as the UN-Singapore Cyber Fellowship, an initiative by Singapore and the UN Office for Disarmament Affairs, which engages high-level national cyber officials from all UN Member States, to facilitate exchange on cyber and digital security policy-making strategies, and develop a network amongst global cybersecurity officials. The Octopus Project is a notable effort which supports nations in their implementation of the Budapest Convention, and offers cybercrime-related capacity building training to that end. The Women in International Security and Cyberspace Fellowship is an effort that reaches across continents, and is funded by contributions from six States and is implemented by both national, international, as well as civic, academic and non-governmental organizations. The Fellowship, which provides opportunities for knowledge and skills development within cyber diplomacy, runs congruently to the 2021-2025 OEWG as well as the Ad-Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. These projects exemplify the multistakeholder nature of global efforts to enhance cyber resilience, exchange best practices, and point to efforts that leverage the multistakeholder nature of CCB.

Further Engagement

Though some States and organizations share information on their projects and activities, the vast majority of funders, implementers and beneficiaries are still reluctant to share details on ongoing projects. A lack of sharing may deprive other players and regions from benefiting from lessons learned, it can hamper coordination, lead to potential duplication, and limit helpful input that the sharing party might otherwise receive. Whilst some have legitimate concerns regarding confidentiality of proprietary information, transparency and the greater sharing of information regarding capacity building should be encouraged as the default practice. We therefore encourage States and other actors to share information on their capacity building projects and activities, which would serve to increase transparency and better coordination. The Cybil team currently engages with, and is exploring opportunities to strengthen collaboration with other capacity building knowledge platforms, such as UNIDIR's Cyber Policy Portal, and EU Cybernet's CCB Projects Mapping table. Such collaboration ensures coordination and cross-checking of information, avoiding duplication of efforts and enhancing accuracy of information.

Finally, we reiterate our commitment and availability to support the OEWG and UN Secretariat with the mapping and stock-taking of existing capacity building efforts, and to contribute to encouraging greater synergy and coordination between such efforts, in any way we can. We also encourage Member States and stakeholders to consider the GFCE as a neutral and apolitical forum which provides a unique opportunity for multistakeholders to exchange best practices and expertise on cyber capacity building, as **only through multistakeholderism, can effective capacity building be delivered**. To that end, **the GFCE is an asset to be leveraged** as part of the many pieces of the puzzle needed to strengthen global cyber resilience and expertise. We also look forward to unlocking potential avenues for concrete and action-oriented collaboration that support the implementation of the Framework for responsible State behaviour. For further information on the GFCE please refer to the website of the GFCE at thegfce.org as well as previous contributions to the UN OEWG.