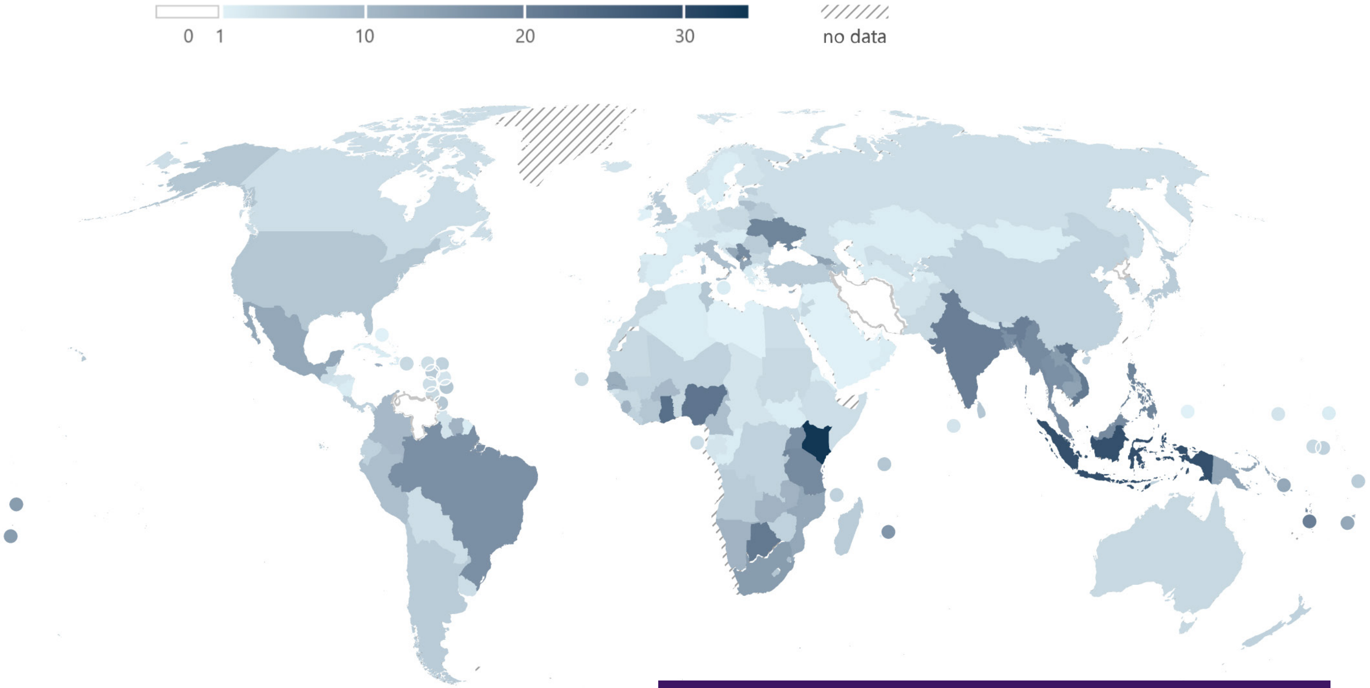
Volume 10, November 2021

GLOBAL CYBER EXPERTISE MAGAZINE

Number of projects by beneficiary country, from 2000 to present.*
Data: Cybil Portal, 2021
*full image on page 10.



TRENDS IN INTERNATIONAL CYBER CAPACITY BUILDING

-page 8-

Volume 10, November 2021

Global Cyber Expertise Magazine

Editorial

Global Developments

Regions

Americas

Europe

Africa

Asia & Pacific

Editorial

On behalf of the Editorial Board, I am pleased to welcome you to Issue 10 of the Global Cyber Expertise Magazine! We are proud to present this edition during the GFCE Annual V- Meeting 2021.

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

In this edition, our cover story takes a look at trends in international cyber capacity building as the field continues to grow rapidly. Also under the global developments section, we celebrate the launch of the 2nd Edition of the 'Guide to Developing a National Cybersecurity Strategy' and learn about how the GFCE is strengthening its demand-driven approach.

From Asia and Pacific, we have an article on cybersecurity in the Pacific and the ASEAN-Japan Cyber Capacity Building Centre (AJCCBC) based in Bangkok. Also, find out more about how Australia is delivering cyber resilience and capacity building projects across Indo-Pacific through cooperation.

From Africa, read about the developments of the AU-GFCE project, an article on the new Network of African Women in Cybersecurity highlights the need to bridge the gender gap and another article introduces the Africa Cyber Capacity Building Coordination Committee.

From the Americas, learn about how the region is consolidating their view on cybersecurity through CBMs and why cybersecurity awareness is so important for the region. Through an interview, the US explains their CCB priorities and why they are providing support to the GFCE.

From Europe, Microsoft shares an overview of the European Cyber Agora as a platform for European multistakeholder discussions on cybersecurity policy. Additionally, we have an article on the role of universities in cyber capacity building.

We thank our guest writers for their valuable contributions to the eighth 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

CONSORTIUM OF GLOBAL EXPERT ORGANIZATIONS LAUNCHES THE SECOND EDITION OF THE GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

Written by: Giacomo Assenza, Cybersecurity Research Officer, International Telecommunication Union (ITU), Francesca Spidalieri, Cybersecurity Consultant, Hathaway Global Strategies and Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Centre (GCSCC)

As of 2021, more than 127 countries have adopted a National Cybersecurity Strategy (NCS) - an increase of 40% in the last three years.[1] However, challenges remain in the adoption and implementation, as well as the adaptation of NCS documents to the ever-changing cyber threat landscape. To help governments in this endeavor, a consortium of leading organizations from the cyber capacity building community jointly published a second edition of the Guide to Developing a National Cybersecurity Strategy. The new edition of this good practice guidance reflects the evolving cybersecurity landscape, emerging security trends and threats, and the growing need for strategic thinking in the development and implementation of the NCS.

National cybersecurity strategies - a global achievement

Over the last two decades, people worldwide have benefitted from the growth and adoption of information and communication technologies (ICTs) and associated socioeconomic and political opportunities. Digital transformation can be a powerful enabler of inclusive and sustainable development, but only if the underlying infrastructure and services that depend on it are safe, secure, and resilient. To reap the benefits and manage the challenges of digitalization, it has become common understanding that countries need to frame the proliferation of ICT-enabled infrastructures and services within a comprehensive national cybersecurity strategy. As a result of this heightened awareness, in 2021, more than 127 countries have adopted an NCS, almost 40% more than three years ago.

NCS in their ever-changing context

In the last decade, most countries have both accelerated their digital transformation and become increasingly concerned about the immediate and future threats to their critical services, infrastructures, sectors, institutions, and businesses, as well as to international peace and security that could result from the misuse of digital technologies and inadequate resilience. This fast-changing nature of cyberspace, the increased dependency on ICTs, and the proliferation of digital risks call for continuous improvements to national cybersecurity strategies and policies.

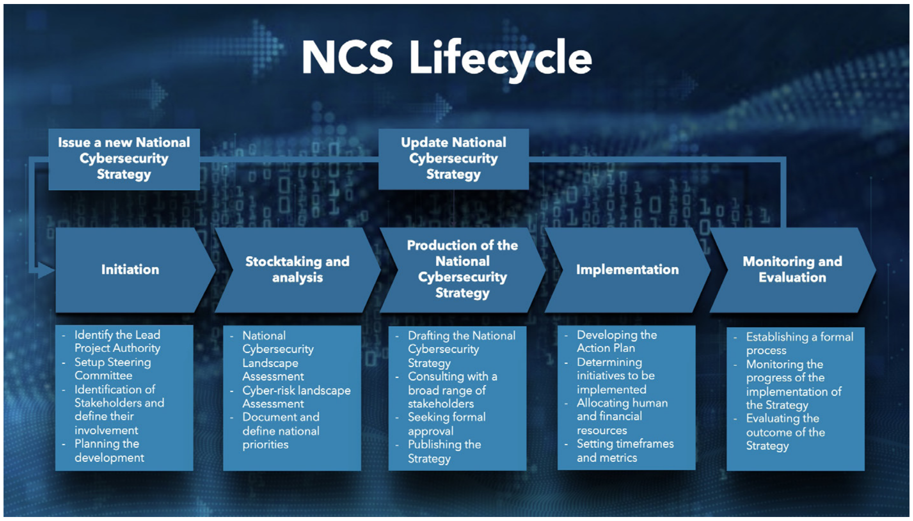
To help governments improve their existing or future NCS, a consortium of nineteen expert organizations (figure 1) working in the field of national cybersecurity strategies and policies came together to contribute their experience, knowledge, and expertise to update the original Guide to Developing a National Cybersecurity Strategy (NCS), v.1. Over the last three years, the first edition of Guide has served governments as an important resource in their NCS journey and it is our hope that the second edition will serve an even growing number of governments and international stakeholders. As in the previous edition, the 2021 edition of the Guide is the result of a unique, collaborative, and equitable multi-stakeholder cooperation effort among partners from the public and private sectors, as well as academia and civil society.

Good practice to prepare an NCS for new risks and challenges

The new edition of the Guide reflects the complex and evolving nature of cyberspace, the requirements for increased cybersecurity preparedness that arise from a growing number of digital risks, as well as other key trends that can impact the cybersecurity posture of a country and should, therefore, be included into national strategic planning. Focus was also given to how to develop, acquire, and prioritize financial and human resources. As in the first version, the objective of the Guide is to instigate strategic thinking and support national leaders and policy-makers in the ongoing development, establishment, and implementation of their national cybersecurity strategies and policies.

> "Cybersecurity is essential to ensure effective and inclusive digital transformation. That is why comprehensive National Cybersecurity Strategies are so important, to reap the benefits and manage the challenges of digitalization, countries need to frame the proliferation of ICT-enabled infrastructure within a comprehensive National Cybersecurity Strategy."
>
> *- Ms Doreen Bogdan-Martin, Director of the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU).*

> "A Strategy is not only a document […] it is how a government is going to play its fundamental role in orchestrating the protection of its national interest in cyberspace."
>
> *- Andrea Rigoni, Global Government and Public Services Cyber Leader, Deloitte.*



NCS Lifecycle

Issue a new National Cybersecurity Strategy

Update National Cybersecurity Strategy

Initiation
- Identify the Lead Project Authority
- Setup Steering Committee
- Identification of Stakeholders and define their involvement
- Planning the development

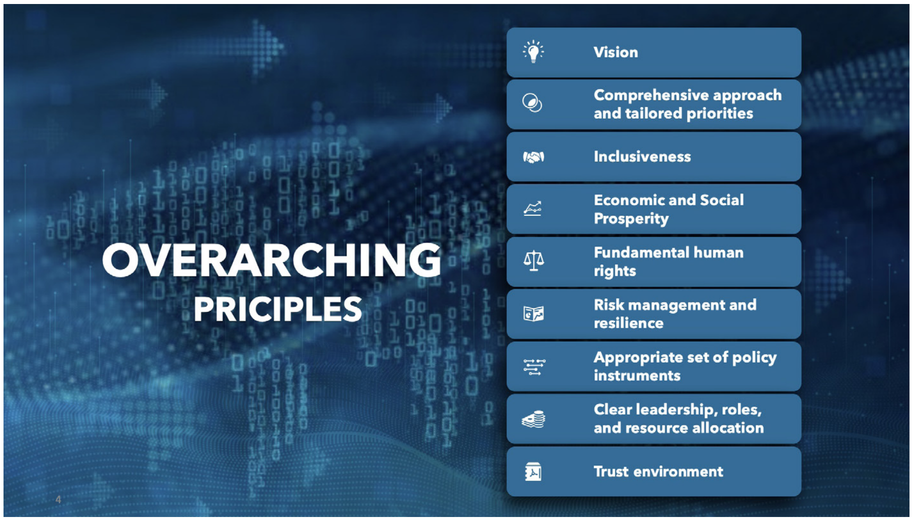
Stocktaking and analysis
- National Cybersecurity Landscape Assessment
- Cyber-risk landscape Assessment
- Document and define national priorities

Production of the National Cybersecurity Strategy
- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy

Implementation
- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources
- Setting timeframes and metrics

Monitoring and Evaluation
- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy

Figure 1. NCS Lifecycle.



OVERARCHING PRICIPLES

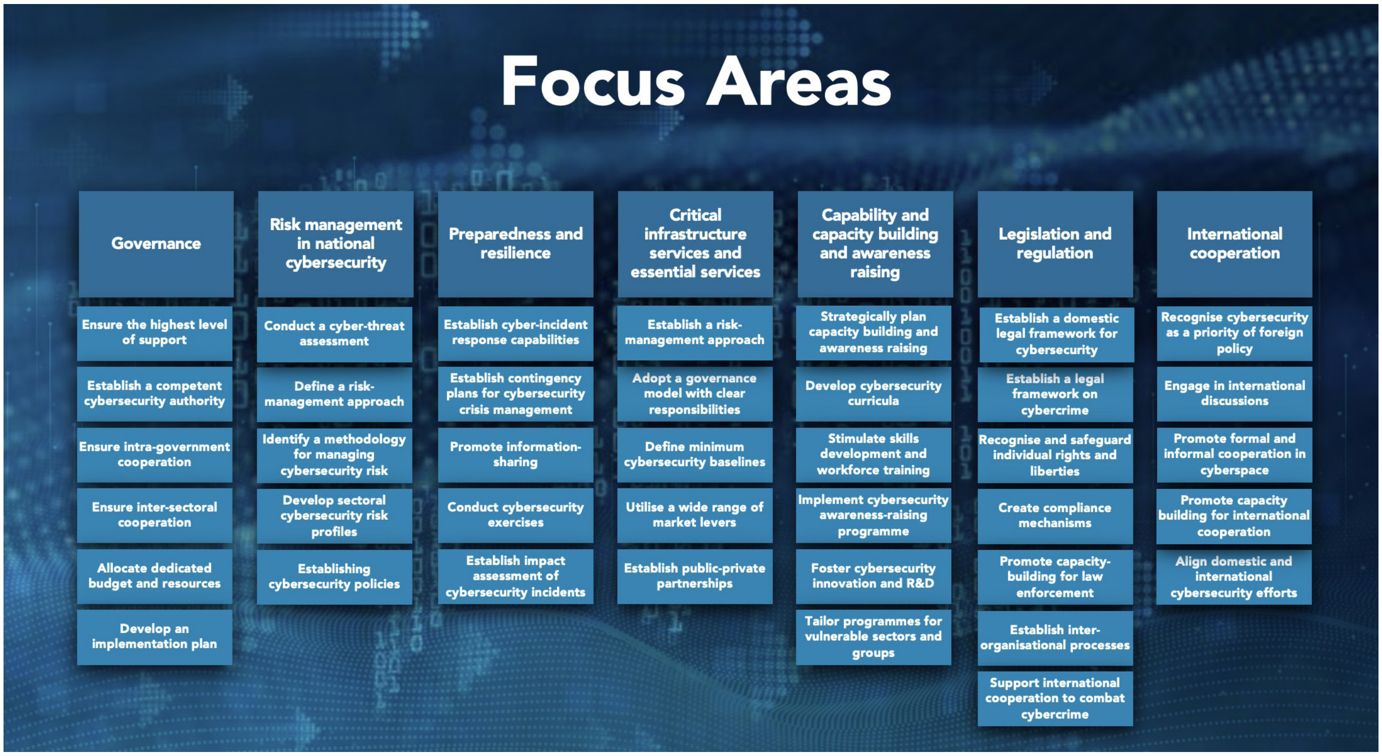
- Vision
- Comprehensive approach and tailored priorities
- Inclusiveness
- Economic and Social Prosperity
- Fundamental human rights
- Risk management and resilience
- Appropriate set of policy instruments
- Clear leadership, roles, and resource allocation
- Trust environment

Figure 2. Overarching principles.

The Guide remains structured in three core areas: 1. NCS Lifecycle (figure 1), 2. Overarching Principles (figure 2), and 3. Focus Areas that should be included in a NCS (figure 3). A reference list of complementary publications and other publicly available resources to support governments on their NCS journey is also provided.

To complement the Guide, a website was launched to further disseminate these good practices included and provide a space for sharing information and experience, provide updates, and contribute to knowledge sharing among governments, as well as implementers and funders of cybersecurity capacity building activities.

Visit: WWW.NCS.GUIDE



Focus Areas

Governance	Risk management in national cybersecurity	Preparedness and resilience	Critical infrastructure services and essential services	Capability and capacity building and awareness raising	Legislation and regulation	International cooperation
Ensure the highest level of support	Conduct a cyber-threat assessment	Establish cyber-incident response capabilities	Establish a risk-management approach	Strategically plan capacity building and awareness raising	Establish a domestic legal framework for cybersecurity	Recognise cybersecurity as a priority of foreign policy
Establish a competent cybersecurity authority	Define a risk-management approach	Establish contingency plans for cybersecurity crisis management	Adopt a governance model with clear responsibilities	Develop cybersecurity curricula	Establish a legal framework on cybercrime	Engage in international discussions
Ensure intra-government cooperation	Identify a methodology for managing cybersecurity risk	Promote information-sharing	Define minimum cybersecurity baselines	Stimulate skills development and workforce training	Recognise and safeguard individual rights and liberties	Promote formal and informal cooperation in cyberspace
Ensure inter-sectoral cooperation	Develop sectoral cybersecurity risk profiles	Conduct cybersecurity exercises	Utilise a wide range of market levers	Implement cybersecurity awareness-raising programme	Create compliance mechanisms	Promote capacity building for international cooperation
Allocate dedicated budget and resources	Establishing cybersecurity policies	Establish impact assessment of cybersecurity incidents	Establish public-private partnerships	Foster cybersecurity innovation and R&D	Promote capacity-building for law enforcement	Align domestic and international cybersecurity efforts
Develop an implementation plan				Tailor programmes for vulnerable sectors and groups	Establish inter-organisational processes	
					Support international cooperation to combat cybercrime	

Figure 3. Focus areas of NCS good practice.

List of Partners

Council of Europe (CoE)
Commonwealth Secretariat (ComSec)
Commonwealth Telecommunications Organisation (CTO)
Deloitte
Forum of Incident Response Teams (FIRST)
Geneva Centre for Security Sector Governance (DCAF)
Global Cyber Security Capacity Centre (GCSCC)
Geneva Centre for Security Policy (GCSP)
Global Partners Digital (GPD)
International Criminal Police Organization (Interpol)
International Telecommunication Union (ITU)
Microsoft
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
Potomac Institute for Policy Studies (PIPS)
RAND Europe
The World Bank
United Nations Institute for Disarmament Research (UNIDIR)
United Nations Counter-Terrorism Office (UNOCT)
United Nations University (UNU)

Observers: Axon Partners Group (Axon), Cyber Readiness Institute (CRI), Global Forum on Cyber Expertise (GFCE), Organization of American States (OAS), World Economic Forum (WEF)

Figure 4. List of Partners.

NOTES

1) ITU Global Cybersecurity Index 2018 and 2020 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

TRENDS IN INTERNATIONAL CYBER CAPACITY BUILDING

Written by: Robert Collett, Researcher and Project Consultant on international Cybersecurity Capacity Building

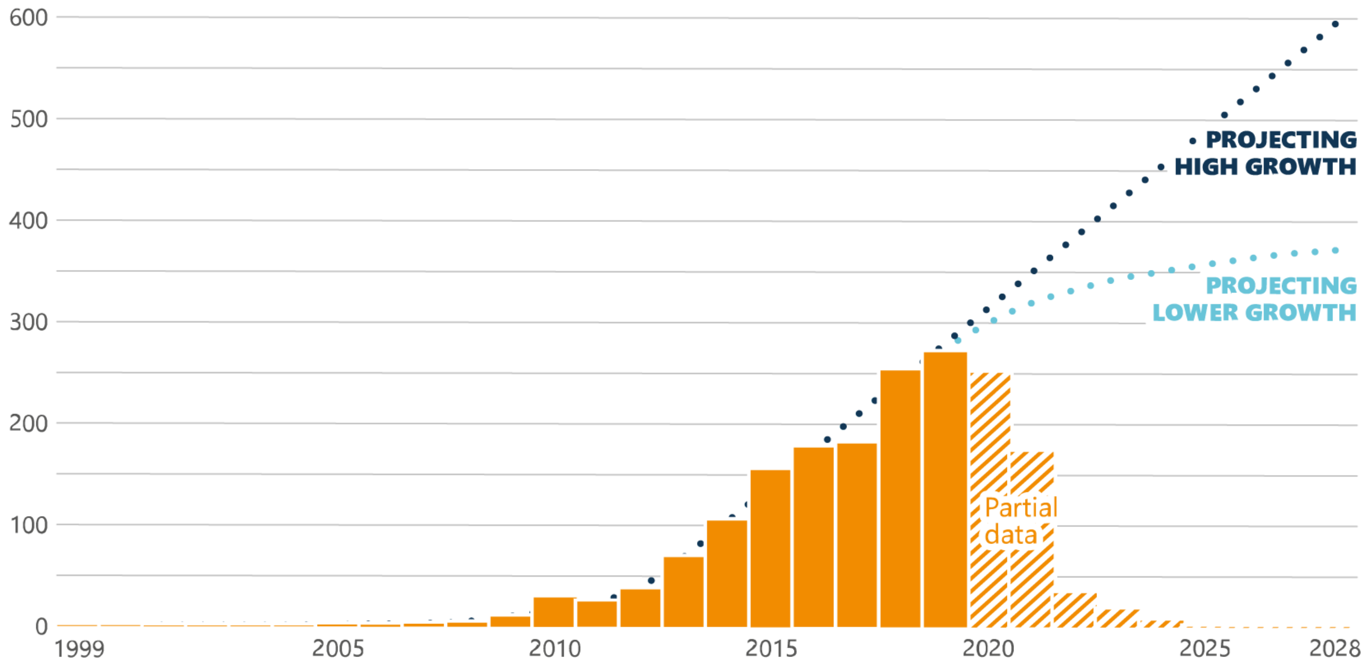
Over two decades, the field of cybersecurity capacity building (CCB) has grown from the first few projects to a busy network of international collaboration with more than 250 projects active each year. The Global Forum on Cyber Expertise (GFCE) community is interested in where this collaboration will go next. To help answer that question, and to inform their own programs, the European Union commissioned a report on global trends and future scenarios in international cyber capacity building. I was pleased to work with my co-author Nayia Barmpaliou and the European Union Institute for Security Studies (EUISS) to publish this report in September. Here I'll share a few of our findings and recommendations.

The first thing to note is that the field of international cyber capacity building has been growing steadily over the past decade. This growth might seem obvious to readers of the Global Cyber Expertise Magazine, but it is worth considering that news of this new form of international cooperation has not reached many outside the cybersecurity capacity building community. Nor has there been an attempt before to estimate the path of its growth. With the help of the information on the Cybil Portal we were able to do just that.

> "The field of international cyber capacity building has been growing steadily over the past decade."

Number of active projects

Per year, 1999-2028



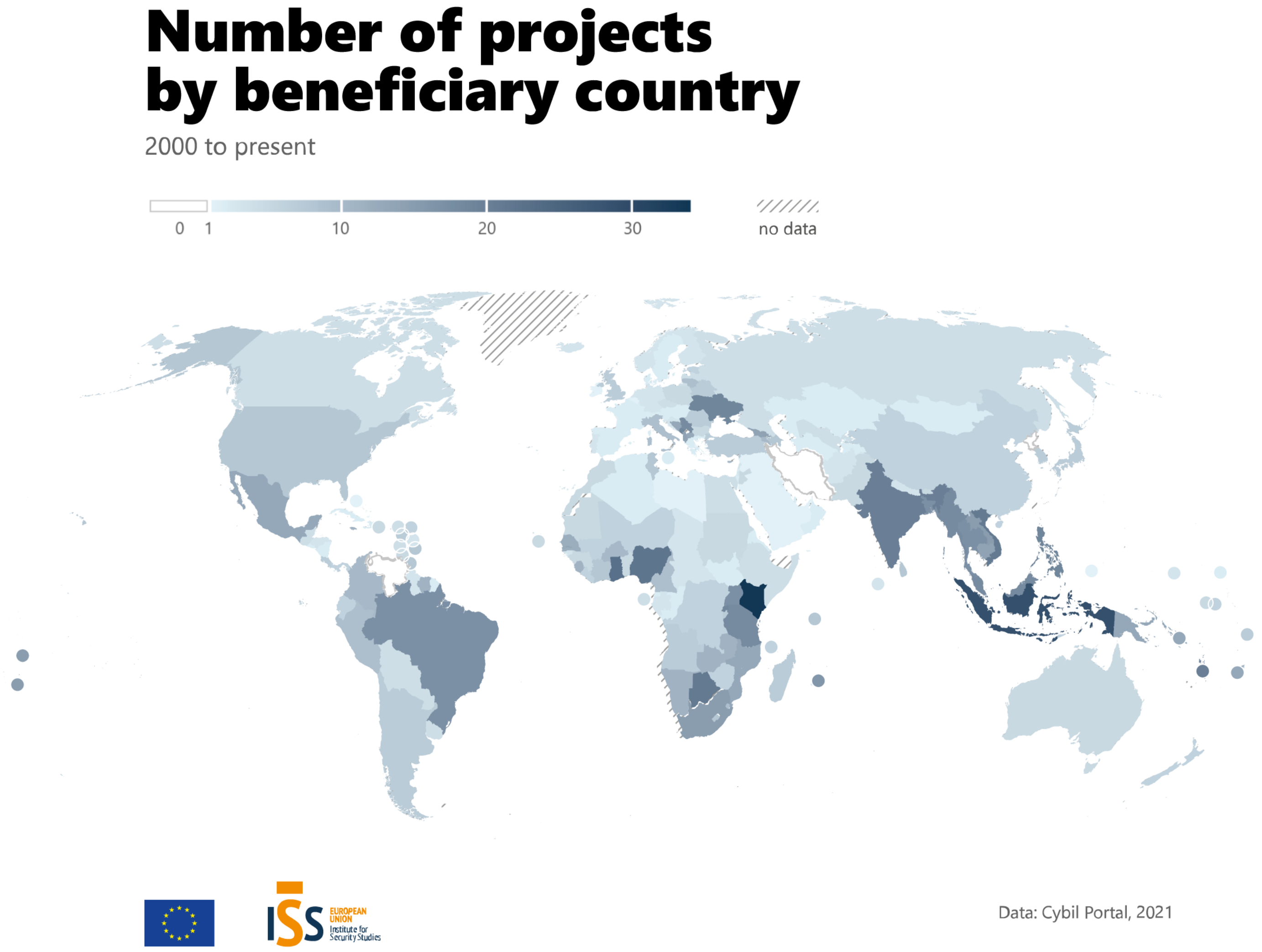
EUROPEAN UNION Institute for Security Studies

Data: Cybil Portal, 2021

Figure 1. Number of active cyber capacity building projects, based on Data from the Cybil Knowledge Portal. Source: Report on International Cyber Capacity Building: Global Trends and Scenarios.

The growth of cyber capacity building leads us to our second observation: the field is an increasingly complex network of organizations and coordination among them will be ever more important. These organizations might be governments, their agencies, companies, universities, international bodies, civil society organizations or regional groupings. They and their projects now connect almost every country with international cyber capacity building. Without coordination, projects will: overload partner government bandwidth; cut across each other; duplicate activity; and leave gaps that a better coordinated approach could fill. We found good examples of coordination occurring in cyber capacity building, but most practitioners we interviewed felt the field's rising aspirations for good coordination were not being matched by the necessary action.

> "The field is an increasingly complex network of organizations and coordination among them will be ever more important."


Number of projects by beneficiary country
2000 to present
0
1
10
20
30
no data
EUROPEAN UNION
Institute for Security Studies

Data: Cybil Portal, 2021

Figure 2. Number of projects by beneficiary country, based on data from the Cybil Knowledge Portal.
Source: Report on International Cyber Capacity Building: Global Trends and Scenarios.

When we trace the field's growth to its roots, we see that the international cyber capacity building is being formed by the coming together of different parent communities. The communities we describe in the report are not an exhaustive or definitive list, but include criminal justice, technical incident response, foreign policy, defense, development cooperation, civil society and the private sector.

Each parent community has its own culture, aims and path into the field of CCB. There is also a wide difference in the degree to which each is integrated into a core cyber capacity building community and participate in the forums such as the GFCE. For example, the foreign policy community was heavily involved in establishing the GFCE out of the Global Conferences on Cyberspace and is still very active. Whereas the development and defense communities are less in such forums and processes. Better connecting cyber capacity building with the development community is something the GFCE hopes to address with its 2022 annual meeting. This will need to be one of several such initiatives to break down the siloes between different communities working in CCB.

> "Better connecting cyber capacity building with the development community is something the GFCE hopes to address with its 2022 Annual Meeting. This will need to be one of several such initiatives to break down the siloes between different communities working in CCB."

Aiming for better coordination is one of the ways in which the field of CCB is professionalizing. The report considers several other signs of professionalization. The average project is tackling more issues. Program teams are expanding and bringing in new staff who specialize in aspects of project management or technical issues such as cybersecurity or economics. There is renewed interest in strengthening evidence-based decision making in CCB, including through a GFCE Research Agenda. There is growing awareness of human rights risks, although program managers worry about whether they have the information and tools to mitigate them. Finally, the approach to delivering projects is shifting from flying international advisors in and out of a country for short visits to other methods, such as: hiring local staff; embedding international staff for longer periods; and remote delivery. The trend towards the professionalization of CCB programming has produced a lot of good practice examples, but it is not yet universal across the field.

In the report, we provide actionable recommendations based on each trend. We also consider potential future scenarios that explore how the path of cyber capacity building could might based on the level of future investment and the quality of coordination. Critically, both high investment and good coordination will be needed to achieve the sort of global cybersecurity and cybercrime capacity improvements that the field is aiming for. We can each help to encourage investment by building the evidence base and case studies that demonstrate the impact of our work. We all have a role to play in improving coordination and knowledge sharing in our day to day work and project design.

The release of the Global Trends and Scenarios report is a prompt to step back and celebrate the creation of a new field of international cooperation, but also a challenge to all of us to contribute to the steps that will be needed to ensure the field continues to grow, and has impact, in the future.

THE GFCE’S DEMAND-DRIVEN APPROACH

Written by: Anna Noij, Advisor, GFCE Secretariat

To fulfill its mission, the GFCE is continuously developing its unique ecosystem, geared towards facilitating the needs of the diverse multi-stakeholder GFCE community and supporting international cooperation on cyber capacity building. As the GFCE continues to grow, it is important that it expands its coordination efforts in line with the need for a demand-driven approach. The GFCE has gained a strong foundation on the supply side of capacity building through the accumulation of best practices, expertise and resources over the years. The challenge today is to tailor expertise and knowledge towards local needs.

The GFCE over the years

During its formative years, the ecosystem of the GFCE evolved in response to what individual Members and Partners had to offer, in addition to considerations of how the GFCE could provide a platform to facilitate these efforts and multiply them on a global level. Throughout this period, the GFCE needed to build a solid foundation of knowledge and resources. Through for example mapping the community’s expertise and encouraging collaboration on GFCE knowledge products in the Working Groups, the GFCE was able to achieve this solid foundation on the supply-side of cyber capacity building.

> “The GFCE needed to build a solid foundation of knowledge and resources.”

GFCE Working Groups

Since 2018, the GFCE Working Groups have been the engine driving the work of the GFCE; it is within these 5 thematic Working Groups that GFCE Members and Partners convene to discuss their cyber capacity building efforts with the aim to coordinate and collaborate. The invaluable expertise of Members and Partners are leveraged for the whole community through showcases and meetings, enabling the dissemination of knowledge and best practices.

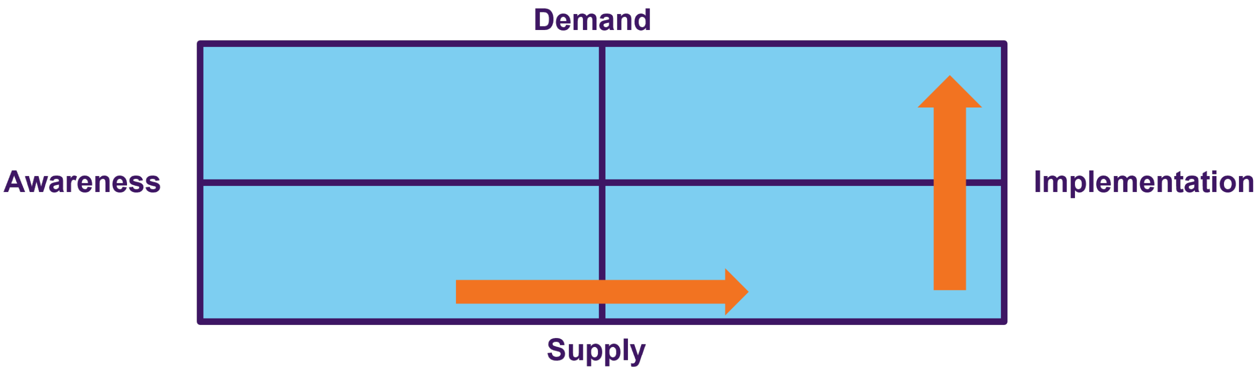


Figure 1. The GFCE's evolving priorities. In 2022, the GFCE will focus on a demand-driven approach, developing upon our past efforts on awareness-raising and implementation on the supply-side.

Moreover, the addition of Partners to the GFCE ecosystem has amplified the community's expertise on implementation, seeing as most GFCE Partners are implementers of cyber capacity building initiatives. This highlights that the growth of the GFCE Working Groups over the years has established a strong stockpile of resources that the community can use in addressing their cyber capacity needs.

GFCE Tools

The growth of the GFCE Working Groups has also initiated the development of other branches of the GFCE ecosystem. Between 2019 and 2020, the GFCE launched three tools to facilitate knowledge-sharing, cooperation and coordination on cyber capacity building. Together, these form the GFCE Toolbox.

As the GFCE community exchanged information and best practices on the five Delhi Communique themes, it became clear that a global instrument to bring together knowledge and expertise through a central resource was needed – a one-stop-shop for cyber capacity building reflecting these five key themes. Thus, in 2018, the idea for a Knowledge Portal was presented to the GFCE community, aimed at making available expertise and knowledge to strengthen cyber capacity building efforts. Recognizing this need, and garnering support from the GFCE Knowledge Partners, the Cybil Knowledge Portal was launched in 2019.

Moreover, in the formative years of the GFCE's evolution, the community had already recognized that cyber capacity building is not a one-size-fits-all model. With this in mind, the GFCE Clearing House was established in 2019, formalizing a process in which the GFCE can play a 'match-making' role through the Working Groups. The Clearing House enables the GFCE to effectively match country, private sector and civil society donors and implementers that can provide key capacity building services to countries that request assistance. Through this process, the GFCE has for example assisted Sierra Leone with their National Cyber Security Strategy, Senegal with setting up a CSIRT (Computer Security Incident Response Team) and their national CIIP framework, and The Gambia with Cybercrime Legislation.

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 research mechanism was introduced in 2020. The GFCE has been collecting and prioritizing these research needs into a Global Cyber Capacity Building Research Agenda, with the first iteration published in 2021. 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.

Looking back at the evolution of the GFCE Toolbox and the GFCE Working Groups, it is clear that the cornerstone of the GFCE has always been the needs of the community. At the same time, as these were the GFCE's formative years, the focus was on understanding what exists, how to avoid duplication and fostering the sharing of expertise and best practices on the supply-side. The accumulation over the years of a strong supply-side foundation has enabled the GFCE to now expand coordination efforts while articulating the need for a more attuned demand-driven approach moving forward.

"The accumulation over the years of a strong supply-side foundation has enabled the GFCE to now expand coordination efforts while articulating the need for a more attuned demand-driven approach moving forward."

Refining the GFCE's Demand-Driven Approach

In 2022, the aim is to strengthening the GFCE's demand-driven approach by focusing on accurately defining needs, stocktaking of the existing supply that the GFCE community has to offer, and addressing gaps to the GFCE community.

This is mainly taking place through the GFCE's regional coordination efforts. The regional coordination meetings throughout 2021 aimed to gain a better understanding of the regional needs. Also the use of the clearing house in these regions can help to identify local needs. As of 2021 , the GFCE has officially established on-the-ground presence in the Pacific, Africa, Europe, Asia, and the Americas; with all continents represented by the GFCE community. In particular, our demand-driven approach and regional focus led the initiation of new collaborative projects in the Pacific and Africa, ensuring that the GFCE supports local capacity by connecting to the local contexts and needs. After identifying the capacity building demands and needs, through conducting mapping and scoping exercises, the GFCE plays a coordination role in bringing them to the community to address, respond and provide support.

An example of regional efforts paving the way for a demand-driven approach is the AU-GFCE Collaboration Project running from 2020-2022. The GFCE, in partnership with the African Union (AU) and with support from the Bill & Melinda Gates Foundation, aims to develop cyber capacity building Knowledge Modules that will enable all African countries to better understand their cyber capacities and identify and address their national cyber capacity needs. After these needs are identified locally, the existing resources offered by the GFCE will be analyzed for any relevant material to help to fill these capacity gaps. Importantly, the project will utilize and build on existing cyber structures, plans, expertise and capacities within the AU and within the multi-stakeholder international GFCE Community, to avoid the duplication of efforts. This will support the strengthening of cyber resilience within African countries and their collaboration with the members and partners of the GFCE community.

Another key project is the GFCE presence in the Pacific, following the GFCE's first Pacific Regional Meeting in February 2020 in Melbourne, in which it was identified that coordination and knowledge sharing was needed among Pacific Island countries, regional donors and project implementers. To facilitate coordination in the region, the GFCE's first Pacific regional liaison was appointed. In order to accurately and locally define the Pacific's cyber capacity building needs, a comprehensive scoping assessment was completed by June 2021. Interviews and consultations with the local community revealed the need to amplify local initiatives across the region, to ensure that donors and implementers understand the local context and existing community leaders in the field. These results highlight the importance of having projects to be demand and locally driven.

"Results highlight the importance of having projects to be demand and locally driven."

Refining the GFCE's Demand-Driven Approach

As the GFCE moves forward with a focus on facilitating the community along a demand-driven approach, certain tools and resources of the GFCE ecosystem will become more central.

Regional projects are projected to become more prominent as they enable scoping and implementation to be completed on a local level. The AU-GFCE Collaboration Project can act as an indicator for the success of the GFCE's regional approach more broadly – this means that the project's success will inform a number of future regional projects. By mid-2022, Knowledge Modules on key cyber capacity building topics will be developed for the region, based on the Project's identified needs in Africa. Building upon this, by the end of 2022 the GFCE aims to develop 'on the shelf' Knowledge modules on key cyber capacity building topics that can be tweaked to address local contexts and needs.

> "Regional projects are projected to become more prominent as they enable scoping and implementation to be completed on a local level."

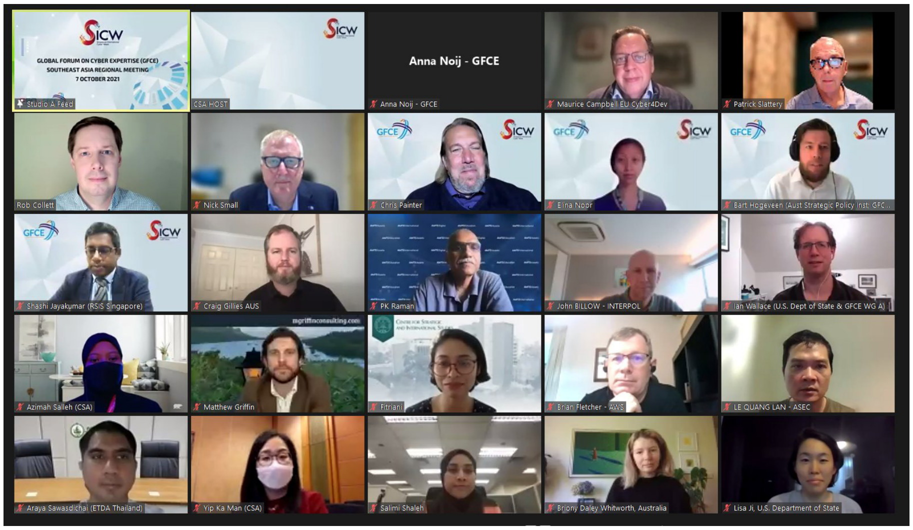

SICW
GLOBAL FORUM ON CYBER EXPERTISE (GFCE)
SOUTHEAST ASIA REGIONAL MEETING
7 OCTOBER 2021
Studio A Feed
CSA HOST
Anna Noij - GFCE
Anna Noij - GFCE
Maurice Campbell EU Cyber4Dev
Patrick Slattery
Rob Collett
Nick Small
Chris Painter
Elina Noor
Bart Hogeveen (Aust Strategic Policy Inst: GFC...
Shashi Jayakumar (RSIS Singapore)
Craig Gillies AUS
PK Raman
John BILLOW - INTERPOL
Ian Wallace (U.S. Dept of State & GFCE WG A)
Azimah Salleh (CSA)
Matthew Griffin
Fitriani
Brian Fletcher - AWS
LE QUANG LAN - ASEC
Araya Sawasdichai (ETDA Thailand)
Yip Ka Man (CSA)
Salimi Shaleh
Briony Daley Whitworth, Australia
Lisa Ji, U.S. Department of State

Figure 2. Participants at the GFCE Southeast Asia Regional Meeting 2021.

Moreover, the GFCE Clearing House, being the GFCE's match-making function, is expected to grow in use in the near future. A Clearing House Coordinator will be appointed to support the community with refining the Clearing House mechanism to articulate a demand-driven approach. The AU-GFCE Collaboration Project has already led to more Clearing House requests as African countries are better understanding their capacity gaps and are in need of being matched to donors and implementers that can assist them in strengthening their cyber capacity. Looking ahead, the Clearing House mechanism is envisioned to be widely recognized by beneficiaries, donors and implementers. As the number of clearing house cases is expected to grow, it would make sense to package them as projects and programs which can receive the necessary support from various stakeholders. In the process, the GFCE will focus on its mandate to make resources available, foster cooperation and provide support in preventing the duplication of efforts.

Interview

MICHELE MARKOFF, ACTING COORDINATOR FOR THE UNITED STATES OFFICE OF THE COORDINATOR FOR CYBER ISSUES

In October 2021, the GFCE Foundation and the U.S. Department of State announced a new partnership, leveraging U.S. funding to increase international and regional coordination on cyber capacity building (CCB) projects that aim to mobilize additional resources and expertise to build global cyber capacities. The partnership has three focus areas: (1) collaboration and coordination within and across GFCE regional projects; (2) development and dissemination of CCB best practices, tools and information that streamline partner nation requests for assistance and influence donor investments; and (3) increased public awareness and political support for CCB projects.

We took time to ask the U.S. Department of State's Acting Coordinator for Cyber Issues, Michele Markoff, about U.S. support for CCB, the GFCE as a global forum for CCB coordination, and predictions for the future.

Q: Why is CCB a priority for the United States?

A: We have seen over the years that CCB has many positive impacts including connecting individuals, increasing access to information, spurring innovation, and driving economic growth. Since the launch of the U.S. International Strategy for Cyberspace in 2011 and subsequent U.S. strategies, we have pursued our vision of an open, interoperable, secure and reliable internet and a stable cyberspace so citizens can benefit from technology, while simultaneously protecting them from the vulnerabilities. By 'open,' we mean an internet that is accessible for all; ‘interoperable’ describes a system of technology that is interlinked and can work together as there are no walls barricading the flow of information that makes the internet what it is; ‘secure’ necessitates that security measures are in place to protect against malicious activities, and ‘reliable’ implies that users can count on and trust the internet and the interconnected digital technologies that make up cyberspace. CCB is foundational to achieving and upholding our vision of the internet and cyberspace.

“CCB is foundational to achieving and upholding our vision of the internet and cyberspace.”

Figure 1. Michele Markoff, Acting Coordinator for the Office of the Coordinator for Cyber Issues.

Q: How have U.S. funding/ investments for CCB changed over the last few years? Any expected trends or forecast for the next few years?

A: It is hard to estimate exactly how much is being spent due to varying definitions of CCB, but there is a general positive trend upwards over the last few years. At the same time, it is difficult to forecast long-term predictions of U.S. funding for CCB; the appropriation by Congress for foreign assistance budgets, including those for CCB, occurs annually, however, we expect the positive trend of increasing U.S. funding for CCB to continue. We also expect to continue to see increased coordination among the U.S. departments and agencies that implement CCB projects.

“We expect the positive trend of increasing U.S. funding for CCB to continue. We also expect to continue to see increased coordination among the U.S. departments and agencies that implement CCB projects.”

Q: Why is the U.S. providing the GFCE with core funding for the benefit of the entire GFCE community?

A: As a founding member, we are supportive of the GFCE's mission and its growth as a forum of stakeholders seeking to uphold the same vision of cyberspace. An important facet for strengthening global CCB is the ability to coordinate efforts, which includes facilitating dialogue and cooperation. The GFCE is doing great work by creating common understandings within the CCB community through the aggregation and dissemination of information, which in turn enables better coordination and cooperation. Acknowledging the time and effort involved, the United States wants to ensure that the GFCE can continue facilitating this coordination role.

Specifically, the GFCE has demonstrated its global leadership in three key areas, earning the support of the United States. Firstly, the GFCE has honed its regional approach since 2021, officially establishing on-the-ground presence in the Pacific, Africa, Europe, Asia, and the Americas, in which the GFCE leverages essential cross-regional information sharing to facilitate CCB at a regional level. Secondly, GFCE has raised the profile of CCB at the highest political levels, increasing public awareness and benefiting the work of the entire community. Thirdly, the GFCE community shares a wealth of knowledge on best practices and expertise and we want to ensure that these are developed and disseminated to the whole CCB community.

> "The GFCE is doing great work by creating common understandings within the CCB community through the aggregation and dissemination of information, which in turn enables better coordination and cooperation."

Q: What is the strategic value of the GFCE in the field of international CCB?

A: The GFCE's strategic value is inherent in its multistakeholder community which enables cross-cutting coordination as opposed to siloed discussions. As a global and neutral platform, the GFCE is well-positioned to collate the invaluable voices of the multistakeholder community working on CCB to achieve our collective vision of an open, interoperable, secure and reliable internet and a stable cyberspace. All 193 UN member states have affirmed that capacity building is essential for international cyber stability so that all states which want to act responsibly in cyberspace have the ability to do so. We also recognize that supporting the GFCE's efforts to strengthen international CCB has a ripple effect on any nation's foreign policy in today's world.

Q: Looking towards the future, what role do you envision for the GFCE regarding regional coordination for CCB? And what is needed to achieve this?

A: Our experience over the past decade has shown that a regional approach to building cyber capacity has numerous benefits. We believe that the global community benefits if the GFCE can tap into those existing networks and relationships; it can only work if the right structures and people are in place to support it. For example, we believe the establishment of the OAS as the GFCE Hub for the Latin America & Caribbean Region provides a unique opportunity to combine the OAS's local knowledge and relationships with the global resources and wider expertise of GFCE. That is why we are bringing the two together through both our funding of the Hub and of a new post within the GFCE Secretariat to support all of the regional Hubs. That's also why we decided to support a new Pacific Hub to combine local knowledge and access to the GFCE's global community of experts and donors.

THE UNTAPPED POTENTIAL OF THE AMERICAS: CYBERSECURITY AWARENESS AND CULTURE

Written by: Gabriela Montes de Oca, Cybersecurity Program Officer, Inter-American Committee against Terrorism (OAS)

The digital revolution and dependence on the use of the internet has accelerated considerably since the beginning of the COVID-19 pandemic. The pandemic has accelerated the reliance on digital avenues to perform daily and essential activities, making society increasingly susceptible to cyberthreats. Latin America and the Caribbean (LAC) is no exception as, according to the Unisys Security Index, since the beginning of the global pandemic, cybercrime has increased by up to 74% in the region. At the same time, the need to create more initiatives around digital literacy and awareness will be exacerbated as more users interact online, evidenced by the high user growth rates across the continent. According to research published by the Economic Commission of Latin America and the Caribbean (ECLAC), in 2019, 66.7% of the region's inhabitants were connected to the Internet. These data points demonstrate that, although digitalization is not reaching all of the LAC region's population equally, cybersecurity threats are rising and awareness should become a priority for governments in the region, as reliance and dependency on them will only continue to increase and the need to protect cyberspace is vital to our prosperity and security, as malicious cyberactivity threatens the functioning of our societies.

National cybersecurity strategies: A first step towards cybersecurity awareness

Within the context of supportive action towards the creation of cybersecurity awareness and culture-building initiatives, a key strategic tool is the national cybersecurity strategy (NCS). Currently, there are 17 countries in Latin America and the Caribbean that have developed a NCS, a number that has grown considerably since 2013. As described by Sadie Creese, Director of the Cybersecurity Capacity Centre of the University of Oxford, countries with improvements in the content or development processes of their NCS have made significant progress in other areas of cybersecurity capacity, which signifies that creating awareness at all levels of government on the need to understand cyber threats has positive results for cybersecurity overall.

Although these strategies provide a wide framework and recognize cybersecurity as a national priority, it is worth noting that some countries in the region have particularly recognized the importance of building a digital culture and developing communication campaigns around their specific objectives and priorities.

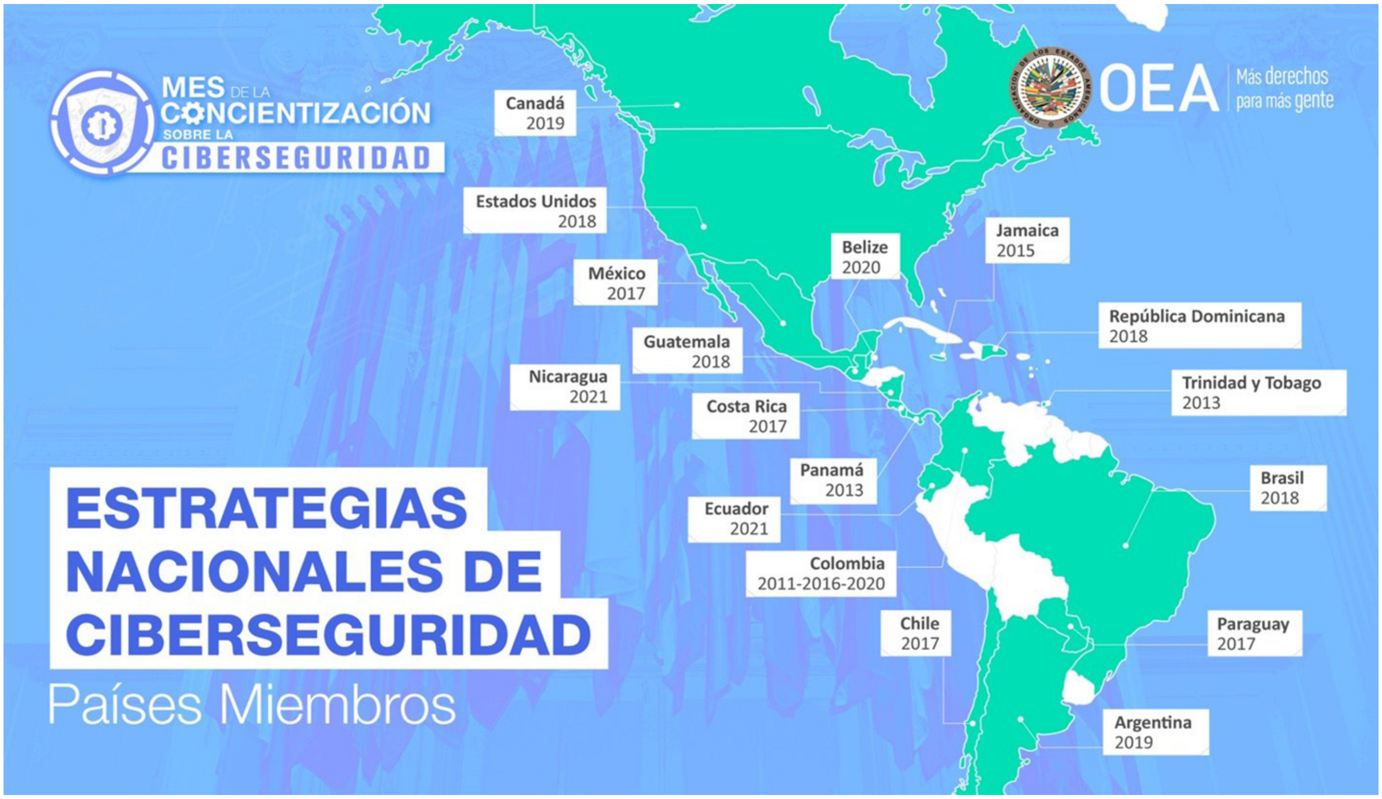


Figure 1: Graphic produced for cybersecurity awareness month that outlines the number of countries in the region with a NCS.

Since 2004, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS) has worked in assisting member states in the development of these policies. From this experience, two examples can be highlighted regarding the importance of creating a cybersecurity culture:

1. During the policy creation process, stakeholder consultations take place in which members of the government, civil society, private sector, and non-governmental organizations are invited to intervene closely and bring their inputs for consideration. This elevates cybersecurity as a shared responsibility, creates awareness around specific issues affecting a country and can help spread the message to each of these sectors' stakeholders.

2. In some cases, awareness-raising activities and initiatives are included in the finalized strategy. As such, countries recognize the importance of creating a cybersecurity culture that encompasses diverse members of the society and outline their responsibilities in safeguarding online security that transcends to non-virtual life.

Case Studies

The following countries recognize and/or mention cybersecurity awareness initiatives as a key pillar of their national cybersecurity strategy.

Colombia

The first objective of Colombia's 2020 National Cybersecurity Strategy is to "Strengthen the trust and digital security of individuals and the Nation, through anticipation and prevention, of the risks identified in cyberspace, generating a cybersecurity culture". An action line within this objective also corresponds to the deployment of a massive prevention campaign in the digital ecosystem, raising awareness of the forms of crime used in the digital environment by cybercriminals, to prevent people from falling victim to these crimes.

Jamaica

This strategy contains a framework divided into 4 pillars - the fourth corresponding to education and awareness. The awareness strategy "seeks to develop targeted campaigns to facilitate each stakeholder group's understanding the potential threats and risks they would likely face." The strategy seeks to build awareness regarding cyber security and develop a culture of cybersecurity.

Paraguay

Paraguay's national cybersecurity strategy mentions awareness through the inclusion of the following objectives:

- Promote initiatives and develop projects to improve the knowledge of IT in the education community.
- Advise and participate in the formulation of national policies related to the use of technologies in education.
- Promote initiatives and develop projects to improve the knowledge of IT in the education community.

National awareness campaigns and initiatives: one step further

In addition to the value added to cybersecurity awareness efforts through a NCS as national policy frameworks, initiatives have also aimed to raise awareness around different cybersecurity issues in Latin America and the Caribbean.

Since 2017, the Cybersecurity Program of the OAS has supported "Cybersecurity Awareness Month", created by the United States' Cybersecurity and Infrastructure Security Agency (CISA). This awareness campaign takes place annually during the month of October. The objective is to raise awareness for cybersecurity issues, as well as build and provide resources to the public to inform citizens and increase their media and digital literacy. Within this campaign, the OAS has organized diverse regional activities such as conferences, webinars, and most recently, due to the COVID-19 pandemic, the creation of social media content to accelerate the dissemination of information around topics such as blockchain technology, online gender violence and social media safety.

The OAS' work in the region has also sparked local initiatives in the region to commemorate cybersecurity during October. For example, in 2018 the Chilean senate convened with academia representatives, members of the armed forces, regional and local representatives, and cybersecurity entities during the first "Cybersecurity international seminar". The objective of this event was "to promote the knowledge and practices of cybersecurity, a discipline that seeks to improve the standards of technology and information security, as well as the need to legislate to protect ourselves as a society from cybercrime". Additionally, the organization of this event coincided with the proclamation of Law 21,113 of Chile, which declares that October is the "National Month of Cybersecurity." Since this first conference, Chile has organized diverse online and in-person events with a strong focus on bringing together diverse stakeholders every October.

In addition to Chile, multiple Mexican government entities have organized "National Cybersecurity Week" every October since 2014. This week aims to raise awareness about the importance of using new information technologies responsibly, through the dissemination of preventive content about cybersecurity risks, to reduce the number of incidences caused by digital illicit behaviors and promote the reporting of cybercrime. Although federal government entities have organized this initiative in the past, in 2019 the Mexican Senate declared the first week of October as the "National Cybersecurity Week" to "raise awareness among citizens about the risks of using cyberspace and the culture of prevention in the face of the advancement and scope of information and communication technologies (ICT), and to provide greater protection and security to users of the cybernetic devices." During the discussions, senators recognized the importance of awareness initiatives on a country's broader cybersecurity resilience, as well as the impact that these proposals have had in other countries that have adopted them.

Apart from these collaborative efforts during October, OAS member states have also developed specific, innovative campaigns around topics of their citizens and governments' interest through alliances with other organizations.

Cybertips for a new
CYBERSECURITY AWARENESS MONTH
CHILDREN AND ADOLESCENTS

If you are responsible for an SME, *Risk Management* is your ally to address Cybersecurity!

Make sure to identify all your valuable assets.

Evaluate the vulnerabilities and threats that affect those assets.

Establishes a Treatment Plan and measures the results obtained.

Don´t forget! Risks are dynamics, repeat these three steps periodically!

CSIRTAmericas Network

Figure 2: Graphic content produced by the CSIRT Americas network for the 2021 Cybersecurity Awareness Month joint campaign.

For instance, STOP.THINK.CONNECT is a global online safety awareness campaign aimed at providing the public and digital citizens with specific tools to stay safer and more secure online. It was created in 2010 by the STOP.THINK.CONNECT Messaging Convention in partnership with the U.S. government. Since its launch, other countries in LAC such as Argentina, Colombia and Panama, have adopted the campaign, adapting its messaging to their specific contexts.

Additionally, the development of Get Safe Online's Caribbean-based campaigns, for instance, tackle topics such as remittances, online children safety and online scams through social media safety, which are particular to the Caribbean. Most recently, the CSIRTAmericas network of the OAS released a joint awareness campaign with digital security topics for diverse publics and counted with the simultaneous support and visibility of Argentina, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, Jamaica, Panama, Paraguay, and United States.

> "Although each country has a unique challenge to advance its cybersecurity culture, the region shares the commonality of the need to increase cybersecurity to optimize the benefits of the Internet usage."

Looking ahead: a shared purpose of cybersecurity awareness

Although progress has been made, areas of opportunity remain especially as a larger number of citizens of the LAC region have Internet access through different devices and subsequently rely on digital solutions to conduct their daily lives. The examples shown above demonstrate the wide interest of the region in providing solutions and educational materials on the current threats affecting our cybersecurity landscape, as well as the key role that awareness can play in elevating cybersecurity as a national priority.

As countries advance digitally, awareness initiatives through national cybersecurity strategy policies and other awareness efforts are strategic steps towards cybersecurity resilience and maturity. Diversity and multiculturalism are factors that have always characterized our region. These characteristics mirror the variety of cybersecurity maturity levels in the region in the case-by-case country. Although each country has a unique challenge to advance its cybersecurity culture, the region shares the commonality of the need to increase cybersecurity to optimize the benefits of the Internet usage.

A REGIONAL VIEW FROM THE AMERICAS THROUGH CYBER CONFIDENCE-BUILDING MEASURES

Written by: G. Isaac Morales Tenorio, Coordinator for Multidimensional Security, Ministry of Foreign Affairs of Mexico

This article presents how recent UN processes have recognized and encouraged the role of regional organizations and forums to contribute to advancing responsible state behavior in cyberspace. By highlighting the creation and work of the OAS Working Group on CBMs, this article aims to present the performance of a regional view on cybersecurity from the Americas. With the identification of three relevant elements for the way forward, the text analyzes how the efforts to implement the CBMs and other commitments regionally will open windows of opportunity to enhance capacity-building programs and improve engagement in multi-stakeholder platforms such as the GFCE.

In the last months, despite the challenges posed globally by the COVID-19 pandemic, very positive cyber news came from the United Nations with the adoption by consensus of the final reports of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security as well as the Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace.

These processes consolidated a common ground to better address malicious, hostile and unlawful uses of cyberspace and digital technologies. They have set the tone for international cooperation and reaffirm multilateralism as an effective platform to put cyber-diplomacy into practice.

Through these reports, the international community has reaffirmed the applicability of international law in cyberspace, identified threats and challenges, decided to jointly advance on the implementation of the non-binding norms for responsible state behavior, developed a robust vision on the relevance of the confidence building measures, and adopted comprehensive commitments to encourage more cooperation and capacity-building programs.

One significant element not sufficiently touched upon yet is UN recognition of the important role that regional organizations and forums have played and will continue to play in implementing commitments reached by multilateral fora and facilitating cyber cooperation, confidence and capacity-building initiatives.

Step by step, in the Americas, a more formal and continuous dialogue on cyberspace has been consolidated. Particularly due to the work of the Organization of American States (OAS), we have seen an increasing relevance of discussions related to cybersecurity, the applicability of international law and cyberspace governance. These discussions are aimed at implementing international commitments in addition to identifying common understandings and concerns to facilitate a regional approach. It should be pointed out that the relevance of such a regional approach is referenced in Chapter Eight of the UN Charter.

From its 2010 report, the UN GGE recommended further steps for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions. Cyber Confidence-Building Measures (CBMs), defined so far by the GGE reports, could be considered precursors of political will and commitment to the collective endorsement and implementation of the voluntary norms of responsible state behavior in cyberspace.

Taking into account the recommendations of the GGE and addressing the need to increase cooperation, transparency, predictability and stability among States and their activities in cyberspace, Member States of the OAS decided in 2017 to create a Working Group on Cooperation and Confidence-Building Measures in Cyberspace within the framework of the Inter-American Committee against Terrorism (CICTE).

Figure 1. Mexico was elected as Chair of the Working Group.

> “Member States of the OAS decided in 2017 to create a Working Group on Cooperation and Confidence-Building Measures in Cyberspace within the framework of the Inter-American Committee against Terrorism (CICTE).”

During the first meeting of the Working Group held from February 28 to March 1, 2018, two initial CBMs were adopted. These two initial CBMs led the region to have a more formal and structural discussion on cybersecurity issues by sharing information on national policies, strategies and general frameworks on cybersecurity, as well as designating national focal points.

The UN and OAS have developed many crucial experiences with CBMs and international security issues which have seen both successes and failures. Moving forward, it has been instrumental to bring these experiences to the realm of CBMs in cyberspace as they perhaps can effectively contribute to ensure CBMs are used peacefully and to prevent conflict.

Figure 2. Second meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace, in 2019.

Confidence-building is a gradual process and even though the developments in cyberspace are fast-paced, it has been shown that significant progress needs to be achieved on a step-by-step basis to identify, with the greatest possible degree of clarity, all those factors which could adversely affect mutual trust in a given situation.

In the second meeting of the Working Group held in April 2019, more participants from other international organizations, academia and civil society were involved. As a result of the meeting, four more CBMs were adopted leading to the addition of a list of “non-traditional” measures to the OAS general list of CBMs.

Learning from our experience in the Americas, it is important to maintain a more comprehensive reading of the whole picture, where CBMs in cyberspace are linked to the norms of responsible state behavior, international law, and capacity-building. With this view, the third and last meeting of the Working Group, held virtually in July 2021, allowed OAS Member States to reaffirm their common interest in advancing regional dialogues, sharing experiences and implementing regional commitments by engaging with more international discussions.

> "It is important to maintain a more comprehensive reading of the whole picture, where CBMs in cyberspace are linked to the norms of responsible state behavior, international law, and capacity-building."

In this last meeting, Mexico was elected as Chair of the Working Group. Together, with the United States as Vice-Chair and the CICTE's Secretariat clearly committed to supports the efforts carried by the Working Group, we will have the opportunity to further advance a regional approach on these core issues along at least three lines:

1) CBMs are clear expressions of international cooperation and so by identifying national good practices, challenges or gaps when trying to implement them, we will have the opportunity to support action-oriented capacity-building and technical assistance projects within the OAS Cybersecurity program and far beyond, taking advantage of the engagement to multi-stakeholder platforms such as the GFCE.

2) The Working Group on CBMs gives Member States the chance to enhance efforts to implementing the UN framework and recommendations of the GGE and the OEWG. But also, as a two-way avenue, it allows Member States to individually put on the table concerns and challenges as well as concrete experiences which, once considered of regional interest, could be elevated to the current and future UN processes as regional inputs. By doing so, we will be able to generate greater awareness and understanding of the evolving cybersecurity concerns of all States, and continue to implement appropriate action, as well as identify new measures of deeper cooperation aimed at addressing these and any new concerns.

3) Further advancing collaboration with other relevant stakeholders and increasing inter-regional and inter-organizational dialogue will be also a way forward for the Working Group. Considering these issues from the scope of international security, keeping in mind the promotion and protection of fundamental human rights, the possibilities given by cyberspace for sustainable development, and the fulfillment of those principles of sovereignty, non-intervention, equality, peaceful settlement of disputes and international cooperation, the OAS Working Group will benefit from promoting the sharing of experiences with other regions and organizations, as well as considering the advancements and contributions of the multi-stakeholder community, particularly on the implementation of Confidence Building Measures.

EUROPEAN CYBER AGORA: LEVERAGING CROSS-SECTORAL COLLABORATION DURING THE IMPLEMENTATION PROCESS OF THE NEW EU CYBERSECURITY STRATEGY

Written by: Nikolas Ott, Project Manager – Cybersecurity and Digital Diplomacy, European Governmental Affairs, Microsoft and Kezia Wexoe-Mikkelsen, Coordinator – Cybersecurity and Digital Diplomacy, European Governmental Affairs, Microsoft

This article provides an overview of the European Cyber Agora. The European Cyber Agora is an initiative launched by the German Marshall Fund, the European Union Institute for Security Studies' Cyber Direct Programme and Microsoft to provide a platform for European multistakeholder discussions on cybersecurity policy. It builds on the EU Cybersecurity Strategy that promotes a more inclusive dialogue with more regular and structured multistakeholder engagement to develop and implement a coherent and holistic cyber policy. The first European Cyber Agora was held on the 2-3 of June 2021 and led to the creation of four working streams, which will focus on various themes and are designed to further support the implementation efforts around the EU Cybersecurity Strategy.

Figure 1. The European Cyber Agora banner.

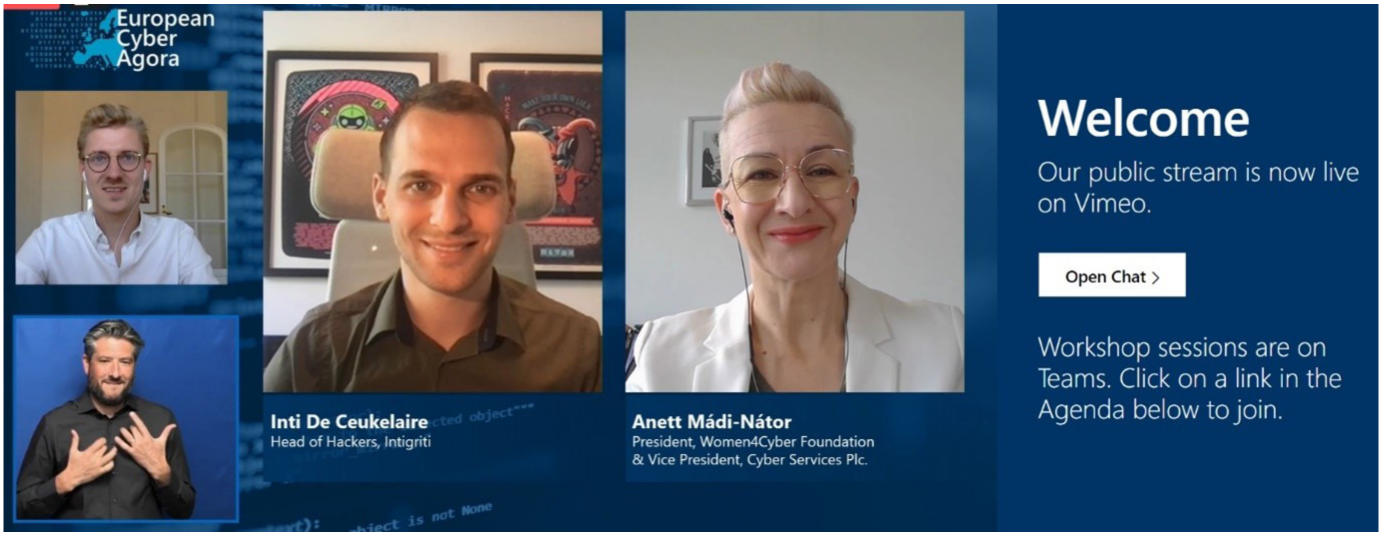
In December 2020 the European Union (EU) published its Cybersecurity Strategy for the Digital Decade. The document outlined an ambitious roadmap for the Union, including on cyber diplomacy issues, capacity building, cyber sanctions, applicability of international law in cyberspace and the development of a Program of Action on cyber norms in the UN. The strategy's implementation, especially its sections on standardization, cyber capacity building and internet governance rely on input from non-governmental stakeholders.

For this reason, together with key stakeholders in the cybersecurity domain such as The German Marshall Fund (GMF) and the EU Institute for Security Studies (EU ISS) Cyber Direct Programme, Microsoft launched a new multistakeholder initiative to advance European perspectives on global cybersecurity policy debates. The European Cyber Agora is designed as a forum for providing multistakeholder guidance and cooperation on EU cybersecurity policy issues through structured exchanges between EU institutions, EU Member States, the private sector, academia, and civil society, with the aim of strengthening the collective EU vision of cyberspace globally. The European Cyber Agora is managed in collaboration with our implementing partners the European Union Cyber Direct Program and the German Marshall Fund of the United States and many other partners across Europe supported the first Agora conference in June.

The European Cyber Agora builds on the objectives of the EU Cybersecurity Strategy, released in December last year, which sets out ambitious plans for the EU and its Member States to advance technical cooperation, crisis management, security standards, cyber diplomacy, capacity building and, in particular, multistakeholderism. This was echoed in the EU Council Conclusions on EU's Cybersecurity Strategy for the Digital Decade, which specifically addressed the goal of this initiative:

"[The Council of the European Union] STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and cybersecurity and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society in international fora, including within the context of the Paris Call for Trust and Security in Cyberspace."

Figure 2. Casper Klynge, the Vice President of European Government Affairs Microsoft, delivers a virtual keynote during the European Cyber Agora.



Inti De Ceukelaire
Head of Hackers, Intigriti

Anett Mádi-Nátor
President, Women4Cyber Foundation
& Vice President, Cyber Services Plc.

Welcome

Our public stream is now live on Vimeo.

Workshop sessions are on Teams. Click on a link in the Agenda below to join.

Figure 3. Panelists during the session 'Agora Talk: The Future of European Cyberspace' on Day 1 of the Cyber Agora.

The European Cyber Agora's main goal is to provide a platform for these regular and structured stakeholder exchanges. With a vibrant community of civil society organizations and vast cybersecurity expertise across universities, think thanks, and industry, Europe has a lot to gain from formalizing a framework for these interactions. This is the first initiative of its kind specifically dedicated to European multistakeholder discussions on cybersecurity. Globally, cybersecurity issues are discussed at the Internet Governance Forum (IGF), the United Nations, the Global Forum on Cyber Expertise (GFCE), but Europe has an opportunity to find new ways to convene and channel more stakeholder voices back into global fora. The European Cyber Agora will aim to bridge this gap and help to advance European positions on the global stage.

> "[The] nongovernmental sector is a valuable resource for policymakers; now is the time to harness this resource in Europe and work together to promote our values globally."
>
> *- Wiktor Staniecki, Deputy Head of Division, Security and Defense Policy Division, European External Action Service (EEAS).*

The first European Cyber Agora met for an online event on June 2-3, 2021. The event featured workshops on topics such as International Cyber Capacity Building, European perspectives on the protection of the health care sector from cyber-attacks and European views on emerging technologies, in the hope of producing tangible guidelines to support the implementation of the EU Cybersecurity Strategy. This resulted in a first report recently published by the German Marshall Fund. The report summarizes key take-aways and outlines how we plan to move the European Cyber Agora forward.

What is the next step?

The discussions during the Agora conference highlighted that a regular and structured exchanges between stakeholders are central to tackle the increasing cybersecurity challenges in Europe. The implementing partners therefore decided to launch dedicated workstreams to work on tangible outcomes within four different thematic areas. The results of these discussions will be presented during the next Agora conference in 2022. If you are interested in contributing to the discussions within one of the workstreams, you can do so very easily. Participation is open to anyone and everyone, also experts based in non-European countries are warmly welcome. The four different workstreams created are:

1. Enhancing cross-sectorial lines of communication

We aim to strengthen the linkages between European cyber policy and non-governmental sectors. As a first step, we plan to conduct a mapping exercise across Europe to identify relevant stakeholders. As a second step, we plan to connect the different stakeholders across Europe among themselves and with EU institutions.

2. Supporting civil society's engagement and improve its preparedness

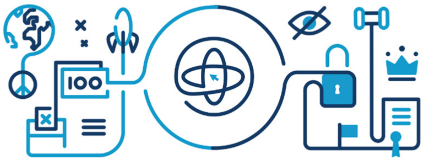
Non-governmental stakeholders are engaged in many ways of strengthening our societies, but sometimes these efforts are not sufficiently appreciated or acknowledged. The aim of this workstream is to link cyber policy goals to related non-governmental efforts that strengthen bottom-up responses to cyberattacks and create more awareness around how to benefit more effectively of non-governmental expertise.

3. Increasing operational capacity to prevent, deter and respond

We aim to develop ideas and suggestions on how to improve the efficiency of the EU Cyber Diplomacy Toolbox by strengthening preventive cybersecurity initiatives and supplement these efforts with non-governmental efforts.

4. Advancing global and open cyberspace

Resolving the conundrum between EU commitments to open cyberspace and calls for strategic autonomy and technological sovereignty shall take center stage within this workstream. Moreover, we will aim to work toward strengthening a credible narrative to convince other countries of the benefits of a democratic cyberspace, and the threat of a splintered Internet.



Conclusion

The road toward the next European Cyber Agora conference is filled with ambition and excitement. We encourage all of you to consider joining the European Cyber Agora community - a group of experts from Europe and beyond and the ambition to meaningfully support the implementation of the new EU Cybersecurity Strategy. If you are curious to learn more about the benefits of this model, then do not hesitate to reach out to us via EuropeanCyberAgora@microsoft.com.

WHAT ROLE CAN EUROPEAN UNIVERSITIES PLAY IN CYBER CAPACITY BUILDING?

Written by: Dr Joe Burton (Universite libre de Bruxelles) and Professor George Christou (University of Warwick), Coordinators of CYDIPLO – European Cyber Diplomacy cyberdiplomacy.net, supported by the Erasmus + Mechanism of the EU

Universities in Europe have an important role to play in cyber security capacity building, not least through developing skills and talent pipelines and providing rigorous research to inform effective cyber security policy. But there are many challenges for the university sector, too. In this article, Dr Joe Burton and Professor George Christou reflect on these challenges and suggest how European universities can further develop their international engagement and impact in cyber security education and training.

The higher education sector in Europe is well placed to play an active role in cyber security capacity building. But there are also numerous challenges, including the need to resource university cyber security programs adequately, the challenge of creating clear career pathways for university students, the need to build genuinely multidisciplinary cyber security education, and the ongoing pressure on university budgets created by the pandemic and corresponding fall in international tuition fee revenue.

What is the next step?

The CYDIPLO consortium, which we coordinate, is playing an active role in this area. We are a group of 5 European universities (University of Warwick, Leiden University, Universite libre de Bruxelles,

Figure 1. CYDIPLO's logo. CYDIPLO is a consortium of seven universities seeking to build cyber capacity through research and training.

University of Bologna, Tallinn University of Technology) and two universities from the Asia Pacific – International Christian University (Japan) and University of Waikato (New Zealand). The goal of the program is to help professionalize cyber diplomacy by creating new educational resources including research publications such as a Handbook on Cyber Diplomacy, which we hope will become an active tool for those that practice cyber diplomacy, as well as teaching and training programs, including workshops and a Massive Open Online Course (MOOC).

The CYDIPLO program is illustrative of the sort of provision that we think is needed in order for universities to build cyber capacity. First, it needs to be genuinely interdisciplinary (researchers involved are from law, computer science, political science, security studies, international relations and European studies). Second, it needs to reach across world regions and build connections between them – this is why we are actively cooperating with universities centered in the Indo-Pacific region and connecting and collaborating with projects (such as EU Cyber Direct) that reach out to academics in Latin America, Africa and North America. Universities also need to recognize the different needs of their audiences. Universities can provide a pipeline from the undergraduate to postgraduate levels that seeks to fill the widely acknowledged skills gap in the cyber security sectors (both in the technical and more policy-oriented fields). Thirdly, the way we build capacity needs to reflect contemporary pedagogy and teaching practices, including producing first class online provisions. This is critical if we are to address the constraints on travel related to the pandemic, but also to level the playing field, so that those from less developed countries wanting to upskill in cyber security can do so without having to move to Europe or face the often unaffordable tuition fees. Online teaching will play an important role in future cyber security provision. It also needs to be innovative in order to achieve what we all want to see, which is the skills gap closing, and graduates emerging from cyber security with a diverse blend of knowledge and skills so that they are well equipped to cope with a complex, diverse, and constantly changing environment of cyber (in) security. In this respect, developing programs which put students in real world situations, such as online scenarios or simulations, will play an important role.

Finally, cyber capacity building needs to be underpinned by excellent and rigorous research. This is where the universities can really play a role in making capacity building more effective, more targeted at priorities, and more mindful of the political and social challenges involved.

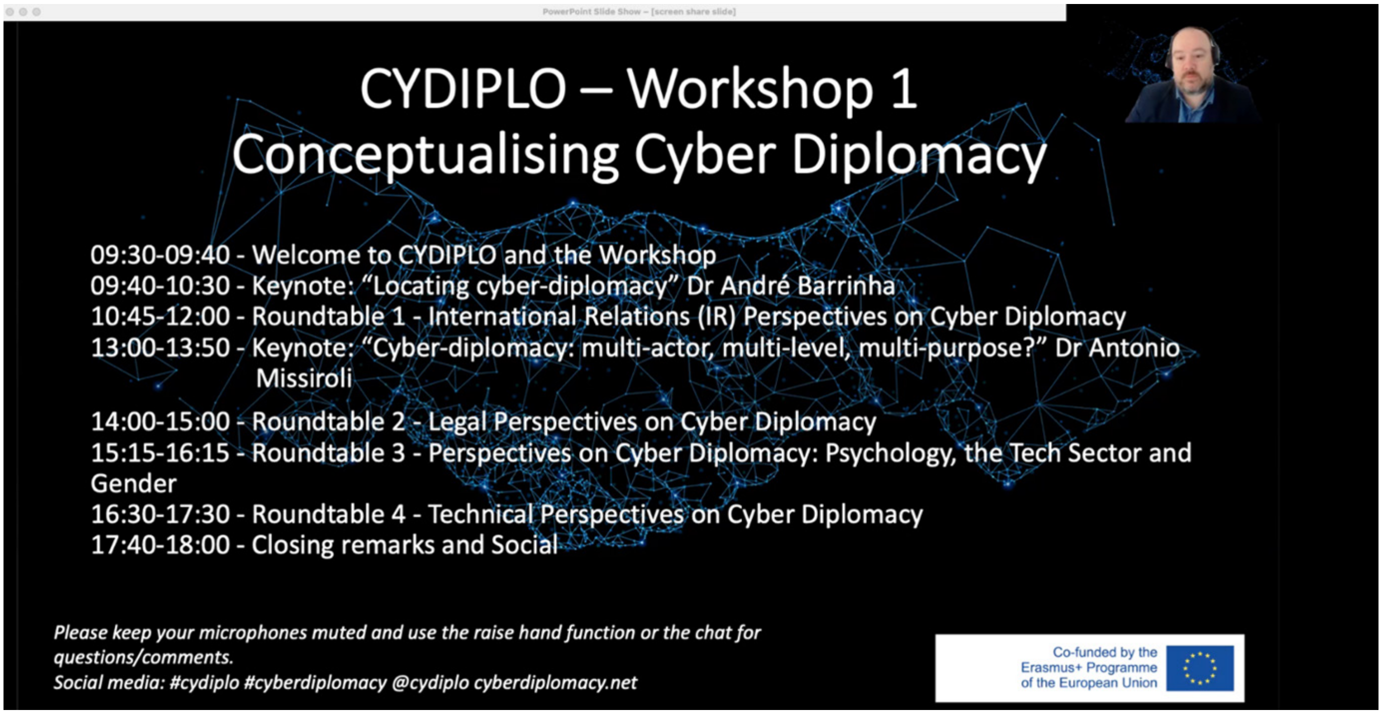
> “Cyber capacity building needs to be underpinned by excellent and rigorous research.”

Universities – Moving Beyond the Ivory Tower

So how can the GFCE community move forward in developing stronger links with the university sector (and vice versa)?

First, while there are already some close connections in place, which is a great start, the GFCE could be more proactive in building sustainable links with the university leadership in Europe and beyond. This could involve reaching out to the Vice Chancellors of European universities and running forums and workshops to engage them in the need to develop cyber security professionals. This needs to reflect the need for clear educational pathways – those who might be interested in enrolling in cyber security degrees need to know what the opportunities will be when they have completed their training and how rich, rewarding and diverse a career in cyber can be. Getting university senior management on side is an important step to greater collaboration and connecting with the European Universities Initiative (the aim of which is to bring together a new generation of creative Europeans able to cooperate across languages, borders and disciplines to address societal challenges and skills shortages faced in Europe) funded by the European Commission would be a practical place to start any such endeavor.

Second, and in recognition that cyber security education needs to be comprehensive,



CYDIPLO – Workshop 1
Conceptualising Cyber Diplomacy

09:30-09:40 - Welcome to CYDIPLO and the Workshop
09:40-10:30 - Keynote: “Locating cyber-diplomacy” Dr André Barrinha
10:45-12:00 - Roundtable 1 - International Relations (IR) Perspectives on Cyber Diplomacy
13:00-13:50 - Keynote: “Cyber-diplomacy: multi-actor, multi-level, multi-purpose?” Dr Antonio Missiroli
14:00-15:00 - Roundtable 2 - Legal Perspectives on Cyber Diplomacy
15:15-16:15 - Roundtable 3 - Perspectives on Cyber Diplomacy: Psychology, the Tech Sector and Gender
16:30-17:30 - Roundtable 4 - Technical Perspectives on Cyber Diplomacy
17:40-18:00 - Closing remarks and Social

Please keep your microphones muted and use the raise hand function or the chat for questions/comments.
Social media: #cydiplo #cyberdiplomacy @cydiplo cyberdiplomacy.net

Co-funded by the Erasmus+ Programme of the European Union

Figure 2. CYDIPLO held its first workshop on conceptualizing cyber diplomacy online on 25 – 26 March 2021.

more work could be done to engage schools and those seeking to reskill later in their career to transition into a cyber security role. Universities naturally focus on undergraduate provision, but there are enormous opportunities for universities to get more involved in continuous education, executive training, and lifelong learning. People are never too old, or indeed too young, to develop cyber security skills. One good example of earlier years' provision is the New Zealand Cyber Security Challenge, run at University of Waikato for the last 10 years. This provides a platform for senior high school students to compete in red team and blue team challenges, enabling the university and indeed potential employers to identify and support promising cyber professionals at an early age. These kinds of efforts could be replicated throughout Europe if the will and resources were there.

Third, there needs to be closer cooperation between international organizations, civil society and universities in this area. There are some promising signs already here. The European Security and Defence College, for example, coordinates a network of education providers in the area of cyber security, and allows universities and academics to build contacts with EU and national officials. ENISA also provides the Cybersecurity Higher Education Database (CyberHEAD), the largest validated cybersecurity higher education database in the EU and EFTA countries, the purpose of which is to provide a point of reference for all citizens looking to upskill their knowledge in the cybersecurity field. This is a good start, but universities can and need to be further engaged with EU agencies and national agencies in identifying and meeting the needs of the modern cyber workforce. EU Cyber Direct and EU Cyber Net are also prominent organizations involved in connecting researchers, universities and policymakers. The NGO and INGO sector is another pathway for greater engagement. Universities could be better represented in a number of key organizations with a role in cyber security.

"Universities can and need to be further engaged with EU agencies and national agencies in identifying and meeting the needs of the modern cyber workforce."

Universities are very much connected to the digital needs and realities of modern societies. In Europe, opening up and facilitating greater academic engagement in developing cyber security policy and skills provides an opportunity to enhance its role and make a strong and innovative contribution to building cyber capacity in Europe and beyond.

AU-GFCE COLLABORATION PROJECT: ENABLING AFRICAN COUNTRIES TO IDENTIFY AND ADDRESS THEIR CYBER CAPACITY NEEDS

Written by: Dr Martin Koyabe, Senior Manager, AU-GFCE Collaboration Project

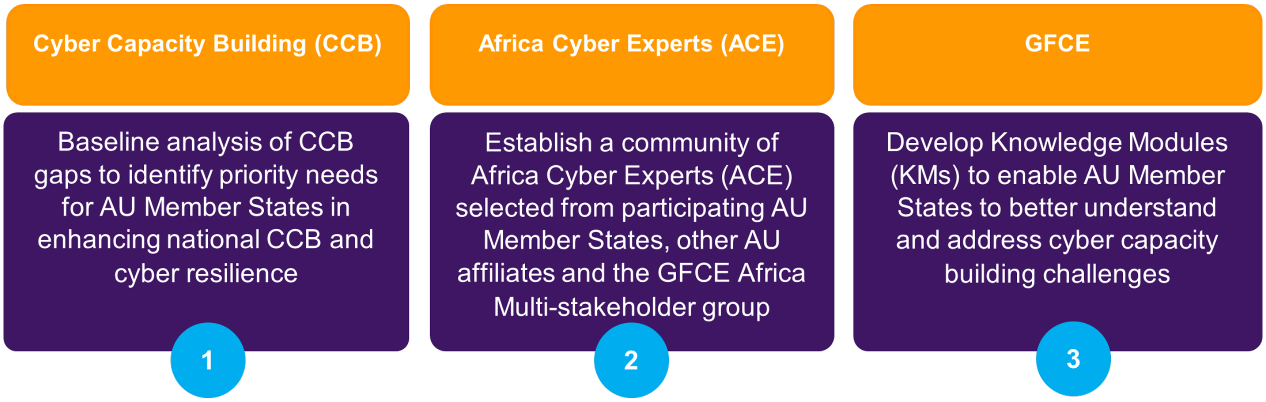
Since its formation in 2015, the GFCE has continued to strengthen cyber capacity and expertise globally by being a pragmatic, action-orientated and flexible platform for international collaboration. Since its formation in 2015, the GFCE has continued to strengthen international cooperation on Cyber Capacity Building (CCB) by connecting needs, resources and expertise and by making practical knowledge available to the global community. The importance of CCB is increasingly being acknowledged globally various key stakeholders including: governments, international organizations, civil society, private and public sector players. However, most CCB efforts are still often underpinned by misconceptions about the processes, involvement and respective responsibilities of main actors. This is exacerbated by the inability to differentiate between global CCB efforts towards cybersecurity, cyber crime or cyber defense. This article highlights the current status and progress of the AU-GFCE Collaboration, and in particular provides a brief on the development of the key objectives of the project.

On-going African Union (AU) and GFCE Collaboration

The GFCE has partnered with the African Union (AU) to develop cyber capacity building knowledge to enable AU member states to better understand cyber capacities and offer support in strengthening their cyber resilience with support from the Bill & Melinda Gates Foundation.

The AU-GFCE collaboration project aims to deliver three main outcomes (see Figure 1):

1. Cyber Capacity Building (CCB) Needs – conduct a baseline analysis of CCB gaps to identify priority needs for AU Member States in enhancing their national CCB and cyber resilience.
2. Africa Cyber Experts (ACE) Community - Establish a community of Africa Cyber Experts (ACE) selected from participating AU Member States and other AU affiliate and GFCE Africa Multi-stakeholder group.
3. GFCE Knowledge Modules - Develop Knowledge Modules (KMs) to enable AU Member States to better understand and address cyber capacity building challenges


Cyber Capacity Building (CCB)

Baseline analysis of CCB gaps to identify priority needs for AU Member States in enhancing national CCB and cyber resilience

1

Africa Cyber Experts (ACE)

Establish a community of Africa Cyber Experts (ACE) selected from participating AU Member States, other AU affiliates and the GFCE Africa Multi-stakeholder group

2

GFCE

Develop Knowledge Modules (KMs) to enable AU Member States to better understand and address cyber capacity building challenges

3

Figure 1. Key Deliverables of the AU-GFCE Collaboration Project.

Cyber Capacity Building (CCB) Needs Analysis

During the initial stages of the AU-GFCE project, we conducted desktop research analysis of the CCB needs of all AU member states. The analysis took into consideration publicly available data sources to provide metrics for assessing the status of CCB in AU member states (see Figure 2). The data sources considered include: Cybersecurity Maturity Model (CMM) (GCSCC); Global Cybersecurity Index (GCI) (ITU); National Cyber Security Index (NCSI) (e-GA); National Cybersecurity Assessment (AUDA-NEPAD) (AU Development Agency) and Luxemburg CERT Assessment (AU).

Our analysis[1] showed most AU member states are progressing incrementally in enhancing Cyber Capacity in terms of awareness and skills alongside Legal and Legislation frameworks at national level. National Cyber Security (NCS) development, Assessments, Cyber Diplomacy, Awareness and CNIP/CIIP remain among the focus areas to be addressed by most AU member states.

Based on this knowledge, further engagement was sought with AU member states to validate the finding and highlight CCB priority needs for AU member countries. These priority needs are currently being categorized as input for development of relevant Knowledge Modules. The Knowledge Modules aim to enhance the understanding of CCB,supporting AU member states in strengthening their national cyber resilience. In addition, the AU-GFCE project will continue updating the CCB status for AU member states, whenever additional information or data becomes available.

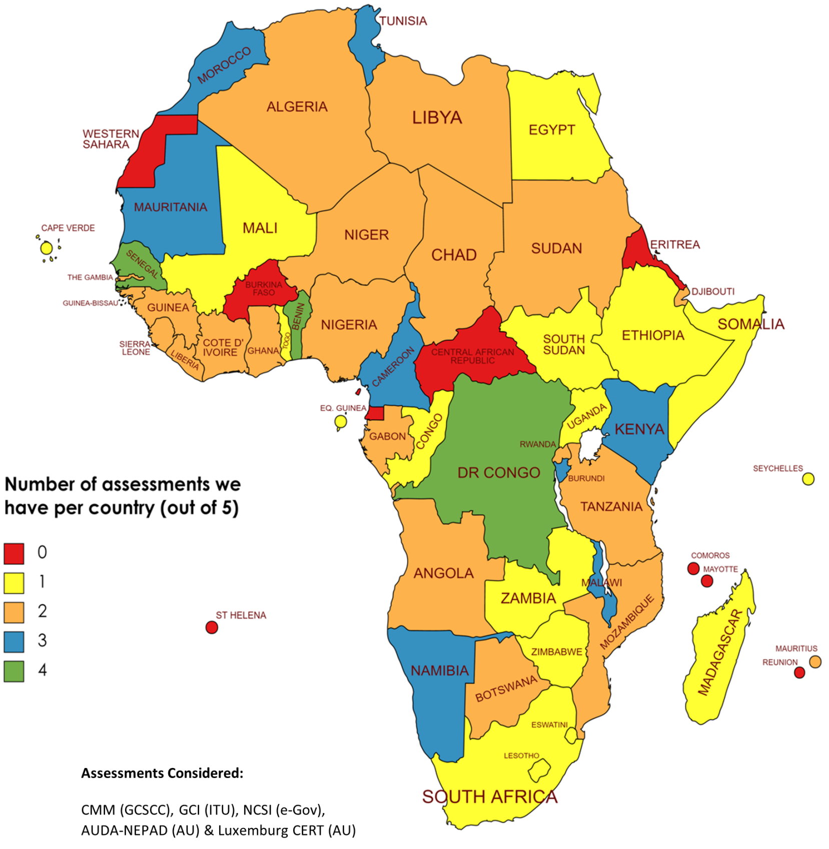


Figure 2. CCB Assessments Status in AU member states.

Africa Cyber Expert (ACE) Community

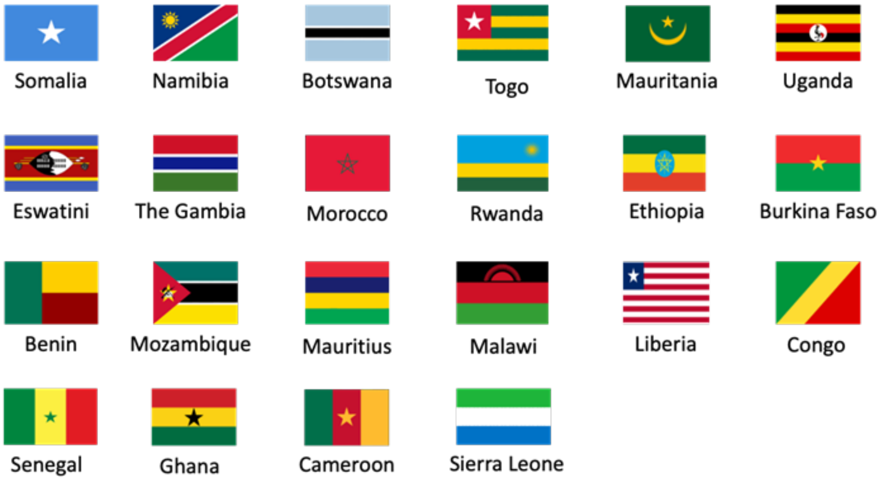


Figure 3. AU Member States who have submitted ACE nominees.

One of the sustainment strategies of the project is the establishment of an Africa Cyber Experts (ACE) community. The ACE community consists of relevant ICT experts selected from participating AU Member States. Together with other African expert communities, such as AU Cybersecurity Group (AUCSEG), the ACE community will participate in the development and deployment of the Knowledge Modules.

Working together with AU Development Agency (AUDA)-New Partnership for Africa's Development (NEPAD), over 20 AU member states (see Figure 3) have approved and submitted nominations of experts to the ACE community, who are currently participating in the development and planned deployment of the Knowledge Modules.

In partnership with AUDA-NEPAD, the AU-GFCE project has established the Africa CCB Coordination Committee.[2] The committee, which is focused in enhancing CCB in Africa, comprises of representatives with relevant expertise in ICT from the following institutions:

- African Union Commission (AUC)
- African Union Development Agency (AUDA NEPAD)
- The African Capacity Building Foundation (ACBF)
- Africa Computer Emergency Response Teams (AFRICACERT)
- African Network Information Centre (AFRINIC)
- The African Union Mechanism for Police Cooperation (AFRIPOL)
- The East African Community (EAC)
- The East African Communications Organization (EACO)
- The Common Market for Eastern and Southern Africa (COMESA)
- Communication Regulator of Southern Africa (CRASA)
- The Intergovernmental Authority for Development (IGAD)
- West Africa Telecommunications Regulators Assembly (WATRA)
- Arab Maghreb Union/Union Maghreb Arabe (UMA)
- United Nations Economic Commission for Africa (UNECA)
- Southern African Development Community (SADC)
- Economic Community of Central African States

The Committee is chaired by the AU and the secretariat is jointly managed by the GFCE and AUDA-NEPAD. It will also ensure that outcomes from the AU-GFCE Collaboration project remain beneficial and relevant to AU member states, as part of the long-term sustainment strategy of the project.

Knowledge Modules (KMs) – Design, Development & Deployment

In October 2021, the AU-GFCE project engaged an external consultant, Diplo Foundation, to lead the design, development and assist deployment of the Knowledge Modules (KMs). The main aim of KMs is to enable AU Member States to better understand and address cyber capacity building challenges.

As part of the development of knowledge modules, all identified CCB priority needs will form the input into the KMs design and development (see Figure 4). A number of KMs focus areas have been identified, including:

- Cybersecurity Policy, Regulation and Strategy
- Cyber Diplomacy, Norms and International Cooperation
- Cyber Incident Management, Critical Information Infrastructure Protection and Critical National Infrastructure Protection

- Cybercrime, Data Protection & Privacy; and Child Online Protection
- Cyber Culture, Awareness, Workforce and Skills
- Cyber Standards and Certification

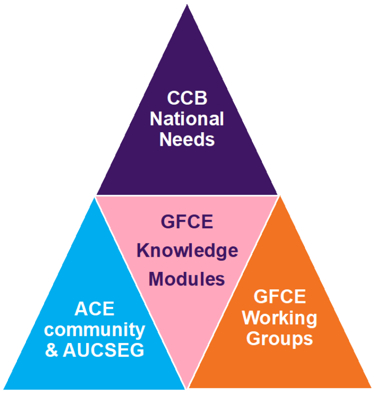


Figure 4. Knowledge Module.

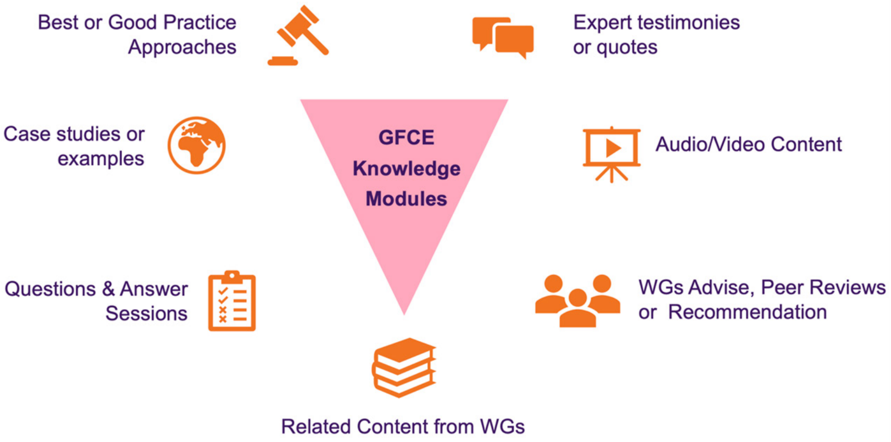

Best or Good Practice Approaches
Expert testimonies or quotes
Case studies or examples
GFCE Knowledge Modules
Audio/Video Content
Questions & Answer Sessions
WGs Advise, Peer Reviews or Recommendation
Related Content from WGs

Figure 5. KM Components.

a) KMs Components

The KM's design and development will comprise various components (see Figure 5). These components will enable the KMs to be effective and enable users to better understand CCB from a national and international perspective.

b) Engaging with both Africa and GFCE Communities

During the development stage of the KMs, the WG and Task Force will be requested to provide input, comments and recommendations to assist the design & development of KMs. Individual participants in the ACE Community will be involved in providing input to the KM's development. Relevant tools and products from both communities will be referenced to and/or mentioned in developing KMs.

The deployment stage of the KMs will involve both Africa (ACE) and GFCE communities. Various virtual sessions are planned that will involve the ACE community engaging in understanding the KMs. The ACE participants will provide discussion points, perspectives, experience and validate the KMs to ensure they address identified CCB priorities for participating AU member states.

GFCE experts will be invited to conduct some of these sessions focusing on relevant topics. These interactions, prior to the In-Person sessions, will enable better understanding and provide more in-depth information on key topics and opportunities for participants to have more clarity. Several experts will be requested to attend the In-Person sessions scheduled for February 2022 and July 2022.

Sustainability

One of the main tenets of the project is the sustainability of the outputs and enhancing anticipated impact of these results. During our outreach, several participating countries have already stated the need for funding and technical assistance. It is expected that such requests will be channeled to the GFCE Clearing House for consideration. If successful, the recipient countries will ensure that their cyber capacity posture is enhanced.

Secondly, the establishment of Africa CCB Coordination Committee, which comprises of nearly 16 Africa based organizations, will ensure that the outcomes from the project remain beneficial and relevant to AU member states after the project is complete.

Finally, AU member states will benefit from the vast resources and expertise offered by the ACE community of experts. Hence ensuring the project output and impact caused remains sustainable.

REFERENCES

1) Cyber Capacity Building (CCB) Needs: Mapping Exercise and Gap Analysis, AU-GFCE Project Report, July 2021.

2) Africa Cyber Capacity Building (CCB) Coordination Committee, Terms of Reference, September 2021.

AFRICA CYBER CAPACITY BUILDING COORDINATION COMMITTEE

Written by: Dr Towela Nyirenda-Jere, Head of Economic Integration at AUDA-NEPAD, and Bernard Brian Cudjoe, AU-GFCE Liaison

Twenty-two institutions from the Regional Economic Communities, the private sector and civil societies have been constituted to form the Cybersecurity Capacity Building Coordination Committee for Africa. Four of the institutions are observers of the committee. The African Union Development Agency and New Partnership for Africa's Development (AUDA-NEPAD) and the African Union Commission act as the committee's chair and co-chair, respectively. The main task of the Coordination Committee is to provide oversight and feedback on specific projects and regularly meet to discuss future CCB efforts in the region and ensure that the implementation of future projects are conducted inclusively and efficiently. The committee has been constituted to represent diverse multi-stakeholder interests and help achieve coherence, efficiency, and effectiveness in implementing cyber projects. The committee has only met once and plans to meet twice a year. Furthermore, the committee is supposed by the GFCE Secretariat.

In tackling the challenges and the gaps in cyberspace in Africa, the African Union and the GFCE are collaborating to further strengthen the cyber capacities of African Union member States with the AU-GFCE Cyber Capacity Building project from 2020 to 2022. There is an urgent need for inclusion in cybersecurity capacity building with a multi-stakeholder strategy that brings together the government, private sector, civil society, and industrial experts. The African Union Development Agency and New Partnership for Africa's Development (AUDA-NEPAD) are implementing this project. One of the project's achievements has been the establishment of the Africa Cyber Capacity Building Coordination Committee known as the CCB Coordination Committee. The coordination committee held its first virtual meeting on the 14th of September 2021 with AUDA-NEPAD, Africa CERT, UNECA, ACBF, AFRINIC, UMA,

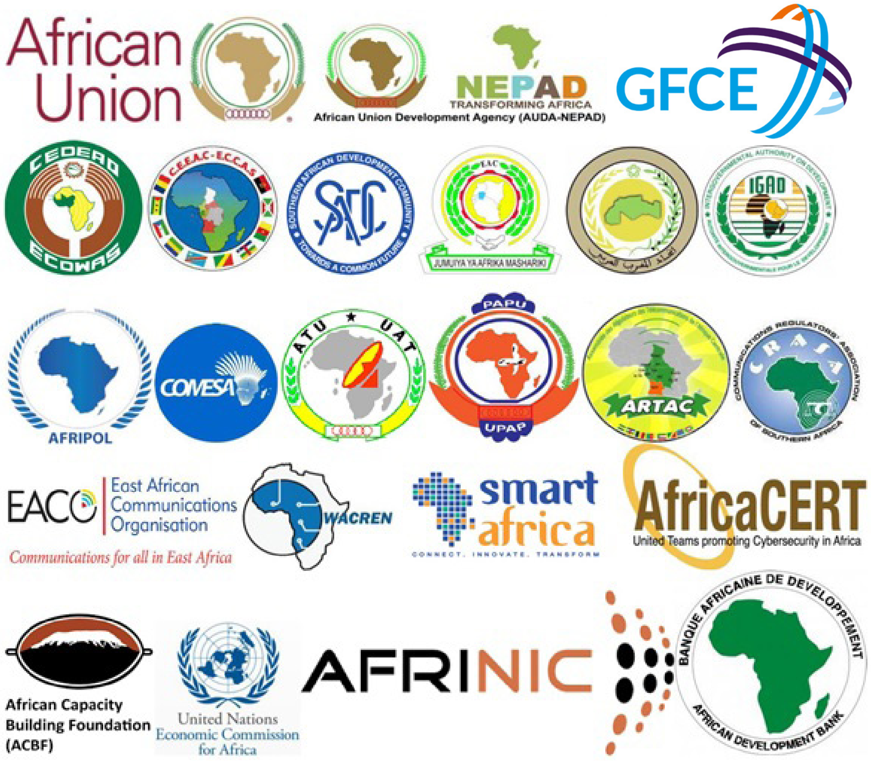

African Union
NEPAD
TRANSFORMING AFRICA
African Union Development Agency (AUDA-NEPAD)
GFCE
CEDEAO
ECOWAS
CEEAC-ECCAS
SOUTHERN AFRICAN DEVELOPMENT COMMUNITY
SADC
TOWARDS A COMMON FUTURE
EAC
JUMUIYA YA AFRIKA MASHARIKI
اتحاد المغرب العربي
IGAD
AFRIPOL
COMESA
ATU
UAT
PAPU
UPAP
ARTAC
CRASA
COMMUNICATIONS REGULATORS' ASSOCIATION OF SOUTHERN AFRICA
EACO
East African Communications Organisation
Communications for all in East Africa
WACREN
smart africa
CONNECT. INNOVATE. TRANSFORM
AfricaCERT
United Teams promoting Cybersecurity in Africa
African Capacity Building Foundation (ACBF)
United Nations Economic Commission for Africa
AFRINIC
BANQUE AFRICAINE DE DEVELOPPEMENT
AFRICAN DEVELOPMENT BANK

Figure 1. Members of the Africa Cyber Capacity Building Coordination Committee.

IGAD, AFRIPOL, AfricaCERT and EAC as members present at the meeting, which the GFCE Secretariat supported. The Committee has twenty-three institutions with five been observers.

The Coordination Committee was initiated because of the GFCE's flagship project, the AU-GFCE Cyber Capacity Building project, funded by the Bill and Melinda Gates Foundation. The project aims to enhance cyber capacity building knowledge to enable African countries to understand cyber capacities better and identify and address their national cyber capacity needs to strengthen their cyber resilience. The Coordination Committee will provide oversight and feedback on this specific project and regularly meet to discuss future CCB efforts in the region and ensure implementation of future projects is conducted inclusively and efficiently.

> "The Coordination Committee will provide oversight and feedback on this specific project and regularly meet to discuss future CCB efforts in the region and ensure implementation of future projects is conducted inclusively and efficiently."

Members of the CCB Coordination Committee are drawn from key institutions representing various stakeholder interests in Information and Communications Technology (ICT) and Cybersecurity in Africa. They will play a role in the implementation of CCB activities in Africa by:

1. Providing general oversight of the implementation of projects,
2. Reviewing and approving the work plan and schedule of activities of projects,
3. Facilitating engagement with African stakeholders for data collection and project activities,
4. Reviewing and approving project task reports and deliverables, and
5. Developing ideas for new CCB projects.

The projects will build on and utilize existing cyber structures, plans, expertise, and capacities within the AU and the international multi-stakeholder GFCE Community. The GFCE Secretariat and AUDA-NEPAD will be responsible for the coordination of the programs.

Speaking during the opening of the meeting, Mr Moctar Yedaly, the Coordinator for Africa at the GFCE, expressed his appreciation for the presence of the members and emphasized the need for a coordinated approach to cyber-initiatives: "We want this Coordination Committee to lead Africa in implementing the various projects and programs that we have across the continent. The Committee has been constituted to represent diverse multi-stakeholder interests and will help us to achieve coherence, efficiency and effectiveness in the implementation of cyber-projects."

> "The Committee has been constituted to represent diverse multi-stakeholder interests and will help us to achieve coherence, efficiency and effectiveness in the implementation of cyber-projects."

Mr David van Duren, Director of the GFCE Secretariat, reiterated the GFCE's commitment to building Africa's Cyber-capacity. The added value of the GFCE is to connect the rest of the world to CCB projects in Africa. During the inaugural meeting, members were briefed on the various elements of the project and their critical role in its implementation. In the discussions that ensued, members welcomed the initiative. They expressed their interest to ensure that the project was linked to existing initiatives and would provide the space for Africa to step up its implementation of cyber-initiatives. The meeting also welcomed the establishment of the African Cyber Experts (ACE) Community which had its first meeting in early October.

AUDA-NEPAD chaired the meeting as an implementing partner of the GFCE. In her remarks, Dr Towela Nyirenda-Jere, Head of Economic Integration at AUDA-NEPAD, underscored the success of this project and other cyber-initiatives rested with the commitment of the Committee.

The meeting ended with agreements for the members of the CCB Committee to exchange information on initiatives they have undertaken or are undertaking across the continent. The next meeting of the Committee will happen later in the year, possibly alongside the GFCE Annual Meeting.

NETWORK OF AFRICAN WOMEN IN CYBERSECURITY (NAWC)

Written by: Nnenna Ifeanyi-Ajufo, on behalf ot the NAWC Steering Committee, and Bernard Brian Cudjoe, AU-GFCE Liaison

Ten experienced professional women from the five African Union (AU) Geographic Regions came together under the auspices of the GFCE to address the contribution and needs of African women and girls in issues relating to cybersecurity and digital development. As a result, they created the Network of African Women in Cybersecurity (NAWC), comprising of experienced women from across the Africa region, who are ready to provide expert advice and technical guidance at various levels, to help bridge the gender gap in gender-responsive Cybersecurity planning, development, and implementation in Africa.

While substantial efforts are being made to address women's involvement and empowerment through ICT development, much more can be done. Early June 2021, saw ten experienced professional women from the five African Union (AU) Geographic Regions come together under the auspices of the GFCE to discuss the specific contribution and needs of African women and girls in issues relating to cybersecurity and digital development.[1] The discussion centered on the fact that the African continent, by all indicators, is considered the least endowed region when it comes to cybersecurity development in the world. Therefore, the underlying reason for focusing efforts and resources on improving the status quo of cybersecurity is because it serves as the basis for the safety and development of all other sectors and total economic growth. In particular, Gender-responsive cybersecurity planning, development, and implementation in Africa needs to be enhanced by concentrating on the special requirements of women and girls – while underlining the need for gender-neutral cybersecurity development.

As a result, the Network of African Women in Cybersecurity (NAWC), comprises of experienced women from across the Africa region, ready to provide expert advice and technical guidance at various levels, to help bridge the gender gap in gender-responsive Cybersecurity planning, development, and implementation in Africa by focusing on the specific needs of women and girls in the process.

> “The NAWC comprises of experienced women from across the Africa region, ready to provide expert advice and technical guidance at various levels, to help bridge the gender gap in gender-responsive Cybersecurity planning, development, and implementation in Africa.”

Figure 1. Steering Committee members of the Network of African Women in Cybersecurity.

The NAWC recognizes that cybersecurity affects development patterns and outcomes, economic opportunities, and resource allocation in markedly different ways for men and women. The network also emphasizes that cybersecurity development should be gender-neutral because men and women have distinct roles and responsibilities. Typically, women face a variety of cultural, institutional, physical, and economic constraints, many of which are rooted in systemic stereotypes. Again, the disparities in how men and women access and utilize ICT services have significant consequences for cybersecurity sector policy and program designs. The Network’s overarching purpose is therefore to increase women’s engagement in cybersecurity at the national, regional, continental, and global levels.

The network draws membership from government officials, officials of Regional Economic Communities, the private sector, academia, women in cybersecurity and business professional associations and the civil societies. The African Union Commission and the African Union Development Agency New Partnership for Africa’s Development (AUDA-NEPAD) will also provide representatives for the membership.

The NAWC is successfully registered under the company registration ACT of the Republic of Ghana. They have instituted the steering committee which comprises of ten members to propose and approve annual activities of the network. The network is looking forward to its first regional consultation in the months to come and also will organize its first continental meeting to officially launch the network and also call for increased membership.

> “The disparities in how men and women access and utilize ICT services have significant consequences for cybersecurity sector policy and program designs.”

NOTES

1) Fifty other African women with expertise in Cybersecurity have been identified and will be invited to contribute to building the network.

BUILDING REGIONAL CYBER AND CRITICAL TECH RESILIENCE THROUGH COOPERATION

Written by: Tobias Feakin, Australia's Ambassador for Cyber Affairs and Critical Technology

Australia is committed to working with like-minded countries and regional partners to ensure everyone can access a safe, secure and inclusive internet. Australia's International Cyber and Critical Tech Engagement Strategy is the overarching framework guiding Australia's global engagement across the spectrum of cyber and critical technology. A key deliverable of this strategy is Australia's Cyber and Critical Tech Cooperation Program (CCTCP) which funds cyber and critical tech capacity building projects throughout the Indo-Pacific. The CCTCP operates in partnership with regional NGOs, government and private sector organizations to deliver cyber resilience and capacity building projects. Our capacity building projects are about more than just cyber security. They also support the governance structures and standards required to seize emerging opportunities in tech, provide a framework for upholding human rights and democratic values online, and promote the responsible use of an open and rules-based cyberspace. This article will explore how CCTCP supported initiatives and programs contribute to Australia's vision of an open, free, safe and secure cyberspace.

Technology is changing the way we interact, do business and experience the world around us. Prosperous countries of the future will be those that can harness the incredible potential of cyber and emerging critical technologies while simultaneously minimizing the risks.

This is particularly true for the Indo-Pacific region, where rising connectivity is increasingly enabling countries to capitalize on opportunities presented by the Internet and digital technologies.

It should come as no surprise then that regional cooperation and partnerships across the Indo-Pacific feature heavily in Australia's International Cyber and Critical Tech Engagement Strategy.

Launched in April this year, the Strategy expands on Australia's first International Cyber Engagement Strategy released in 2017 and charts a course towards realizing Australia's vision of a safe, secure and prosperous Australia, Indo-Pacific and world enabled by cyberspace and critical technology.

Investing in regional cyber and critical tech resilience benefits everyone just as a strong collective security posture means a safer cyberspace for all.

Cyber capacity building should be on the radar of all countries concerned with securing a brighter online future and Australia is no exception.

We aim to lead by example through our support for a number of significant and effective cyber and critical technology capacity building projects abroad.

The Cyber and Critical Tech Cooperation Program

Australia's total investment across all cyber cooperation and capacity building initiatives is just under AUD$100m over nine years. The vast majority of this funding is dedicated to Australia's Cyber and Critical Tech Cooperation Program (CCTCP) which has supported our Indo-Pacific neighbors since 2016.

The CCTCP's success is based on its strong partnership model working closely with more than 40 entities from industry, academia, government and the not-for-profit sector to deliver 94 cyber capacity building projects across 25 Indo-Pacific nations.

Figure 1. Cyber and Critical Tech Cooperation Program Logo.

Of these, 48 have been completed with a further 46 currently under way.

Australia takes a holistic approach to strengthening regional cyber and critical tech resilience and while certainly important, cybersecurity is just one piece of the puzzle.

Our international engagement seeks to shape the design, development and use of secure, resilient and trusted technology in line with Australia's democratic values.

It is important to note Australia does not seek to impose its values on others, our focus is contributing to an inclusive cyberspace which upholds liberal institutions and human rights built on values of transparency, fairness, respect and integrity.

This includes enhancing the development and implementation of internationally recognized and industry-led critical technology standards and strengthening institutional capacity to identify and assess risks to counter online harms while fostering a safe and inclusive online environment.

Three main pillars – values, security and prosperity – guide Australia's international cyber and critical technology engagement and are a useful lens through which we can explore some of our capacity building projects.

> "Our focus is contributing to an inclusive cyberspace which upholds liberal institutions and human rights built on values of transparency, fairness, respect and integrity."

Values

Australia takes a values-based approach to building regional cyber and critical tech resilience.

These values are not defined by race or religion but rather a shared commitment to political, religious and economic freedom, the rule of law, racial and gender equality and mutual respect.

Our flagship Cyber Bootcamp Project (CBP) is one such program building strong values-based governance and capability.

Delivered in partnership with the Australian National University's National Security College (NSC), the CBP provides practical expert advice and skills to government officials in Southeast Asian countries, most recently the Philippines.

Other courses funded by the CCTCP aim to uphold human rights online by examining the intersection of state interests and individual rights regarding matters of mass surveillance, managing harmful online content and reliance on digital service providers.

Australia works alongside Plan International to equip young people in Solomon Islands with the knowledge and skills to apply protective strategies for responsible and safe internet usage while actively promoting the rights of children and young people online.

We've also partnered with Independent Diplomat to strengthen the capacity of Pacific island leaders, officials, and negotiators to engage in UN cyber processes.

Supporting liberal democratic values also means championing gender equality in all arenas including cyber and critical technology.

Australia is proud to operate programs supporting the career advancement of mid-career women in the internet industry in Vietnam, Thailand, Philippines and Cambodia.

We also partner with the APNIC Foundation to develop the network engineering and management skills of the next generation of female tech leaders in Southeast Asia while the Girls Online! program empowers young women in Tonga and Vanuatu to engage safely online by exploring cyber safety rights, experiences, and issues in partnership with ABC International Development.

Security

Guided by the security pillar, Australia's cyber engagement includes numerous programs and initiatives throughout the Indo-Pacific helping to support a region powered by secure, resilient and trusted technology.

The Pacific Cyber Security Operational Network (PaCSON), supported through Australia's CCTCP, is one such initiative increasing regional cyber and critical tech resilience through a strong partnership and collaborative approach.

PaCSON brings together a network of Pacific cyber security response professionals to encourage best practice through closer collaboration, information sharing and the development of greater regional incident response capability.

The network has also developed linkages with Cyber Safety Pasifika (CSP) and the Pacific Islands Law Officers' Network (PILON), two other CCTCP funded initiatives.

Figure 2. PaCSON Annual General Meeting 2019.

CSP delivers cybercrime investigative and awareness training to 19 Pacific countries in partnership with the Australian Federal Police; this is in addition to their Cyber Safety Asia program which aims to increase cyber law enforcement capability throughout Southeast Asian countries.

PILON brings together senior law officers from Pacific Island countries, including Australia and New Zealand, to discuss domestic and regional law and justice issues including cybercrime.

In the Philippines we work with cyber security experts FireEye to deliver training in cyber security operations and risk assessments. We also support a similar series of cyber security advisory and uplift programs throughout the Pacific in partnership with Trustwave.

In addition to our CCTCP funded initiatives, Australia supported Papua New Guinea's (PNG) National Cyber Security Centre (NCSC) through the Australia and PNG memorandum of understanding on cyber security cooperation.

PNG's NCSC has delivered real cyber security uplift for one of the Indo-Pacific's fastest growing online populations helping to protect key government services by establishing a cyber security stack for their Department of Health while also playing an important role in protecting the 2018 APEC meeting in Port Moresby.

Prosperity

Prosperity is the final pillar guiding Australia's cyber and critical technology engagement, ensuring our efforts support sustainable economic growth and development.

Technological developments are now at the center of economic growth and access to modern and resilient financial technologies are key to upholding the economic circumstance of citizens everywhere.

We have partnered with Pacific financial institutions to increase access to secure digital banking services and boost digital product security.

As access to online banking becomes widespread, more citizens are able to start a business, access credit, invest in their communities and develop new employment opportunities.

Digital banking also fuels positive economic decentralization as people are empowered to work or conduct business remotely mitigating the disruptions caused by future pandemics or other natural catastrophes.

A prosperous and inclusive cyberspace is one that operates in an open and rules-based manner.

Australia's cyber capacity building initiatives also build awareness of how international law can apply to cyberspace through executive education courses for Pacific and ASEAN advisers.

We are also supporting the delivery of training and resources to Vietnam, Thailand, Myanmar and Laos regarding standards development in producing secure critical technologies as well as a pilot project with Standards Australia to support the development, adoption and use of recognized international standards for critical and emerging technologies in Southeast Asia.

> "Building an open, free, safe and secure cyberspace is more than an aspiration, it is a top foreign policy issue"

Reflections

The experience of COVID-19 confirmed that the days where countries, businesses and individuals could afford to ignore cyber and critical technologies are firmly over.

In an instant, millions found themselves totally dependent on cyberspace for work, education, tele-health and social engagement.

Building an open, free, safe and secure cyberspace is more than an aspiration, it is a top foreign policy issue.

This is why Australia is proud to work alongside our international partners through the CCTCP to support cyber and critical technology capacity building programs across the Indo-Pacific.

If you would like to learn more about Australia's International Cyber and Critical Tech Engagement Strategy or our capacity building programs, please visit internationalcybertech.gov.au.

Critical Technologies explained

The Australian Government defines critical technologies as those technologies with the capacity to significantly enhance, or pose risks to, Australia's national interests, including our prosperity, social cohesion and national security.

This includes, but is not limited to, technologies (or applications of technologies) such as cyberspace, Artificial Intelligence (AI), 5G, Internet of Things (IOT), quantum computing and synthetic biology.

These, and other emerging technologies, will transform economic competitiveness, national and international security as well as democratic governance and social cohesion. These new technologies are often enabled by, and reliant on, information that is created, stored and transmitted through digital networks.

CYBERSECURITY IN THE PACIFIC: REGIONAL IN NATURE, LOCAL IN PRACTICE

**Written by: Bart Hogeveen, Head of Cyber Capacity Building,
ASPI's International Cyber Policy Centre (ICPC), and
Cherie Lagakali, GFCE Pacific Liaison**

In the past year, the GFCE team in the Pacific has prepared a context analysis of cyber capacity building in the region and prepared a recommendation for a potential GFCE role. From the interviews and consultations we held, two strong messages resonated:

In their activities, the international cyber capacity building community should look to work with local communities of practice; and they should be absolutely certain that any activities, materials and solutions are fit for purpose and can be absorbed in the local Pacific context. In this article we share examples of local organizations and regional networks in the incident response community that have taken up the challenge of strengthening local awareness in cybersecurity, and of the recent Cyber Smart Pacific campaign that was launched regionally but delivered locally in 14 individual Pacific Island nations.

Even though most islands in the South Pacific ocean have been spared from the worst of the Covid-19 pandemic, people were prevented from regional travel for almost two years. Internet connectivity, once again, served as a lifeline for people, businesses and governments, but it also exposed users to new sorts of risks.

> *"We, in the Pacific, never really had to fight cyber incidents previously. For Samoa - we are new victims to cyber attacks, we can't do it ourselves. We have never experienced this in the Pacific before - the islands need to come together and form crucial partnerships for a more inclusive approach to fight emerging challenges in our cyberspace."*
>
> *- Fualau Talatalaga Mata'u Matafeo, CEO of the Ministry of Information and Communication, Samoa*

Figure 2. PNG's Department of Information and Communications Technology, in Port Moresby.

On 22 October, the government of Papua New Guinea, a nation of 9 million people, was hit by a ransomware attack affecting the central financial management system. While the exact cause of the incident is yet unknown, Minister for ICT Timothy Masiu called on the need to "escalate ICT to the strategic level in the Public Service" and underlined the need for "(...) appropriate mechanisms for enforcement of cyber security standards and a governance framework for ICT functions" (from: Srly Risky Biz, 4 November).

Last year, PNG became the first Pacific member of the GFCE. Since then, assistance has been provided in preparing a Digital Government Bill which is currently with Cabinet for approval. Earlier, in 2018, the Australian government had already agreed to fund the establishment of a Cyber Security Operations Centre in Port Moresby and a national CERT.

The ransomware incident, however, shows that cybersecurity practices and the adequate use of the expertise of a national cybersecurity center should not be taken for granted.

> "Cybersecurity practices and the adequate use of the expertise of a national cybersecurity center should not be taken for granted."

National incident response teams in the Pacific have been going above and beyond their primary technical responsibilities and have played a pivotal role in broadening the reach and impact of digital safety and cybersecurity awareness campaigns.

Earlier this year, Samoa (200,000 inhabitants) opened the doors to their national Computer Emergency Response Team (CERT). SamCERT is the latest addition to the growing network of Pacific incident response teams that have been established in a concerted effort by national authorities supported by partners such as APNIC, and the New Zealand and Australian governments. National CERTs are now operational in Tonga, Vanuatu, Papua New Guinea and Samoa.

As the group of local CERTs is expanding, it has become more common for colleagues to reach out to one another and ask for advice from lessons learnt and best practices in building incident response capabilities. Additionally, CERT NZ has been offering the community dedicated technical advice - recent examples include advice on dealing with ransomware, and a series of capacity building sessions ("Remote Session") which reached over 295 participants.

This is further amplified by the Pacific Cyber Security Operational Network (PaCSON) which was established in 2018. Currently chaired by Tonga, the network brings together operators and technical experts of the recognized teams from Australia, the Cook Islands, Fiji, Kiribati, Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu, and Vanuatu.

CYBER SECURITY
Protect Yourself from Cyber Attacks
Be CAREFUL what you share ONLINE. DON'T BECOME AN EASY TARGET
MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
Communications Sector 2017/18 – 2021
SamCERT
Samoa Computer Emergency Responce Team

Figure 2. Samoa's National Computer Emergency Response Team (SAMCERT).

Collaborative regional effort, localized delivery

For a second year in a row, members of the PaCSON Awareness Working group, chaired by CERT VU, set about preparing the regional Cyber Smart Pacific cybersecurity awareness campaign. Spearheaded by CERT NZ, regional template materials such as posters, flyers, video clips and stickers were produced with the motto: Cyber UP Pacific.

> "While the Pacific may appear a relatively homogeneous group of small island nations, navigating the region requires tailored and localized approaches."

While the Pacific may appear a relatively homogeneous group of small island nations, navigating the region requires tailored and localized approaches. Therefore, the local PaCSON members were responsible for translation in local languages, distribution and campaigning. For instance, in the Cook Islands (population 18,000), the government worked together with Vodafone. Their subscribers received daily text blasts with reminders of cybersecurity pitfalls and easy-to-action tips to up their safety. This was in tandem with 15-second video clips that ran at prime time on national television.

In Tonga (population 106,000), the Cyber UP materials were translated in Tongan while CERT Tonga used their Facebook and Twitter channels to reach local communities. In addition, workshops were hosted for government departments and local businesses.

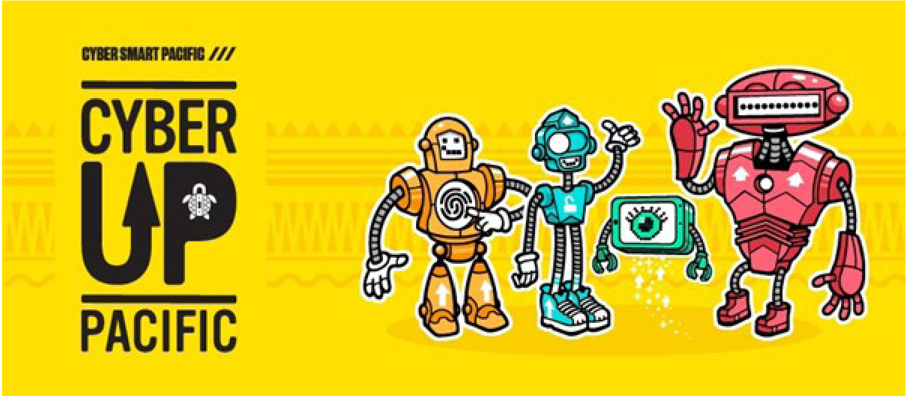
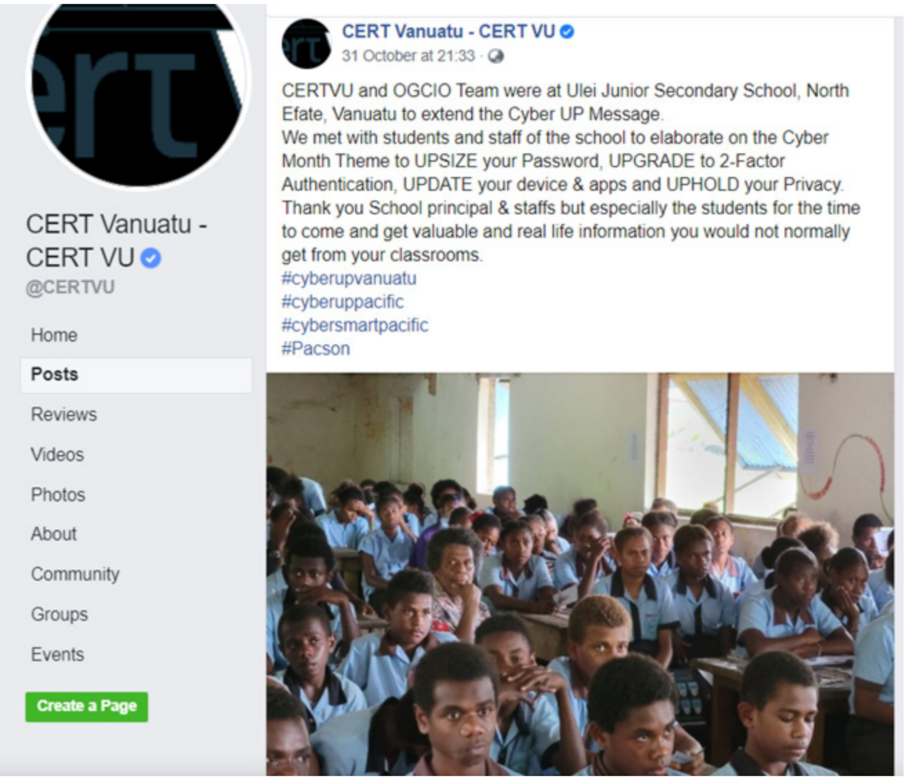


Figure 3. Cyber Smart Pacific cybersecurity awareness campaign banner, using the motto "Cyber UP Pacific.".



CERT Vanuatu - CERT VU
31 October at 21:33

CERTVU and OGCIO Team were at Ulei Junior Secondary School, North Efate, Vanuatu to extend the Cyber UP Message.
We met with students and staff of the school to elaborate on the Cyber Month Theme to UPSIZE your Password, UPGRADE to 2-Factor Authentication, UPDATE your device & apps and UPHOLD your Privacy.
Thank you School principal & staffs but especially the students for the time to come and get valuable and real life information you would not normally get from your classrooms.
#cyberupvanuatu
#cyberuppacific
#cybersmartpacific
#Pacson

Figure 4. CERTVU and OGCIO Team were at Ulei Junior Secondary School, North Efate, Vanuatu to extend the Cyber UP Message. From: Facebook.

In Vanuatu (population 307,000), cybersecurity capacity building is a collaborative effort of the Government Chief Information Office, Vanuatu Internet Governance Forum and CERT VU. In October, staff visited schools and other community locations on the main island and various smaller islands to speak about privacy, passwords and keeping devices up to date.

In Kiribati, the government already had plans for a cybersecurity awareness week, including through local community ambassadors appointed in government departments. They experienced that producing localized content on cybersecurity and online safety is no easy feat.

“The Kiribati language lacks most of the technical terms used to emphasize the concept of cyber security and that makes it difficult to achieve the objective which is to make the articles clear and understandable to non-technical people.“ - Wayne Reiher, Director of ICT, MICTTD (Source: Get Safe Online)

In fact, developing local content and context for a community of 120,000 people spread out over 33 atolls and 3.2 million km2 is a time-consuming, difficult and complicated process.

Instead, the Ministry of Information, Communication, Transport and Tourism Development decided to call a four-day retreat of ministries and state-owned enterprises. Collaboratively participants updated available e-safety and cybersecurity content to accurately reflect the local Kiribati language and they customized select materials from the Cyber UP campaign.

At the GFCE regional meeting in Melbourne in 2020, participants raised the concern that training for national CERTs and digital safety projects were at risk of becoming crowded areas of international assistance. In fact, the Pacific is receiving attention from a growing group of international partners. This includes donors, industry partners as well as providers of cyber capacity building assistance.

As the GFCE is finalizing the feasibility study for a Pacific hub, the team in the Pacific has been relying on the relentless support from the Pacific community who participated in interviews, consultations and meetings.

One of the expected outcomes of the future Pacific hub is to record the many exciting grass-root cyber developments that are occurring across the region, and help donors, implementers and Pacific partners establish a good understanding of any capacity building requirements, local context and community leaders in cybersecurity.

INTRODUCING THE ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE (AJCCBC)

Written by: AJCCBC Management Team

Cybersecurity has become increasingly important around the globe as we move towards a digital world with a high number of daily activities involving cyberspace, whether for personal or business usage. As a global shortage of competent cybersecurity professionals is evident, ASEAN and Japan collaborated to build an ASEAN-Japan Cybersecurity Capacity Building Centre in 2018 in Bangkok, Thailand with the aim to train 700+ cybersecurity professionals for the ASEAN region. Currently, the Centre has conducted 16 training sessions and a number of related activities for more than 550 ASEAN Member States (AMS) participants and will reach its 700+ goal by 2022.

Background and Significance of the Centre

As the world becomes more interconnected and more devices are linked to the Internet, maintaining a safe and secure environment for citizens and businesses becomes increasingly challenging for governments, especially when cyber criminals constantly deploy innovative tools to attack unsuspecting targets around the world. Moreover, the shortage of competent cybersecurity experts in the public and critical information infrastructure (CII) sectors in ASEAN further exposes nations to potential cyber-attacks that could severely impact social and economic well-being. The 9th ASEAN-Japan Information Security Policy Meeting in 2016 noted that

Figure 1. AJCCBC Office.

the shortage of cybersecurity professionals will become more serious in the coming years since many organizations and institutions increasingly, and in some cases even exclusively, conduct their communications, processes, and businesses online.

Cyber threats are prevalent and threat techniques have also been rapidly evolving. In 2018, to commemorate the 45th anniversary of the ASEAN-Japan Friendship and Cooperation agreement, the Japanese government offered multi-year financial support worth approximately USD4.4 million to build and operate the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok, Thailand to strengthen the cybersecurity competencies of ASEAN Member States (AMS), particularly CII operators and actors from government agencies.

Centre Achievements and Challenges

Developing 700+ cybersecurity professionals has been the primary objective of the Centre from the start. The Centre aims to equip AMS participants with technical skills in incident response, malware analysis, network forensics, and other relevant activities. From 2018 to November 2021, the Centre successfully hosted 16 training sessions and 4 Cyber SEA Games for more than 550 AMS participants. Illustrating the Centre's goal to enhance the capacities of the participants, the bar chart in Figure 2 shows a comparison between pre-test capacities and post-test capacities of the 3 training courses. It is clear that the capacity of the trained personnel significantly improved. The average score from the incident response courses increased from 3.5 to 6.11 out of 10, while malware analysis increased from 5.14 to 7.85, and network forensics rose from 4.81 to 7.97.

> "The shortage of competent cybersecurity experts in the public and critical information infrastructure (CII) sectors in ASEAN further exposes nations to potential cyber-attacks."

AJCCBC ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE Partnership by ASEAN and Japan

Japan-ASEAN Cooperation

MIC Ministry of Internal Affairs and Communications

ETDA www.etda.or.th

AJCCBC Training facility for ASEAN Bangkok, Thailand

$4.4M

Approved Budget

Supported by Japanese Government and operated by Thailand

550+

Participants from AMS

Government officers and CII operators have participated in the trainings

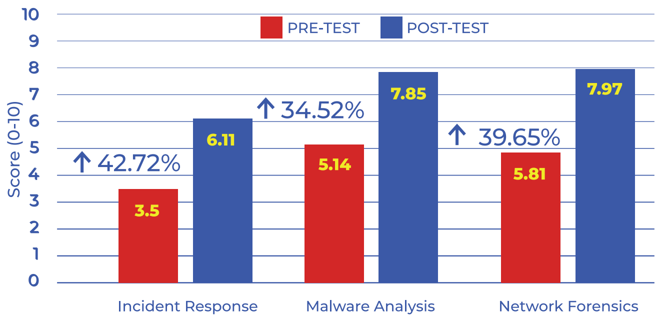
16 Training Sessions

Year-round intensive hands-on cyber courses (online format during covid-19)

4 Annual Cyber SEA Games

AMS professionals competed in the unique cyber drill exercise annually

AMS Cyber Improvement



Past Cyber SEA Game Champions

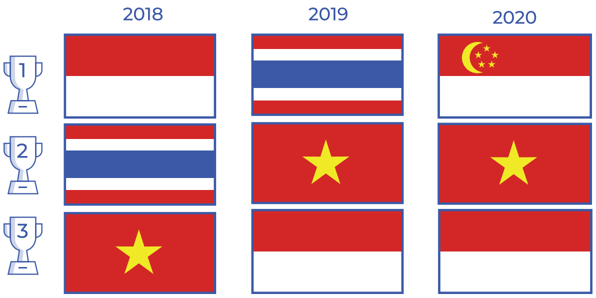


Figure 2. Numerical summary of the AJCCBC's progress.

"From 2018 to November 2021, the Centre successfully hosted 16 training sessions and 4 Cyber SEA Games for more than 550 AMS participants."

Acknowledging the importance of the role played by a new generation of trained professionals to strengthen cybersecurity, the Centre conducts annual Cyber SEA Games to challenge Southeast Asian participants The Centre values the importance of expanding abilities to solve difficult computer security problems and developing in-depth cybersecurity-related skills as well as bringing those working in cybersecurity together. It is important to build stronger bonds among cybersecurity officials and key critical information infrastructure operators to strengthen regional cybersecurity in the region

Throughout 2020-2021, the COVID-19 challenge has become the main obstacle to conducting the Centre's face-to-face training sessions. Although the Centre managed to sustain its operations by converting to online training and activities, it still faced many hurdles such as Internet connection instability and the limitations of online training tools. The Centre is still discussing how to improve the situation and develop better solutions for future training sessions.

Current Focus of Cybersecurity Capacity Building Centre

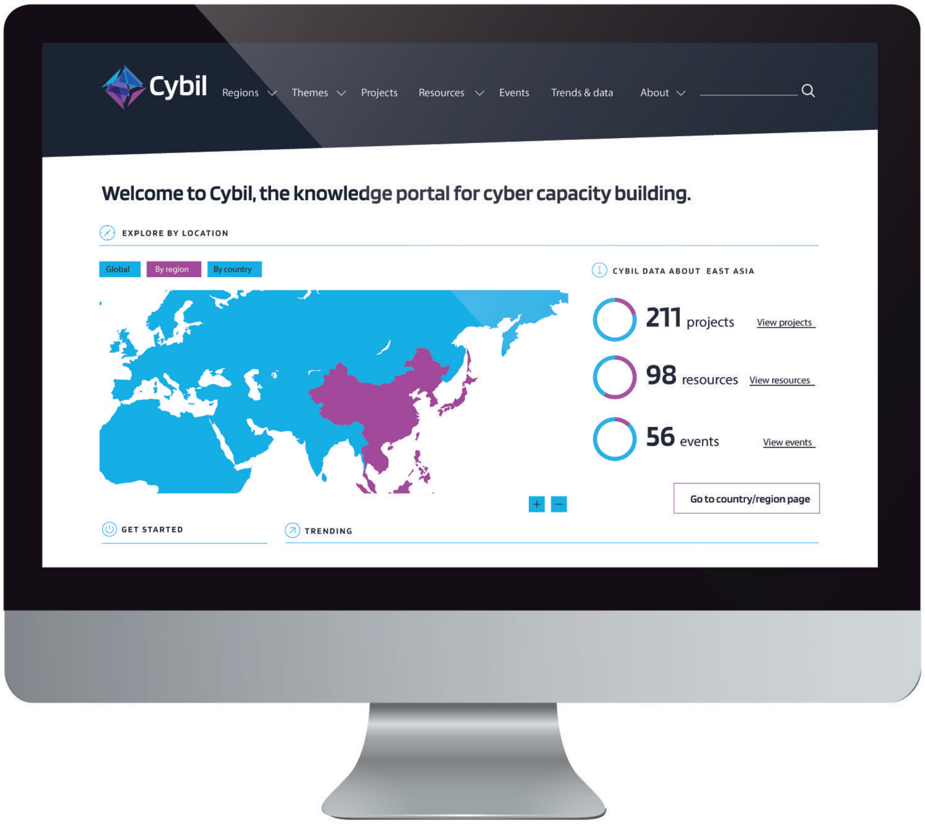
Having successfully trained more than 550 participants, the Centre aims to upskill approximately 200 additional personnel in technical sessions and other relevant activities to continue its effort to strengthen the cyber community in the region by addressing the shortage of cybersecurity professionals. The Centre expects to reach its 700+ goal by December 2022. The Centre also prioritizes gender equality to ensure that there is no gender discrimination. All AMS are welcome to participate and are treated equally and respectfully. Currently about 20% of those who have completed the training organized by the Centre are female and more are encouraged to apply.

Sustainability of Cybersecurity Capacity Building Centre

The Centre plans to provide capacity-building programs to fulfil AMS training demands through a three-fold strategy. Firstly, the Centre aims to collaborate and acquire knowledge provided by international experts; Secondly, it will share such knowledge among AMSs through activities such as on-site and online cyber incident response exercises, malware analyses, digital forensics, trusted digital services courses, Cyber SEA Games, workshops, conferences, and seminars; and Thirdly, the Centre plans to exchange learned-lessons, good practices, and accomplishments with the international cybersecurity community.

Cybil 2.0 is here.

The global knowledge hub on cyber capacity building



Cybil

Regions · Themes · Projects · Resources · Events · Trends & data · About

Welcome to Cybil, the knowledge portal for cyber capacity building.

EXPLORE BY LOCATION

Global · By region · By country

CYBIL DATA ABOUT EAST ASIA

211 projects · View projects

98 resources · View resources

56 events · View events

Go to country/region page

GET STARTED

TRENDING

More interactivity

Discover projects and resources through maps and filters

New resources

Tools, publications and now recordings of webinars

Events calendar

A calendar of past and upcoming cyber capacity building events

www.cybilportal.org

Got an initiative, report, event to share? Get in touch with us via the portal or email us at contact@cybilportal.org.

Volume 10,
November 2021
Global Cyber
Expertise Magazine

Colophon

Editorial Board:

Adil Sulieman (AU)
Georgiana Macovei (EU)
Gabriela Montes de Oca (OAS)
Kathleen Bei (GFCE)

Guest Editors:

Giacomo Assenza
Francesca Spidalieri
Carolin Weisser Harris
Robert Collett
Michele Markoff
Gerardo Isaac Morales Tenorio
Nikolas Ott
Kezia Wexoe-Mikkelsen
Joe Burton
George Christou
Martin Koyabe
Towela Nyirenda-Jere
Bernard Brian Cudjoe
Nnenna Ifeanyi-Ajufo
Tobias Feakin
Bart Hogeveen
Cherie Lagakali
AJCCBC Management Team

Artwork & Design:

Roguer Restrepo Estrada (Colorful Penguins)
Anna Noij (GFCE)

Chief editors:

Anna Noij (GFCE)
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 11 submission deadline:
1 March 2022