Volume 9, June 2021

GLOBAL CYBER EXPERTISE MAGAZINE

African Union

GFCE

OAS More rights for more people

Volume 9, June 2021

Global Cyber Expertise Magazine

Editorial

Regions

Africa

Americas

Asia & Pacific

Europe

Global Developments

Editorial

On behalf of the Editorial Board, I am pleased to welcome you to the ninth (9th) edition of the Global Cyber Expertise Magazine! This edition is released in conjunction with the virtual GFCE Consultation Meeting 2021, an opportunity for the GFCE Community to gather and share their ideas and input.

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

In this issue, our cover story takes a look at why cyber portals are important for cyber capacity building, from our Americas section. The Americas section also includes an article exploring the importance of public-private partnerships in the aftermath of COVID-19. From Africa, we have an article on the development of Sierra Leone's national cybersecurity strategy, in addition to an article focused on building local partnerships to help young Batswana to be 'cyber smart'. From Asia and the Pacific, we have an article highlighting the development and workings of the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), and another article analyzing the use of the CMM in the Pacific region. From Europe, we have a follow-up article from one of our previous issues on EU CyberNet. In addition to the regional section, we have three articles in our global developments section. Firstly, this issue dives into the GFCE Women in Cyber Capacity Building Network to highlight gender empowerment in cyber. Next, we have an article rethinking cybersecurity capacity building based on revelations from the healthcare sector. Last but not least, this issue features an article on the GFCE's regional approach as one of the key GFCE Strategic Building Blocks.

We thank our guest writers for their valuable contributions to the ninth (9th) 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

TOWARDS AN INCLUSIVE CYBERSPACE: DEVELOPING SIERRA LEONE'S NATIONAL CYBERSECURITY STRATEGY

Written by: Daniela Schnidrig, Senior Program Lead, Global Partners Digital

Inclusive and human-rights based cyber policymaking is critical to realize the full potential of cyberspace and ensure that it continues to underpin social and economic prosperity and promote a society for all. Between 2018-2021, the Ministry of Information and Communications of Sierra Leone developed its national cybersecurity strategy with support from Global Partners Digital (GPD) and in collaboration with other international implementers via the GFCE's Clearing House Function. The development process featured several instances of stakeholder consultation and capacity building to inform the strategy. This article aims to share the experience and lessons learned from developing Sierra Leone's national cybersecurity strategy in an inclusive way, to help inform future policymaking processes and capacity building efforts.

> "There is an urgent need to reinforce the importance of inclusive and human rights based cyber policymaking ."

Inclusive and Human Rights Based Cyber Policymaking

There is an urgent need to reinforce the importance of inclusive and human rights based cyber policymaking in order to realize the full potential of cyberspace, ensuring that it continues to underpin social and economic prosperity and promote a society for all.

The value of this approach is clear: an online environment that enables individuals to exercise their rights and enjoy their freedoms is a prerequisite for user trust, which, in turn, is crucial for sustained uptake and use of the Internet. The absence of such conditions – where, instead, users fear their privacy may be undermined through lack of data protection or due to pervasive surveillance – has been identified as one of the key obstacles for meaningful access and future growth of the digital economy.

An inclusive approach to cyber policymaking goes hand in hand with this by helping to ensure that views of those that are affected are taken into account and not side-lined by securitized and threat-driven narratives. In fact, experience from countries that have developed their national cybersecurity strategies in an inclusive way has shown that this approach not only enables stakeholder views to be better represented, but also helps increase buy-in from relevant stakeholders when it comes to implementing the strategy, thus ensuring a more sustainable, effective and robust response to cyber threats. One example is Sierra Leone, who recently adopted a national cybersecurity strategy developed in consultation with local and international stakeholders.

Between 2018-2021, Global Partners Digital (GPD), with financial support from the United Kingdom Foreign, Commonwealth and Development Office (UK FCDO) and in collaboration with other international implementers, supported the process of developing Sierra Leone's national cybersecurity strategy. On the ground, the process was led by the Ministry of Information and Communications (MIC). This article aims to share the experience and lessons learned from developing Sierra Leone's national cybersecurity strategy with the GFCE and the broader cyber capacity building community to inform future cyber capacity building and policymaking efforts..

Background and Sierra Leone's CMM

The process goes back to 2016, when Sierra Leone underwent a cybersecurity capacity review (best known as a "CMM") carried out by Oxford's Global Cyber Security Capacity Centre and the International Telecommunication Union. The final CMM report highlighted the need for Sierra Leone to develop a national cybersecurity strategy, with one of the recommendations being for Sierra Leone to "Embark toward developing a National Cybersecurity Strategy to set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. This strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives."[1] With the strategy being a clear priority to improve its cyber maturity and resilience, Sierra Leone's MIC got to work.

In 2018 Sierra Leone joined the GFCE and started liaising with GPD, a UK based civil society organization whose aim is to support cyber policymaking processes to make them more open, inclusive and transparent, and its policy outcomes more rights respecting. With support from a cybersecurity consultant from the region, GPD delivered several activities in partnership with MIC, aimed at developing the strategy with local stakeholders' input. For example, GPD and the Ministry co-convened a civil society training workshop in December 2019 to build the capacity of civil society groups to enable them to engage in cyber policy discussions, and the strategy development process in particular. Subsequently, in March 2020 GPD and the Ministry convened a multistakeholder workshop to increase awareness among stakeholders on cyber policy issues, gather information on the landscape, increase coordination, and provide a space for stakeholders to discuss their priorities and inform the process of NCSS development. Shortly after, the COVID-19 pandemic hit worldwide and as a result, in-person meetings had to be put on hold. Despite being unable to host in-person workshops, MIC continued working on the strategy and, in February 2021, they convened a validation workshop with over 80 representatives from different stakeholder groups to gather their feedback on the revised drafts of the National Cybersecurity Strategy and Policy and discuss priorities and roles in the implementation. The Strategy and Policy documents were adopted by the Cabinet in March 2021.

It's important to note that, in addition to the strategy, Sierra Leone had also been working on other cyber efforts, such as undergoing a National Cyber Risk Assessment (NCRA) supported by the UK Home Office, receiving pro bono strategy, policy and technical cybersecurity advice from Templar Executives, and receiving support from Council of Europe's GLACY+ project on cybercrime. Given the different initiatives going on, the informal "Friends of Sierra Leone" group was created through the GFCE's Clearing House Function. In this regard, the GFCE played a crucial role in providing a platform for implementers supporting Sierra Leone to stay informed and coordinated. In addition, different

Figure 1. Multistakeholder workshop participants, March 2021.

GFCE events presented opportunities for the different implementers to meet with each other and with the Sierra Leone Government.

As a result of project efforts, the strategy development process featured strong multistakeholder engagement and contributed to a rights-based approach to cyber policymaking in Sierra Leone, as evidenced by a commitment to protecting and promoting human rights being featured in the strategy.

> "Sierra Leone's strategy reflects stakeholders' priorities, and the buy-in built through the consultations has the potential to make the implementation process smoother."

Lessons learned

Meaningful stakeholder input can lead to better informed policy

Cybersecurity affects a range of different stakeholders, many of whom have differing experience and areas of expertise on the subject. Much of this is unlikely to exist within government alone. Bringing different stakeholder groups' rich expertise into cyber policymaking processes can help foster a more accurate and evidence-based picture of the cybersecurity landscape, the possible implications of different policies being considered, and how best to engage with those other stakeholders during a policy's implementation. Sierra Leone's strategy reflects stakeholders' priorities, and the buy-in built through the consultations has the potential to make the implementation process smoother.

Ensuring coordination between the donor and implementer communities is essential

There are often numerous donors and implementers operating in a given environment with similar activities, and a lack of coordination mechanisms and measures can, for example, result in multiple events which seek to address similar issues and invite similar target groups. Insufficient activity coordination can therefore contribute to fatigue among local actors, risks stretching their capacity to engage and remain interested, and threatens local buy-in. Mitigation of this situation relies on deliberate coordination efforts by both donor and implementer communities to identify potential overlap, share information, and actively seek to avoid duplication. Mechanisms like the GFCE Clearing House can play a critical role in facilitating this type of coordination.

It's a marathon, not a sprint

Projects that seek to impact government policy processes in a sustainable way should take note of the average length of the policy process on the ground, as well as pandemic related delays. Short-term interventions are unlikely to be effective as they may fail to cover the full length of the process. This, compounded by the COVID-19 pandemic and restrictions related to curbing its spread, has the potential to introduce more delays that can affect project implementation. Therefore, flexibility in project timelines can contribute to project success.

Inclusive processes are themselves a way to build capacity

The value of stakeholder engagement extends beyond creating better policy outcomes and ensuring effective implementation– it also acts as a capacity building effort in itself.

Depending on the existing interest and capacity of local stakeholders, additional investment and efforts might be necessary to facilitate meaningful engagement and leverage the knowledge and expertise that stakeholders can bring to the process. The above-mentioned training workshop hosted in December 2019 illustrates this: the event was a way to increase awareness and build the capacity of civil society groups to be able to subsequently engage in the strategy development process.

Ministry of Information and Communications
National Multi-Stakeholder Validation Workshop
"TOWARDS AN INCLUSIVE CYBERSPACE: DEVELOPING SIERRA LEONE'S NATIONAL CYBER SECURITY STRATEGY"
Thursday 4th February 2021
Radisson Blu Hotel

Figure 2. From left to right, Permanent Secretary of the Ministry of Information and Communications of Sierra Leone, Mr. Kenneth Adu-Amanfoh, Hon. Minister of Information and Communications Mohamed Rahman Swaray, and Ag. Director of Communications Mr. Mohamed Jalloh.

"Sierra Leone's strategy reflects stakeholders' priorities, and the buy-in built through the consultations has the potential to make the implementation process smoother."

REFERENCES1

1. Page 17, Cybersecurity Capacity Review, Republic of Sierra Leone. Global Cyber Security Capacity Centre, Oxford Martin School, University of Oxford, and International Telecommunications Union. https://cybilportal.org/projects/cmm-review-sierra-leone/

BUILDING LOCAL PARTNERSHIPS HELPS YOUNG BATSWANA TO BE ‘CYBERSMART’

Written by: Cyber4Dev Communications Team

Established in 2018, Cyber4Dev, funded by the European Union, aims to support the capabilities of nations across the globe to formulate and implement strategies and campaigns that increase cyber resilience. To achieve this, our project works collaboratively with partners and stakeholder organizations across nine priority countries as well as our growing network of associate countries in Africa, Asia and the Americas. In response to an increasing number of socially engineered cyber scams aimed at young people, in October 2020 the Cyber4Dev worked in conjunction with local partners in the Republic of Botswana and embarked on a month long Cyber Hygiene campaign ‘CyberSmartBW’ with the aim of raising the awareness of the importance of good cyber hygiene.

Over the past decade, The Republic of Botswana has been on an accelerated drive to join the digital revolution. Adoption of digital technologies in various spheres of society has seen internet penetration in the country grow by over 600% between 2010 and 2020 and in an increasingly digitized world, the volume of cyber scams and hacks on everyday citizens continues to rise. Botswana is no different in this respect and with a young and growing population, the importance of supporting local efforts to inform and encourage strong and resilient cyber citizens has never been more important.

Developing a Digital First Cyber Awareness campaign

Like many countries, despite its growing digital connectivity, Botswana is still on a journey to expand its digital and cybersecurity awareness. Young people are particularly vulnerable to social engineering, scams and blackmail. Cyber hygiene teaching in schools is still limited and so far, the media has not picked up on the potential dangers of poor cyber hygiene.

In the ever evolving digital media landscape, where mobile devices are quickly becoming the dominant means of accessing information, the need to develop innovative and engaging content that can easily be shared online is paramount to the success of public awareness campaigns.

Many of the messages pertinent to the lives of young people also apply to those in other age categories. In devising a campaign that would be translatable to all age groups, it was therefore essential that digital content was carefully combined with traditional print and broadcast media, which continues to have broad national reach.

Working collaboratively with local stakeholders

Building connected networks has always been at the very heart of the work of Cyber4Dev. At the core of our work is the endeavor to mentor, support and encourage our partner countries to enhance not just their technical cyber capacities, but their ability to engage, encourage and build the cyber literacy of their citizens, enabling them to maintain strong cyber resilience in their everyday lives.

The project has been engaged in Botswana since 2018, working alongside the Ministry of Transport and Communications, the Botswana Communications Regulatory Authority (BOCRA), as well as local and regional stakeholders in support of Botswana’s efforts to further increase its cyber capacity.

Botswana has a number of niche organizations operating within the youth services space. As a project, we have observed the crucial role that local grassroot partners play in designing and implementing campaigns. Working alongside our experts Nick Small and Sylvia Beamish, the ‘CyberSmartBW’ campaign was implemented in collaboration with:

- **InFuture Foundation:** A non-governmental organization (NGO) delivering eBotho - a program dedicated to raising cyber awareness among young people.
- **Inspired Horizons:** A non-governmental, non-profit making youth organization which focuses on youth development and skills building through innovative education and capacity building.
- **Ministry of Transport and Telecommunications:** The leader of national Cybersecurity and Cyber Resilience programs and initiatives
- **Botswana Communications Regulatory Authority (BOCRA):** The telecommunications sector regulator providing oversight of the growing cyber environment

> “Just as we teach our children how to tie their shoes or ride a bike, we must also educate them about the risks of the internet and how to adopt safe online practices.”

The Campaign

CyberSmartBW was launched in September 2020 by the Deputy Head of the EU Delegation to Botswana, Silvia Bopp-Hamrouni who remarked;

‘Just as we teach our children how to tie their shoes or ride a bike, we must also educate them about the risks of the internet and how to adopt safe online practices. The CyberSmart BW campaign is designed to teach young people about both the risks of the internet, and the precautions they can take to protect themselves.’

The campaign ran along two parallel tracks; the first being a public information campaign including TV and radio broadcasts, online forums and a media workshop; the second being an interactive digital competition throughout October 2020.

Working with local influencer Zeus Bantsi and broadcasters in Botswana, a series of public information videos were developed aimed at increasing awareness of online threats and providing viewers with the tools to combat them. The videos provided tips on encryption, creating strong passwords, protecting social media profiles and securing networks.

Following tips from the public information campaign, young people were challenged to showcase their own creative flair and digital savvy through the creation of short two minute videos and social media posts aimed at educating their peers of the dangers of cyber risks, with prizes for the top four entries.

The competition asked entrants to consider -

Why cyber security is important to their lives?

How can they protect themselves from attacks?

Figure 1. Cyber Smart BW campaign logo.

The result? The competition garnered over 100 long listed entries, with young people from across Botswana presenting their view on ways to tackle scammers and build resilience.

The Impact

By design, the campaign was ambitious in its overall goal to start conversations about online safety and increase the cyber awareness of young people in Botswana. As lofty a goal as this was, judging from the response and engagement that the campaign received it was clear that engaging young people in serious conversations about their lives online was invaluable in enabling them to express their understanding of cyber risks, as well as enabling us to gather a true insight into their digital lives and the potential risks they are exposed to.

Why is this important for policy makers?

Creating campaigns with citizen participation at their core gives policy makers a rare insight into how cyber awareness, or lack thereof, can impact upon the lives of the people that policies are designed to serve. Working collaboratively with local expert practitioners, who work with young people directly, also allows for practical discourse to take place in a way that is relevant and meaningful to the target audience.

Galvanizing media interest

The topic of cyber security is often one that is veiled by a level of complexity meaning that it is often overlooked by the media. As part of the national promotional campaign, we were able to engage 35 local journalists at an interactive workshop which helped to demystify cyber scams, guided them on how to report about the threats at hand and thus enabled them to fully understand the public interest aspect of cyber security.

> "The topic of cyber security is often one that is veiled by a level of complexity meaning that it is often overlooked by the media."

Legacy and continuing to build momentum

Creating campaigns with citizen participation at their core gives policy makers a rare insight into how cyber awareness, or lack thereof, can impact upon the lives of the people that policies are designed to serve. Working collaboratively with local expert practitioners, who work with young people directly, also allows for practical discourse to take place in a way that is relevant and meaningful to the target audience.

Figure 2. Ambassador Jan Sadek with Selwana Motsemeng.

Lessons Learned

- Building partnerships– Recognizing that developing and maintaining cybersecurity and promoting cyber hygiene is a continuous effort, it is vital that a broad range of stakeholders are engaged and contribute– building a network of supportive partners. As highlighted in Botswana's National Cybersecurity Strategy, participation of civil society is key to reaching out into the community and promoting the importance of staying safe online. The campaign focused on this, establishing partnerships between the public sector and civil society organizations, and importantly, creating a network of CSOs that embraced the objectives of promoting cyber hygiene.
- Sharing experiences – At its very heart, the campaign was designed to provide a platform for young people to share their experience online and to use this to devise innovative messages regarding the importance of staying safe online. With their unique understanding of how they and their friends use the internet each day, which platforms they rely on, and what threats they are exposed to, campaign participants brought real-world knowledge to bear in developing promotional messages that resonated with the target audience.
- A Repeatable Solution – While the campaign was designed and developed specifically for Botswana, it can be a template for similar programs in other environments. The approach, tools and content developed, can provide a basis for jump-starting targeted campaigns to promote cybersecurity and cyber hygiene and, importantly, to help establish the much-needed cooperation and collaboration across sectors.

NOTES
For more information, visit:
www.cyber4dev.eu/botswana-cybersmartbw-campaign/

CYBERSECURITY AND THE PANDEMIC: THE IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIPS IN THE AFTERMATH OF COVID-19

Written by: Mariana Jaramillo, Cybersecurity Program Intern, CICTE/OAS

The COVID-19 pandemic has accelerated the reliance on digital platforms to perform daily and essential activities, making them increasingly susceptible to cyberthreats. According to the Unisys Security Index, since the beginning of the global pandemic, cybercrimes have increased up to 74% in Latin America and the Caribbean (LAC). These cyberthreats are increasingly becoming more sophisticated and complex, outpacing both the governmental and private sector's ability to respond, but represents an opportunity to handle cybersecurity challenges jointly and face them as a shared responsibility. The devastating effects of the pandemic on the region call for the need to reinforce and revise cybersecurity Public Private Partnerships (PPP) as an approach to address shared threats.

The Road to Recovery – PPP in the Cyber Pandemic

Strengthening cybersecurity is a determining factor in the advancement of LAC's digital transformation. The impact of the pandemic on digitalization has increased world spending in the cybersecurity industry, with a forecast amounting to US$54 billion by 2021. However, according to the OAS-IBD 2016 Cybersecurity Report, the financial damage caused by cybercrime in Latin America and the Caribbean represents more than US$90 billion per year, amounting to nearly 1.6% of the region's GDP and 9.5% of the current cost of cybercrime worldwide. This has undeniably been exacerbated due to the pandemic-driven vulnerabilities of the "new normal." Contrary to the assumption that underfunding in cybersecurity is a significant factor for increased threats, the primary reason for successful cyberattacks is often the sectors' isolated response to constantly evolving cyberthreats. Considering the complexity and interconnectedness of the cyberspace, no sector can address regional cybersecurity alone.

The benefits of collective action in cybersecurity are evident in a highly interdependent cybersecurity landscape. Particularly, cyberthreat intelligence sharing regarding attackers and their associated methods, enables organizations to better prepare for and respond to risks. Building on the premises of collective response to cybersecurity, information exchange contributes to trusted and transparent partnerships. Consequently, information sharing is commonly perceived as one of the most valuable commodities in industry-government partnerships, despite being a challenging element to achieve. In the public sector, the hesitation to exchange information can mainly be attributed to the factors associated with protecting national security when sharing more classified and sensitive information. At the same time, companies, may be concerned with the confidentiality and protection of their data maintained by the public sector. Nonetheless, an increasing trend shows governments and industry alike recognize that mutual information exchange is within national security interest, as threats can significantly damage both sectors.

Coordination is particularly vital when it comes to protecting critical infrastructure. Globally, 85% of critical infrastructure is privately owned. In Latin America, private investment in critical infrastructure is 56%, whereas 44% is attributed to public investment. Given the proportionately equal investment of both sectors, protecting national assets is an intertwined interest. Meaningful collaboration in a PPP is perceived to rely on articulating mutual benefits and value propositions within this context.

The benefits of PPPs go beyond information sharing. Partnerships have the potential to respond to cyberthreats, as well as adopt more proactive approaches to cybersecurity. PPP is shown to be optimal for building cybersecurity capacity to close the gap of notorious cyber breaches in the region. An effective PPP cybersecurity framework can create an environment that protects and nurtures innovation.

> "The likelihood of a PPP succeeding is commonly observed to be based on the existence of a robust framework, entailing defined principles, inputs, and expected benefits by both the government and industry"

Recommendations for Partnership Success

Public-private cybersecurity partnerships must continuously adapt to effectively respond both reactively and proactively with the necessary agility to combat the dynamic environment of cyber threats. The likelihood of a PPP succeeding is commonly observed to be based on the existence of a robust framework, entailing defined principles, inputs, and expected benefits by both the government and industry.

The European Union Agency for Network and Information Security (ENISA) has identified the following recommendations to mitigate any potential collaboration discrepancies and ensure effective PPP evolvement:

- **Open Communication:** As both sectors have specific expectations, compromise is usually required. Clear and honest communication is vital to establish pragmatic and stimulating common expectations.
- **Reciprocity Approach:** The discouragement of a partnership is commonly driven by hesitation and disinterest from both partners. Cultivating active participation through resource and knowledge sharing should be at the forefront of discussions and activities.
- **Legal Basis:** Cybersecurity is highly interdisciplinary, involving many entities from both sectors. Thereby, developing a legal basis in the form of a national legal act or a memorandum of understanding can consolidate a coordinated framework.
- **Inclusion of SMEs:** Many SMEs provide third-party services to large and critical service providers. The involvement of SMEs and startups in PPPs can increase their experience, cybersecurity capacity and drive for innovation.
- **Point of Contact:** Commonly, multiple public bodies are involved in PPPs, such as the Ministry of Defense, Ministry of International Affairs and Ministry of Economy. Appointing a government point of contact that coordinates public entities' efforts is fundamental to ensure coherent communication internally and with the private sector.

Figure 1. Cybersecurity Innovation Fund 2020 banner..

> “In 2019, the OAS and Cisco created the Cybersecurity Innovation Councils in Latin America, a space for multi-stakeholder collaboration, which aims to provide solutions to the cybersecurity gaps and risks faced in the region.”

Cybersecurity Innovation Councils: How the public and private sectors can enhance alternate cybersecurity solutions in the region

In 2019, the OAS and Cisco created the Cybersecurity Innovation Councils in Latin America, a space for multi-stakeholder collaboration, which aims to provide solutions to the cybersecurity gaps and risks faced in the region. The initiative represents joint effort between the public and private sectors to democratize and improve cybersecurity capacities in Latin America through education, dialogue, and support to civil society stakeholders.

As a continuity of the partnership, and with the added support of the Citi Foundation, the Cybersecurity Innovation Fund was created. The fund, endowed with US $200,000, seeks to foster innovation in the execution of projects that can develop local cybersecurity solutions in the context of the COVID-19 pandemic. The first edition of the fund demonstrated the region’s talent, as 117 nominated projects from distinctive sector organizations participated. The proposed projects are segmented in eight categories related to cybersecurity: education and awareness, critical infrastructure, capacity development, national agencies and public policies, cybersecurity innovation for small and medium-sized enterprises (SMEs), digital crime, incident response mechanisms, and remote work.

A key component of this PPP is the capacity to enable the diversification of cybersecurity solutions through participation from the civil sector, which expands their scope with the inclusion of distinctive societal groups. Likewise, more than half of the winning projects have a gender and diversity approach in their leadership and expected project impact. The twelve selected projects are led by organizations based in Argentina, Brazil, Chile, Colombia, Mexico, and Uruguay. In a region severely affected by COVID-19, this Fund and, most importantly, the cybersecurity projects that were selected, show that talent can come from different sources and that through collaboration, they can be expanded to provide solutions to diverse cybersecurity challenges. A few of the selected projects include:

Cybersecurity Innovation Fund – Project beneficiaries examples		
Country	**Name of the Project**	**Project Description**
Argentina	NGEN	Programmable and configurable infrastructure software capable of supporting the management of security incidents in the scope of work of a CSIRT.
Brazil	The LGPD Data Hunter	Text mining software to identify confidential information stored on organization devices
Chile	Programing our Future	Basic cybersecurity training targeted for female teenagers.
Colombia	Hackers wanted	Initiative to strengthen technical and educational capacities in cybersecurity at EAN University.
Mexico	Interactive on Digital Security in Indigenous Language	Portal that provides recommendations on digital security for educators, children and adolescents, and parents of indigenous communities.
Uruguay	ModSecIntl	Portal that provides recommendations on digital security for educators, children and adolescents, and parents of indigenous communities.

Figure 2. Cybersecurity Innovation Fund, examples of project beneficiaries.

In an increasingly challenging digital environment, the protection of cyberspace requires collaborative action. Considering the dynamic and borderless nature of cybersecurity, public and private sector cooperation is vital to mitigate risks and strengthen capacities that adequately encounter regional vulnerabilities. The damages inflicted by cybercrime in Latin America and the Caribbean during the COVID-19 pandemic call for the expansion of amultistakeholder approach to cybersecurity. Policymakers and cooperation can leverage Public Private Partnerships as an effective instrument to reaching common agendas. The entrenched nexus of both sectors lies on a common goal: raise the level of cybersecurity for the security and economic prosperity of the region.

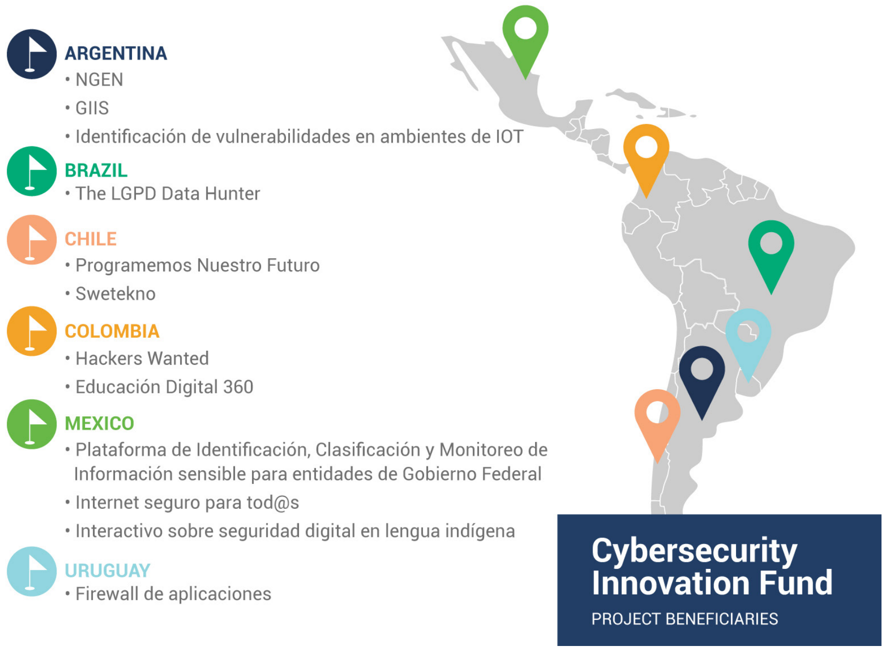

ARGENTINA
• NGEN
• GIIS
• Identificación de vulnerabilidades en ambientes de IOT
BRAZIL
• The LGPD Data Hunter
CHILE
• Programemos Nuestro Futuro
• Swetekno
COLOMBIA
• Hackers Wanted
• Educación Digital 360
MEXICO
• Plataforma de Identificación, Clasificación y Monitoreo de Información sensible para entidades de Gobierno Federal
• Internet seguro para tod@s
• Interactivo sobre seguridad digital en lengua indígena
URUGUAY
• Firewall de aplicaciones
Cybersecurity Innovation Fund
PROJECT BENEFICIARIES

Figure 3. Cybersecurity Innovation Fund, map of project beneficiaries.

WHY ARE CYBER PORTALS IMPORTANT FOR CCB?

—

Written by: Louise Marie Hurel, Digital Security Program Lead, Igarapé Institute

Cyber portals play an important role in assembling, communicating, and facilitating access to information about cybersecurity – helping policymakers, diplomats, civil society organizations, academia, and the private sector in making sense of the growing landscape of initiatives and policies. As different organizations develop international and regional portals, the Igarapé Institute has recently launched the Brazilian Cybersecurity Portal to map the country's national cybersecurity governance landscape. Louise Marie shares below some reflections on the importance of Cyber Portals to CCB and the lessons learned from the process of developing the national portal.

A complex landscape

—

From the Morris worm to the Colonial pipeline ransomware attack, the past 30 years have been marked by the increasing notoriety of both the vulnerability and interconnectedness of systems, networks and infrastructures. All sectors have not only witnessed but also increasingly sought to include cybersecurity as a key concern in technical and policy development. Internationally, discussions at the Open-Ended Working Group and the UN Group of Governmental Experts have revolved around the development and operationalization of cyber norms, in particular, the applicability of international law to cyberspace. Regionally, many organizations such as the OAS, OSCE and ASEAN have sought to work with member-states on the consolidation of cyber–Confidence Building Measures. Nationally, governments have been developing their national cybersecurity strategies and other policies that establish minimum standards for cybersecurity across sectors.

All these developments have contributed to what today is a rich and complex landscape of policies, standards, actors, projects, CCB initiatives, institutions, and spaces in which these discussions take place. However, amidst a growing patchwork of initiatives, policymakers, diplomats, civil society organizations, academia, and the private sector are faced with the challenge of keeping up with the growing field and navigating what has become a fragmented landscape of activities.

In response to this challenge, different organizations have started to develop a range of repositories and portals to aggregate, organize and make available information about norms and initiatives in a systematic and accessible way. Some examples are UNIDIR's Cyber Portal, the GFCE's Cybil Portal, OAS's Observatorio de Ciberseguridad and, more recently, the Brazilian Cybersecurity Portal (Portal Brasileiro da Cibersegurança), developed by the Igarapé Institute.

> "Cyber portals play an important role in assembling, communicating, and facilitating access to information about cybersecurity."

The rise of Cyber Portals

—

Cyber portals play an important role in assembling, communicating, and facilitating access to information about cybersecurity. They are both a resource for other sectors looking to understand and navigate some of the latest developments in the field and an important mechanism that can support organizations in planning their own capacity building efforts. Some portals focus on a thematic issue-areas and others on specific levels of analysis (national, regional, or international) or sectors. Rather than ideal types, there are some basic characteristics that enable portals to target and actively respond to knowledge gaps in cybersecurity. A few examples include:

Level-specific Portals: These are the portals that focus on mapping international, regional and/or national cybersecurity developments. UNIDIR's Cyber Policy Portal, for example, provides an extensive map of UN Member States' profiles and cyber policies.

Theme-specific Portals: Those that are dedicated to one or multiple thematic areas without the demarcation or explicit commitment to one specific level of analysis (national/regional/international). This is the case of Diplo Foundation's Geneva Internet Platform Digital Watch Observatory that monitors and provides an overview of issues that range from cybersecurity and human rights to economic and infrastructure-related ones. Another example is the GFCE's Cybil Portal that focuses mapping cyber capacity building initiatives and creating knowledge that can foster better targeted initiatives.

Repositories: Initiatives that are primarily dedicated to the consolidation of a digital archive for cybersecurity or presentation of the result of a mapping exercise. The National Security Archives Cyber Vault Library provides primary-source material that ranges from court case documents, to maps and glossaries. The OAS Cybersecurity Observatory is another example of a portal that has sought to periodically map cyber capacities and maturity across countries in the Americas region.

Building national capacities through Portals

—

In April 2021, the Igarapé Institute launched the Brazilian Cybersecurity Portal - one of the first portals fully dedicated to the mapping the national environment and discussion. The Portal gathers more than 70 documents and 100 national initiatives from 10 sectors, seeking to systematize and map the national cybersecurity governance landscape, that is, the key institutions, norms, and history of the field in Brazil.

In so doing, our objective was (and is) to (i) shed light on the particularities of cyber policy taking place in the national agenda, (ii) integrate knowledge from different sectors in developing their respective policies, and (iii) contribute to raising the baseline understanding of the current capacities and gaps for multistakeholder collaboration in national cybersecurity.

The Portal is the result of over two years of data collection and a series of interviews, consultations and meetings with experts from different sectors. More importantly, it is one of the responses to a diagnostic analysis of the national landscape in which we had identified that, while all sectors understand the importance of building cyber capacities and shared responsibility in doing so, there were some challenges for action, namely: (i) a lack of shared vocabulary to address cybersecurity threats and risks; (ii) existence of varying level of cyber maturity across sectors; (iii) lack of normative, strategic, and operational align-

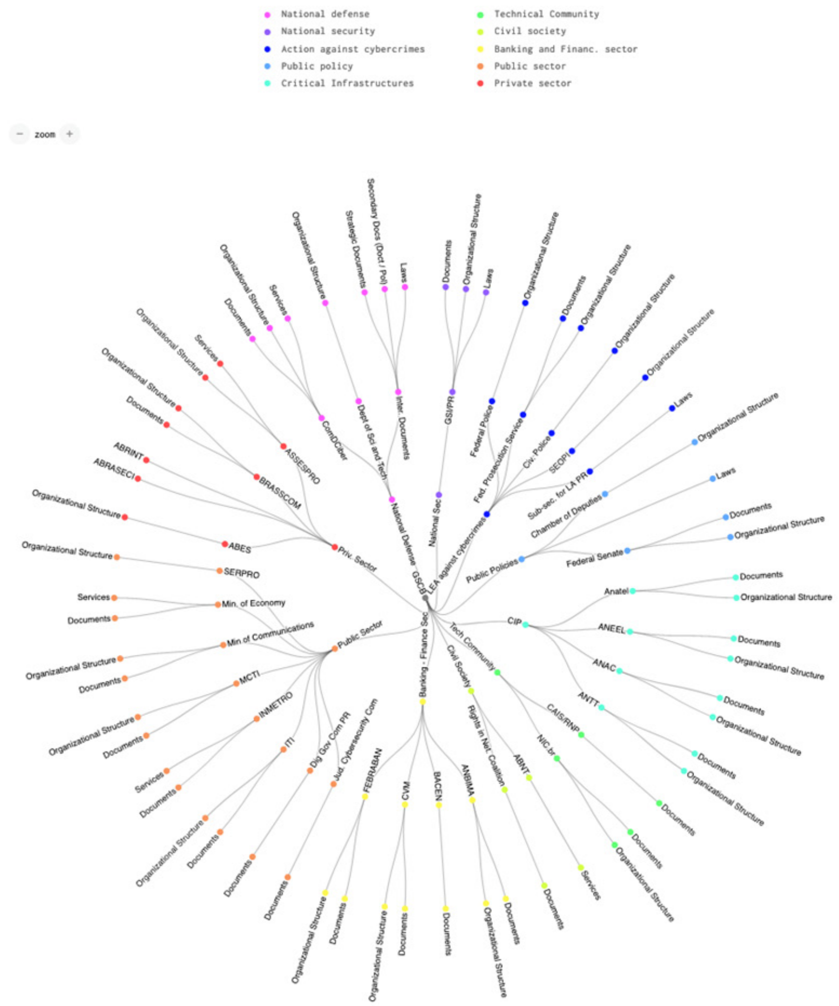


Figure 1: Mapping Brazil's Cybersecurity Governance Ecosystem // Source

ment; and (iv) different understandings of specific and shared risks across sectors – to name a few.

Portraying the national cybersecurity governance landscape can be a challenging task due to the fast-paced changes in regulation, the shifting and evolving institutions, and the sometimes-blurry lines between concepts such as cybersecurity, cybercrime, critical infrastructure protection and others. The Brazilian cybersecurity Portal responds to those challenges by providing a repository of legislations, policies and official documents; an interactive map of key actors (and what they have produced so far in terms of cybersecurity); a timeline of key developments; and recommendations for an integrated and multistakeholder approach to digital security risks.

> "More than a shared responsibility, cybersecurity requires consistent collective action – and Portals are one way of levelling the playing field of understandings."

A complex landscape

More than a shared responsibility, cybersecurity requires consistent collective action – and Portals are one way of levelling the playing field of understandings. By integrating knowledge and working on strengthening cyber capacities, they serve as an increasingly relevant tool for national and international policy development.

Academia and civil society organizations have an important role to play in developing and implementing CCB initiatives such as building repositories and facilitating access to knowledge, especially at the national level – as many of the examples in the sections above show. Many of these organizations are actively following cybersecurity debates in different sectors, continually work with primary open-source data, and engage with key experts in the field.

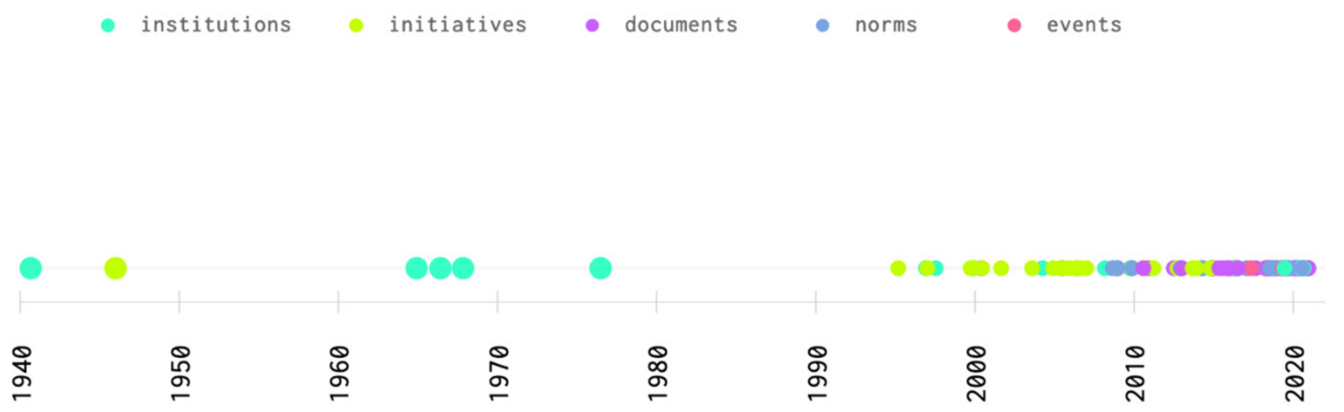


Figure 2: Cybersecurity Timeline in Brazil // Source

Finally, our experience in building a national portal and collaborating with other portal developers has shown that there are multiple benefits in consolidating knowledge that go well beyond facilitating access, such as:

Mapping existing policies and what has already been achieved. Especially at the national level and in developing countries, it might seem that cybersecurity is a relatively new subject. What we found is that this is not always the case – Brazil, for example, has only launched its national cybersecurity strategy in 2020, but has engaged in the subject since the early 2000's at least.

Identifying gaps in policy and institutional development. By gathering policy data in a systematic and methodologically rigorous manner, we were able to understand some trends in policymaking across the years – such as the securitization and militarization of the cybersecurity agenda from 2008-2016 and an increasing push towards sector specific regulations and data protection and security since 2018.

Translating how cybersecurity is framed within a specific country. Beyond international documents, national data allows for different sectors to better understand how cybersecurity is approached in a particular country and/or region. Some governments have concentrated the development of a national cybersecurity agenda to the ministry of economy, others to the ministry of defense, tracking these developments allows for a better positioning of the debate within these national realities.

Going beyond the 'usual suspects' or cybersecurity experts. Depending on the portal, it can serve as an important hub for both experts working in the field, but also to students, policymakers and others that might not be acquainted with cybersecurity.

Last, but certainly not least, portals can also be **an invitation for sectors to contribute to collectively building knowledge on cybersecurity.** All sectors have an important role to play in providing information and jointly building what is a holistic account of national capacities, policies, and institutions. NGOs and think tanks can meaningfully contribute to the discussion and development, ensuring that mapping efforts are reflective of human rights, provide greater transparency over cybersecurity policy and integrate a human-centric approach to new initiatives.

THE ASEAN-SINGAPORE CYBERSECURITY CENTRE OF EXCELLENCE (ASCCE)

Written by: : Ka Man Yip, Head of Capacity Building Programs, Cyber Security Agency Singapore

Cyber capacity building serves an effective tool, not only to strengthen our collective cybersecurity posture, but also enable countries to contribute meaningfully to international discussions, which is a key step towards achieving security and resilience in cyberspace. The Association of Southeast Asian Nations (ASEAN), as a region, has recognized the importance of coordinated capacity building at both the policy and technical levels. In the first ever ASEAN Leaders' Statement on Cybersecurity Cooperation issued in 2018, under Singapore's ASEAN Chairmanship, ASEAN Leaders tasked relevant Ministers to closely consider and recommend feasible options to coordinate regional capacity building. It is with these guiding principles that Singapore established the ASEAN Cyber Capacity Program (ACCP) in 2016, which was subsequently expanded with the establishment of a full-fledged ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in 2019.

Importance of Cyber Capacity Building

Cybersecurity is both a transnational and multi-disciplinary issue which requires international partnerships and cross-regional cooperation. The current pandemic has emphasized our increasing dependence on the digital domain. This dependence has been accompanied by increased risks and vulnerabilities. As the cybersecurity threat landscape continues to evolve rapidly, our discussions on this matter have to progress in tandem and achieve tangible outcomes. We cannot afford to have a break in momentum and need to continue with cyber capacity building as it is an effective tool to forge international cooperation to ensure an open, secure, stable, accessible, interoperable, and peaceful ICT environment.

As clichéd as it may sound, we are only as strong as our weakest link. The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare for and respond to cyber threats. There is a global consensus on the importance of cyber capacity building in ensuring a more secure and stable cyberspace as illustrated in the Final Substantive Report of the United Nation Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security. Capacity building will not only strengthen our collective cybersecurity posture, but also enable countries to contribute meaningfully to international discussions, which is a key step towards achieving security and resilience in cyberspace.

Singapore believes that in order to be effective, cyber capacity building should be a shared responsibility and reciprocal endeavor amongst various stakeholders. Cyber capacity building programs should also be sustainable and politically neutral so as to effectively address the needs of a diverse set of countries in the long-term. In addition, a coordinated capacity building effort is needed to minimize overlaps and ensure resources are channeled to areas where they are needed most. To this end, taking a regional approach to capacity building is useful as it allows for sharing of experiences when dealing with problems relevant to the region. This also helps to build and strengthen the network of officials dealing with cybersecurity issues who assist one another during times of need.

Figure 1. ASCCE office.

What Singapore is doing and the ASCCE

It is with these guiding principles that Singapore established the ASEAN Cyber Capacity Program (ACCP) in 2016. In response to the positive feedback from our partners in the region and beyond, and with a view of better coordinating and delivering our cyber capacity building programs, the ACCP was expanded with the establishment of a full-fledged ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) in 2019. The ASCCE which was set up with a commitment of SGD$30 million (approx. USD$22.5 million) continues to support a coordinated build-up of cyber policy, operational and technical capacities amongst senior ASEAN officials.

The ASCCE has three principal functions. First, it conducts research and provides training on national cybersecurity strategy, legislation and cyber norms. Second, the ASCCE provides Computer Emergency Response Team (CERT) training, focusing on technical CERT-related skills as well as the exchange of information and best practices related to cyber threat and attacks. Lastly, the ASCCE also partners with academia for a Cyber Range to deliver virtual cyber defense training and exercises to participants for practical hands-on experience.

To date, we have organized 18 distinct capacity building programs on topics ranging from cybersecurity strategy, norms, Confidence Building Measures (CBMs), international law, to CERTs and incident-response related skills. In total, we worked with 7 governmental partners and more than 22 non-government partners from the industry and academia to deliver these courses to over 700 participants across all 10 ASEAN Member States (AMS).

"Regional organizations have risen to the challenge, and many regions now have dedicated cyber capacity building initiatives. ASEAN, as a region, has recognized the importance of coordinated capacity building at both the policy and technical levels."

Challenges to Cyber Capacity Building

The last decade and a half has seen a rise in global awareness on the importance of coordinated international cyber capacity building efforts in building a secure and stable international and regional cyberspace. Regional organizations have risen to the challenge, and many regions now have dedicated cyber capacity building initiatives. ASEAN, as a region, has recognized the importance of coordinated capacity building at both the policy and technical levels. In the first ever ASEAN Leaders' Statement on Cybersecurity Cooperation issued in 2018, under Singapore's ASEAN Chairmanship, ASEAN Leaders tasked relevant Ministers to closely consider and recommend feasible options to coordinate regional capacity building.

However, challenges remain. There have been increasing calls for better coordination of international and regional cyber capacity building efforts so as to ensure that global resources are maximized and efforts are not duplicated. There have also been calls for global repositories and portals where information on capacity building activities can be made available, so that the international community can identify synergies and build on them to better coordinate our global efforts for a more collaborative and sustainable approach to cyber capacity building.

The Cybil Portal established by the GFCE is a good initiative that has enabled us to tap on the rich exchanges of cyber capacity building initiatives which help foster public-private partnerships and optimize resources. Closer to home, the ASCCE strives to work with AMS, ASEAN Dialogue Partners as well as our colleagues at the ASEAN-Japan Cyber Capacity Building Centre (AJCCBC) in Bangkok in supporting the call of our Ministers and Senior Officials in raising regional cyber capacity through offering complementary capacity building programs on cybersecurity policy, operational and technical topics.

Figure 2. ASCCE office.

Future of Cyber Capacity Building

We also need to acknowledge that limiting ourselves to only identifying capacity building needs is insufficient. We will need to develop metrics to measure the effectiveness of cyber capacity building programs, so that timely adjustments can be made to the content and delivery of programs and ensure their value and effectiveness. This will ensure that the resources committed to capacity building are prudently used and maximized.

Singapore sees the importance in measurable outcomes of cyber capacity building programs so as to ensure the effectiveness of these programs as well as the effective channeling of resources to address these capacity gaps. In this regard, Singapore is working on a metrics framework to measure the effectiveness of the various initiatives that we are running under ASCCE. Using the ASCCE curriculum as a test-bed, we hope to share with the wider international community on how they can apply the metrics to their programs as well.

Besides the metrics development, the ASCCE's focus for the next 2 years also includes our work with UNODA on the development of a Norms Implementation Checklist. The Checklist will be a simple guide for a set of actions that developing countries could take to implement the 11 voluntary norms of responsible state behavior in the 2015 UN GGE report. It will also identify the capacities needed to help nations implement such norms. Together with UNODA, Singapore will work with partners in ASEAN to help developing countries implement these norms under the United Nations-Singapore Cyber Program (UNSCP) workshops.

Lastly, alongside with the COVID-19 pandemic and an always changing cyber and digital landscape, we have seen an acceleration of a growing overlap between cyber and cyber adjacencies such as data and supply chain security and disinformation, as well as emerging technology issues such as AI, Quantum Computing and Cloud. There is a need for cyber capacity building to address these new gaps as we have also been receiving feedback and interests from AMS on capacity building around such issues. As the ASCCE is demand driven, we are looking to delve more into programs which will more tightly link policymakers with the operational aspects of cybersecurity, as well as programs on securing digital technologies and cyber adjacencies.

As we gradually move toward a post-COVID world, it would also be useful for the GFCE community to start considering these cyber adjacencies and how it would impact the future trajectory of cyber capacity building. Given the GFCE community's diversity, perhaps it is timely now to consider moving discussions beyond the traditional definition of cybersecurity and onto the wider digital domain for a truly holistic, multi-disciplinary and multi-stakeholder approach to capacity building.

"It would also be useful for the GFCE community to start considering these cyber adjacencies and how it would impact the future trajectory of cyber capacity building."

THE CMM IN THE PACIFIC

Written by: Dr. James Boorman, Head of Research and Capacity Building, OCSC

The Melbourne conference with the Pacific family seems like a distant memory. The COVID-19 pandemic will have long-lasting impacts. No community has escaped untouched. In the Pacific family, the islands who have been fortunate enough to have no cases are still impacted. The world has changed and our daily routine with it. Building digital resilience for the new 'normal' is a global priority that requires a multi-dimensional approach, looking beyond IT. The CMM review process is a useful step on the digital resilience journey, helping partner nations to understand where they stand now and the next steps to take. The OCSC continues to work with the Pacific family, our partners and the GFCE community to coordinate online CMM reviews. We look forward to being part of capacity building projects that meet partner nation's identified priorities, are tailored to the local context, and deliver sustainable capacity with impact.

Melbourne a distant memory

Melbourne, May 2021. Australia, the 'lucky country' - a saying that rings true more than ever today. Another day working from home and chatting with our Pacific friends and colleagues over coffee, instant messaging, and webcam with an island backdrop that reminds us all of different times. Was it really February 2020 when we all last met at the OCSC hosted Global Cybersecurity Capacity Building Conference and GFCE regional meeting in Melbourne? The Melbourne meeting with the Pacific family seems like a distant memory.

COVID-19

In February 2020 we could move freely, chat during coffee breaks or over lunch and dinner, and bid our friends farewell at the end of the conference before they flew home. In March 2020 the World Health Organization declared COVID-19 as a pandemic, initiating social distancing and the closing of borders. The COVID-19 pandemic is an ongoing disaster, with immense and long-lasting impacts across public health (physical and psychological), communities and the regional and global economies. No community has escaped untouched. In the Pacific family, the islands who have been fortunate enough to have no cases are still impacted by the necessary pause in international travel and the knock-on delays for imported goods and supplies.

Figure 1. The CMM review in the Federated States of Micronesia was part of an APT Expert Mission and in coordination with World Bank for the Digital FSM Workshop.

Building digital resilience for the new 'normal'

The world has changed and our daily routine with it, making us even more reliant on the digital environment at a pace that no one was prepared for. For many, recovery from the impacts of COVID-19 will be more about rapidly adapting to this new way of life rather than returning to how things were before. Digital transformation is here to stay and along with it the demand for equitable access to digital technology within a safer and more secure environment which protects human rights, information, and national infrastructure.

Building digital resilience requires a view beyond IT. It necessitates comprehensive planning, robust and extensive infrastructure, and sufficient resources to develop and implement national strategy and policy that considers: the local culture; attitudes toward digital technology; building awareness; enabling access to education and professional training; regulation and legislation; and practices and technical controls to prepare for, detect, respond, and recover from incidents.

> "For many, recovery from the impacts of COVID-19 will be more about rapidly adapting to this new way of life rather than returning to how things were before."

Where to start?

The Cybersecurity Capacity Maturity Model for Nations (CMM) was developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. The CMM considers cybersecurity to comprise of five dimensions, which together constitute the breadth of national capacity that a country requires to deliver effective cybersecurity. The five dimensions cover: cybersecurity policy and strategy; encouraging responsible cybersecurity culture within society; building cybersecurity knowledge and capabilities; creating effective legal and regulatory frameworks; and controlling risks through standards and technologies.

The CMM review process is a useful step on the digital resilience journey, helping partner nations to understand where they stand now and the next steps to take regarding the development

Figure 2. A snapshot form the Tuvalu online CMM review.

or revision of their national plans. To this end, in 2020 a formal and independent evaluation of the CMM's impact with countries who have undergone reviews found that the review process was foundational to the country's strategy and policy development.

Working with the Pacific Family

Since 2018 the not-for-profit Oceania Cyber Security Centre (OCSC) has had the privilege of working closely with the Pacific family in Samoa, Tonga, Vanuatu, Papua New Guinea, Kiribati, the Federated States of Micronesia, and Tuvalu. Where possible the OCSC works in coordination with the capacity building community, including partners such as the ITU, APNIC, Asia-Pacific Telecommunity (APT), and World Bank.

The OCSC has been engaged with the Pacific family face-to-face since 2018, including: hosting a Pacific panel for the Asia Pacific regional IGF in Vanuatu; working with the community to start to map regional initiatives to raise awareness of existing efforts, avoid duplication and facilitate further collaboration at The Asia Foundation and APNIC foundation event in PNG; discussing regional challenges at the APT Policy and Regulatory Forum and APT Symposium on Cybersecurity and Samoan Government hosted Digital Pacific Conference; updating mapping efforts at the GDP workshop in Fiji; and hosting the Melbourne events. Throughout the pandemic we have continued to engage remotely, informally and formally, through regional panel discussions, workshops, and wargames via events hosted by several organizations: The Asia Foundation and APNIC foundation, ITU, APT, Samoan Government, George C. Marshall European Center for Security Studies, Daniel K. Inouye Asia-Pacific Center for Security Studies, UNDP, and the GFCE.

The last face-to-face CMM review in the Pacific was conducted in January 2020 in collaboration with APT as part of an Expert Mission at the invitation of the Department of Transportation, Communications, and Infrastructure (TC&I), National Government of the Federated States of Micronesia (FSM). Through coordination with TC&I and the World Bank, stakeholders from all four states of FSM were able to participate in a three-day consultation process following the Digital FSM Workshop held on the 27 January 2020. Through the Digital FSM Project, FSM's digital transformation journey is well underway. The CMM review is helping FSM to prioritize the next steps they want to take, with the OCSC and partners continuing to support FSM on their chosen journey towards digital resilience.

> "Collecting data across the different dimensions of the CMM from multiple sources enables the research team to build up a rich picture of the local strengths, priorities, challenges, and opportunities toward contextualized recommendations for next steps."

The remote CMM

Although the pandemic has disrupted this work, the response has accelerated the need for digital resilience. The Tuvalu Ministry of Justice, Communications and Foreign Affairs (MJCFA) has a vision for Tuvalu to actively participate in the global digital economy, not just consuming content but also creating it in the form of digital goods and services. In March 2021, the OCSC had the honor of being invited by the MJCFA to work with them on their journey towards digital resilience by conducting the first ever remote CMM review in the Pacific. The remote review enabled the OCSC team to work with the MJCFA at least 12 months earlier than expected, with international travel bans currently in place.

The CMM review process relies on extensive desk research, analysis of unpublished documents provided by participants and discussions in-country with decision makers and technical leads across 10 or more sessions to gain insights from the private sector, public sector, and civil society. Collecting data across the different dimensions of the CMM from multiple sources enables the research team to build up a rich picture of the local strengths, priorities, challenges, and opportunities toward contextualized recommendations for next steps. The team often find that the act of bringing people together in the same room for these discussions is itself a capacity building activity, with the discussions amongst participants flowing on beyond the focus group sessions over coffee or lunch.

With no COVID-19 cases in Tuvalu, the focus group participants were able to meet face-to-face in-country, while the OCSC team joined via video conferencing. This enabled the participants to step away from their desks or day jobs and benefit from having the time to engage and network with colleagues within the focus group and beyond. Over four days, the team engaged with more than 30 key stakeholders from: emergency response, criminal justice and law enforcement, education and civil society, critical infrastructure, government, and parliamentarians. The outcome of the review process will be a detailed report to the government with specific recommendations on next steps to strengthen existing capacity toward a safer and more secure cyberspace for all Tuvaluan citizens.

Where to next?

The next Pacific CMM review is planned with our friends in the Cook Islands. The OCSC team continues to work with the Pacific family, our partners and the GFCE community to coordinate future reviews, joint missions, and capacity building. We look forward to being part of projects that meet partner nation's identified priorities, are tailored to the local context, and deliver sustainable capacity with impact.

The team await the opportunity when we can all meet again and say Bula; Talofa; Malo e lelei; Halo; Ko na mauri; Kaselehlie; Mogethin; Ran annim; Len wo; Kia Orana; iokwe; Ekamowir Omo; or Alii.

The not-for-profit Oceania Cyber Security Centre (OCSC) in Melbourne is formed by eight Universities in Victoria, Australia with substantial funding from the Victorian Government.

EU CYBERNET – SAME KID, NEW AND LARGER BLOCK

Written by: Siim Alatalu, Director, EU CyberNet

EU CyberNet, the EU's external cyber capacity building network introduced in GCEM issue 6, has recently been granted an extended mandate with new tasks. With the CynAct platform now online and regular events taking place for the cyber security experts enlisted in the network, the project is to launch a new competence center for the Latin American and Caribbean region as well as to reach out to the EU Delegations worldwide. Siim Alatalu, Director of EU CyberNet, explains why this would be a good time to get involved.

A year in the 'American mountains'

It has been about a year since the Global Cyber Expertise Magazine's issue 6 in spring 2020 featured an article introducing EU CyberNet as the 'new kid on the cyber capacity building block'. Little did any of us reading it know of what was to follow? Needless to say, the pandemic changed a lot on the global cyber capacity building scene, posing new challenges for both the various projects as well as the increased teleworking bringing cybersecurity to limelight around the world. No doubt, it was a real rollercoaster, or as we call it in Estonian – 'American mountains'; as in order to stick to the work plans, creative thinking became useful. However, by December 2020, we had two more surprises waiting.

Having led the project for a little over a year, we received two major decisions from the European Commission. First, EU CyberNet was included in the new EU Cybersecurity Strategy whereby the EU is to leverage EU CyberNet's expertise in implementing the cyber capacity building related parts of the strategy. Secondly, the European Commission proposed to extend the project by two years and added tasks that were to take EU CyberNet's activities to a new level. The new tasks are to train the entire network of EU Delegations in cyber security capacity building and to provide lead support in establishing a regional cybersecurity competence center in the Dominican Republic that would cover the entire Latin America and the Caribbean region.

> "In the context of cyber security, the countries in Latin America and the Caribbean are important partners for the EU."

Why Latin America and the Caribbean?

In the context of cyber security, the countries in Latin America and the Caribbean are important partners for the EU due to their ambition to digitalize their societies and achieve better preparedness to counter cyber incidents, as well as the existence of shared values between the two regions in general. However, as was highlighted in the 7th issue of the Global Cyber Expertise Magazine, there are also several areas where EU-funded cyber capacity building initiatives could be of particular value.

Cyber attacks on critical infrastructure continue to increase in frequency and venture into new areas. Just to highlight the most recent cases, the Colonial Pipeline attack in the United States or ransomware attacks such as the one against the health sector in Ireland inter alia indicate the need for the inclusion of such threats in nation-wide risk management . In addition, a regional approach is essential. Not only would it mean developing regional capabilities, but also building uponthe routine of collaboration and sharing of information, which is ever more important in the ever more connected cyberspace. Thirdly – there can never be an OSFA (one size fits all) label on countries when it comes to cybersecurity maturity – as cyberspace realities evolve, so should legislation, policies and initiatives.

The levels of cyber resilience and the general awareness in Latin America about cyber threats differ from country to country. Few have established rules for the cyber defense of critical infrastructure or an effective partnership between the state and the private sector. Cyber exercises are rather rare and practical collaboration between the continent's countries are often not as close as, for example,in the EU. At the same time, the region has a booming ICT sector and some governments have taken the pandemic as an opportunity to revise and redefine what cybersecurity means. EU CyberNet and its growing network of experts can therefore become a practical tool for the various EU projects that are already active in the region.

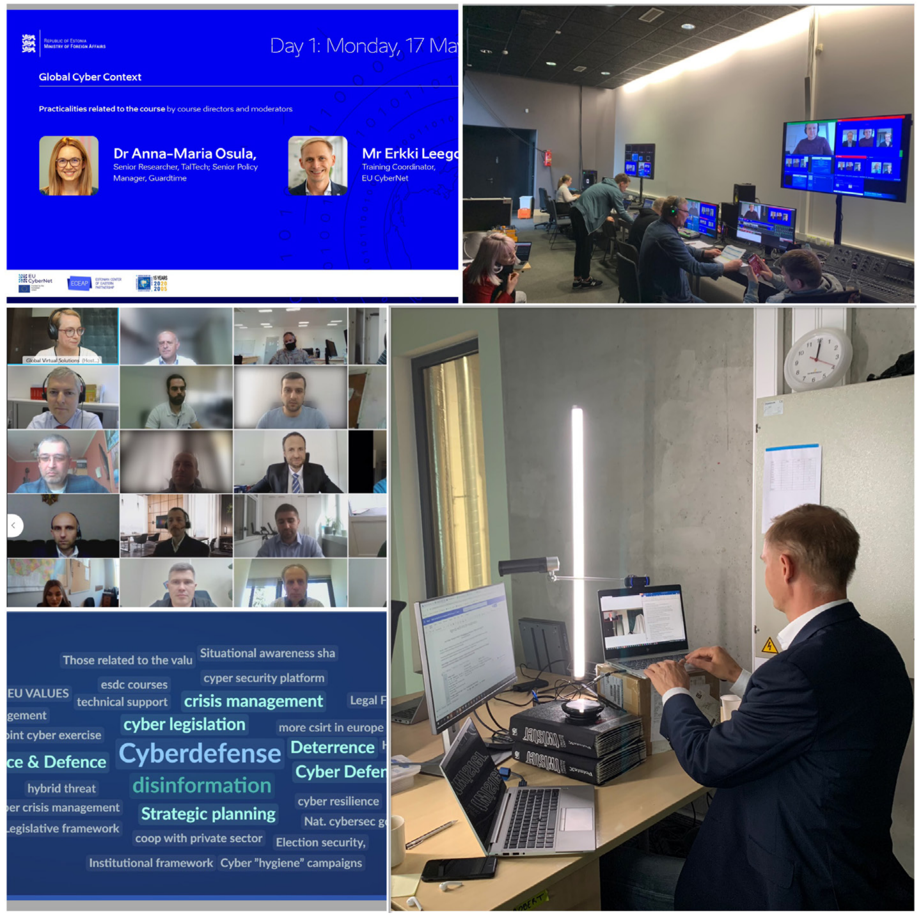


Figure 1. Collage of the various backstage scenes of our 1-week online EU Cyber Ecosystem course in May.

Figure 2. A moment captured during the 'Ciber Llamas' exercise in the Dominican Republic.

What is a regional cyber competence centre?

Spearheaded by the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia in 2008, the number of regional cyber centers has continued to grow. For example, in 2019 Singapore created a regional cyber center, the ASCCE, for fostering cybersecurity in the ASEAN countries. There are at least two similar initiatives in Africa. So far, Latin America and the Caribbean does not have one and this presents the EU and RIA with a great responsibility.

An international and regional organization cannot be established overnight. Fortunately, EU CyberNet can leverage both its host nation's know-how - Estonia has the unique experience of initiating and developing the NATO CCDCOE - as well as that of an international group of experts who on time for this issue of the Magazine have completed a feasibility study on the future center.

The implementation plan foresees that the regional center in Santo Domingo should achieve initial readiness by the end of 2021. Negotiations with the Dominican Republic authorities concerning the location of the center's facilities are already ongoing. Our goal is to create maximum synergy with the original tasks of the EU CyberNet, i.e. the establishment of an international network of experts and organizing trainings. Therefore, we see the conduction of trainings as an essential part of the center's activities.

Preparations for the first engagements in this area are ongoing. In cooperation with the Cyber4Development project on May 19 we supported the Dominican Republic authorities to conduct a cybersecurity exercise "Ciber Llamas". In the coming years, the center should develop into a regional hub that covers the full range of cybersecurity needs of the regional participants, similarly to how EU CyberNet is to furnish the full range of needs of the EU. Reaching out to regional experts and building capacity will be a key functionality of the center that will support its long-term sustainability

Building sustainable bridges in cyber security expertise

EU CyberNet's expert pool today covers many areas of expertise, making it possible to support raising awareness of cyber security matters in general and to strengthen links between governments, academia, and the private sector. In March we launched our online technical platform CynAct that will allow the stakeholders of the network to inform experts of their upcoming missions and find potential contributors. Further development of the platform will continue in 2021-22.

In May 2021 another important milestone was reached when we launched the monthly online EU CyberNet Club event series – an expert-to-expert forum where experts can learn from and discuss with other members of the EU CyberNet community of various issues happening on the cyber security scene today. Over the coming months we aim to cover topics that touch upon the full span of cyber security, from strategic to technological issues, and from operational to legal and regulatory issues.

The task of providing cyber capacity building related training to EU delegations are targeted at well-versed experts in the delegations that can act as reliable and knowledgeable partners in the cooperative effort of cyber capacity building. In cooperation between the EU, the host nations and cybersecurity experts can be supported in order to prevent the critical infrastructure of the countries from falling victim to hostile activity as this could start a cyber crisis with global implications.

In the end, however, the sustainability of our activities depends on the people. EU CyberNet is already open for EU experts to sign up as members of the network. If you know, for example, how to carry out sectoral and/or national strategies, increase institutional capacity, prepare laws that respect human rights, defend the critical information infrastructure, organize the work of CERT, or build international cooperation networks, please check out our website: www.eucybernet.eu/expert-pool. The past couple of months have seen rapid growth in the opportunities for experts to become involved in different activities of the network. Therefore the best time to join is now.

> "EU CyberNet's expert pool today covers many areas of expertise, making it possible to support raising awareness of cyber security matters in general and to strengthen links between governments, academia, and the private sector."

GENDER EMPOWERMENT IN CYBER: GFCE WOMEN IN CYBER CAPACITY BUILDING NETWORK

Written by: Giouli Lykoura, Advisor, GFCE Secretariat

With women representing less than one-quarter of the global cybersecurity workforce, a growing need has become increasingly visible in recent years: networks among women in the field. We needed toaddress existing global and regional challenges, promote the participation of more women in STEM and cybersecurity professions and secure a diversified cyber workforce. To address these needs within the GFCE Community, the Women in Cyber Capacity Building (WiCCB) Network was launched in 2019 during the GFCE Annual Meeting in Addis Ababa by Ms. Carmen Gonsalves, GFCE Co-Chair and Head of International Cyber Policy at the Ministry of Foreign Affairs of the Netherlands.

Added value of the WiCCB Network

Today, despite the growing demand for cybersecurity professionals, women are underrepresented in the global cyber workforce and still face a variety of challenges that prevent their inclusion and advancement in the field. To tackle these challenges, there is a need to promote, encourage and support women's participation in the field of cybersecurity. In pursuit of these objectives, female professionals need to be able to connect with others globally, share experiences and challenges, promote best practices and create awareness .

It was for this reason that the GFCE Women in Cyber Capacity Building (WiCCB) Network was launched in 2019, by Ms. Carmen Gonsalves GFCE Co-Chair, during the GFCE Annual Meeting in Addis Ababa: to facilitate and coordinate a strong, inclusive and growing network of female professionals in cybersecurity and cyber capacity building who can learn from each other and raise awareness on capacity building issues, encouraging the inclusion and empowerment of women in the field.

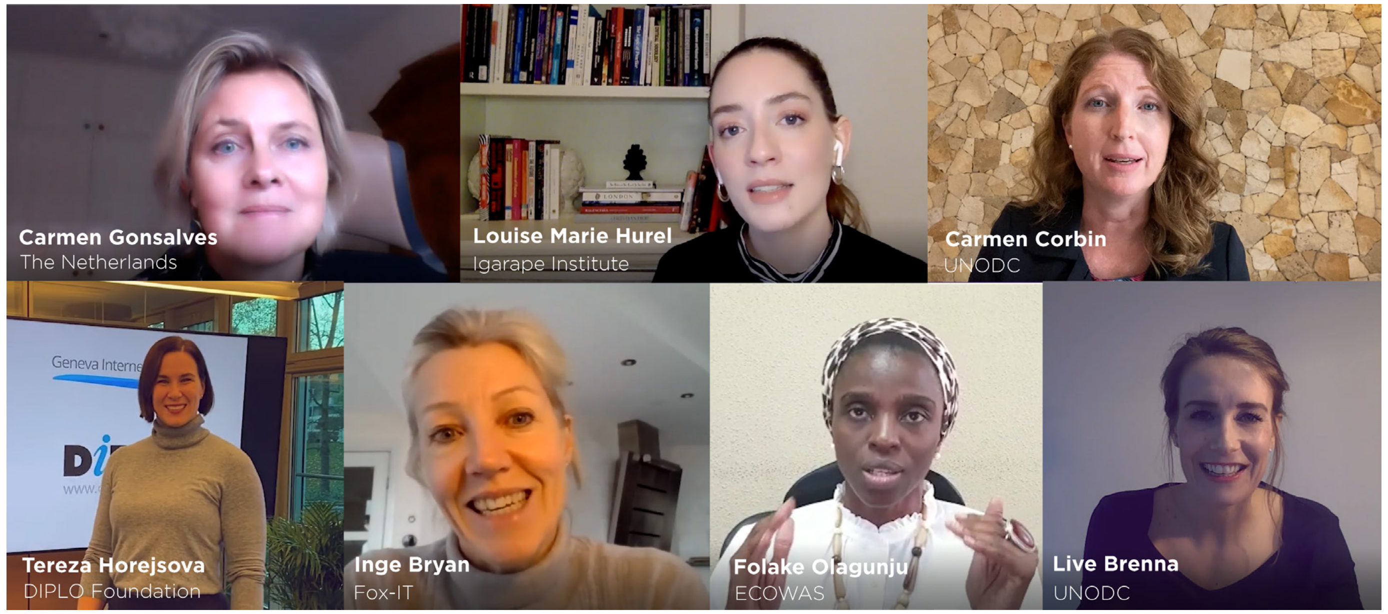


Figure 1: Colleagues from the WiCCB Network during the GFCE Annual V-Meeting 2020.

With more than 100+ female professionals in the GFCE community from different cyber backgrounds, the Women in Cyber Capacity Building Network plays a positive role, helping women feel included and supported, addressing challenges, identifying key success factors, and increasing their involvement in cyber capacity building. To support the network's mission, the GFCE aims to enhance the following:

1. Cooperation and knowledge sharing among women involved in cyber capacity building;
2. Identification of women's cyber capacity needs on a regional level;
3. Growth of a trusted community of cyber experts building a diversified workforce;

> "Female professionals need to be able to connect with others globally, share experiences and challenges, promote best practices and create awareness."

Bringing the Network together

Over the past year, the GFCE organized virtual meetings to bring the WiCCB Network together; the 'Women in Cyber Capacity Building' online meeting in May 2020 was dedicated to celebrating women globally by sharing achievements, experiences and discussing the added value of the network. A second session followed for 'Empowering the GFCE WiCCB' (read report: page 6) during the GFCE Annual V-Meeting 2020 which focused on identifying opportunities for collaboration within the network. In March 2021, a first regional session on "Breaking the regional barriers to empower women in cyber capacity building" took place, as part of the GFCE-OAS Meeting for the Americas, with female representatives from the LAC region discussing the main challenges women face in cybersecurity. In addition to such meetings, the GFCE is also encouraging knowledge sharing through tools, publications, projects related to gender which are uploaded on the 'Women' target audience group on Cybil Knowledge Portal.

Based on the input and active participation of our female colleagues, the GFCE WiCCB Network has managed to:

1. Enhance knowledge sharing on cyber capacity building challenges between women from different regions;
2. Provide the opportunity to demonstrate knowledge and expertise on different career paths in cybersecurity;
3. Allow the community to better understand regional needs and connect with one another;

What's Next

The GFCE has identified three pillars to enhance its efforts in supporting the WiCCB Network in 2021:

Coordination

The GFCE ***plays a coordinating role***, connecting female cybersecurity professionals across the world to collaborate, enhance knowledge and information sharing, create networking opportunities and develop regional and global meetings. The GFCE aims to further enhance collaboration between the WiCCB Network and other global or regional initiatives,platforms and processes , to better coordinate and strengthen efforts towards common goals for women in cybersecurity.

Regional Network Chapters

The GFCE will ***increase the regional focus of the network***, by identifying regional needs and challenges through regular consultations and collaboration with regional organizations. Regional needs and priorities will be discussed and identified on a variety of topics related to cyber capacity building, contributing to creating regional network chapters. This goal relates to the GFCE's efforts towards increasing its regional focus in 2021, setting regional perspectives and priorities for cyber capacity building.

Knowledge Module

In parallel to the creation of regional consultation sessions, and based on the findings of cyber capacity building needs per region, an online ***knowledge module*** on "Reducing the Gender Gap in Cybersecurity Leadership" will be developed, facilitated by the AU-GFCE Collaboration Project with a specific focus on the Africa region. The knowledge module, developed by the end of December, will highlight the importance of women in cybersecurity leadership and encourage the conversation on how to reduce the gender gap.

> "The GFCE aims to further enhance collaboration between the WiCCB Network and other global or regional initiatives,platforms and processes."

Outcomes 2021		
Coordination	Regional Network Chapters	Knowledge Module
• Database of global and regional initiatives for women in cybersecurity and capacity building; • Connect with other existing networks to avoid the duplication of efforts and explore opportunities for collaboration; • Formation of a GFCE WiCCB Ambassadors Group	• Formation of regional consultation roundtable discussions on key topics in cyber capacity building; • Creation of Regional Network Chapters to identify regional needs for women in cyber capacity building;	• Develop a training module to reduce the gender gap in cybersecurity leadership • Identify other topics on cyber capacity building to develop a series of training module for women;

Figure 2: Outcomes of WiCCB Network Work Plan 2021 .

Ms. Carmen Gonsalves' Testimonial

Since the launch of the WiCCB Network in Addis Ababa, I am heartened by the enthusiasm of many women in the GFCE community being involved in the network, actively supporting the need for women to connect and collaborate on cyber capacity building. Women are able to bring different perspectives, act as role models and make a real impact on international processes related to cyber capacity building. For this reason, we aim to increase the exchange of best practices, ideas and different point of views by organizing regular panel discussions and seminars, connecting with global and regional networks. Our female colleagues in the GFCE WiCCB Network have a broad spectrum of talent, skills, knowledge and expertise on cyber capacity building and that is the reason why we all ought to inspire and support the next generation of cyber professionals worldwide, building a diversified and inclusive network".

Looking ahead

In the coming years, the GFCE aims to empower the WiCCB Network and support global and regional efforts of women in cybersecurity and cyber capacity building, while continuing to look for ways to collaborate with other initiatives and bring greater awareness to those beyond the GFCE community to the network's mission and accomplishments. If you would like to connect with the WiCCB Network and join our efforts supporting diversity and inclusivity in the field of cyber capacity building, please get in touch with the GFCE Secretariat by emailing contact@thegfce.org

RETHINKING CYBERSECURITY CAPACITY BUILDING: HEALTHCARE SHOWS THE WAY

Written by: Stéphane Duguin, CEO, The CyberPeace Institute

In the course of the past twelve months, we have seen exponential growth of criminal attacks, massive disinformation campaigns and systematic attacks targeting the healthcare sector in particular. Paradoxically, the same period has also seen the emergence of evolving coalitions of individuals and entities allying in urgency to protect cyberspace as a common good. Despite the multiplication of assistance and capacity building initiatives, we still have little understanding of their impact on individuals and vulnerable communities. How can the complex jigsaw of initiatives and resource allocation be reconciled with sustainability and long-term impact, particularly in local contexts, where needed most? With the analysis and recommendations in its report Playing with Lives: Cyberattacks on Healthcare are Attacks on People' the CyberPeace Institute proposes a paradigm shift for cybersecurity capacity building based on an evidence-led approach prioritizing the involvement of all stakeholders, especially civil society organizations and empowering local communities.

The Importance of Cyber Capacity Building

In the course of the past twelve months, we have seen an exponential growth of criminal attacks, massive disinformation campaigns and systematic attacks. To tackle these threats and achieve a peaceful cyberspace, cybersecurity capacity building (CCB) activities are indispensable and the work of the GFCE is remarkable in this regard. As emphasized in the latest final report of the OEWG, to mitigate the malicious use of information and communication technologies, each State, and particularly in the developing world, should have the capacity to respond to cyberattacks and the major global risks they present to our societies, targeting notably vulnerable and stressed sectors and industries. In the current context, exacerbated by the COVID-19 pandemic, healthcare has been one of the most targeted sectors, accentuating the crucial need for stepping up capabilities, including via effective capacity building. As cyberattacks increased, amplifying the vulnerabilities created by the pandemic, the same period also witnessed the emergence of assistance efforts in the form of innovative coalitions. Individuals and entities are allying with the aim of protecting our common good by securing cyberspace, defending the health sector, bringing assistance to victims of extortion, protecting elections, and denouncing violations of our fundamental rights, among other urgent actions.

Assistance and capacity building are often complementary with fostering cyber awareness, cyber hygiene, and a more secure cyberspace. Despite the multiplication of such initiatives, we still have little understanding of their final impact, especially on individuals and vulnerable communities. One main challenge lies in the fact that building capacity, in the sense of building well-functioning and accountable institutions able to effectively respond to cybercrime and enhance countries' cyber resilience, comes at a cost often out of reach for the most vulnerable communities.

The CyberPeace Institute has documented the often shadowed societal impact of malicious activities against the healthcare sector. Building on the findings of this analysis, with this article, the CyberPeace Institute proposes recommendations for stronger cybersecurity capacity building based on an evidence-led approach and the empowerment of communities.

> "There can be no sustainable cybersecurity unless all communities can access cybersecurity and resilience programs."

Case Study: Healthcare as a vulnerable sector in need of reinforced preparedness and resilience

As the healthcare sector increasingly depends on digital, often converging systems and devices, it becomes increasingly vulnerable to attacks and malicious activities without having had access to the economic and organizational means required to build effective cybersecurity skills and resilience. Indeed, privacy and data breaches have populated the cyber threat landscape and given rise to a daunting convergence of cyberattacks against hospitals, research laboratories, non-governmental organizations and vaccination centers, further exacerbated by the spread of the COVID-19 pandemic.

Research on the economic impact of cyberattacks against healthcare abounds, but little to no research is currently available on the societal impact of those attacks and on the specific capacity-building needs of affected communities. Aiming to fill this gap, the CyberPeace Institute recently published a strategic analysis focusing on the societal impact on victims. The key findings show that as a vital human service and hence vulnerable sector, healthcare requires more effective cybersecurity capacity building measures as cyber threats take advantage of technical, societal and individual vulnerabilities.

Figure 1. Malicious activities against the healthcare sector often have a shadowed societal impact.

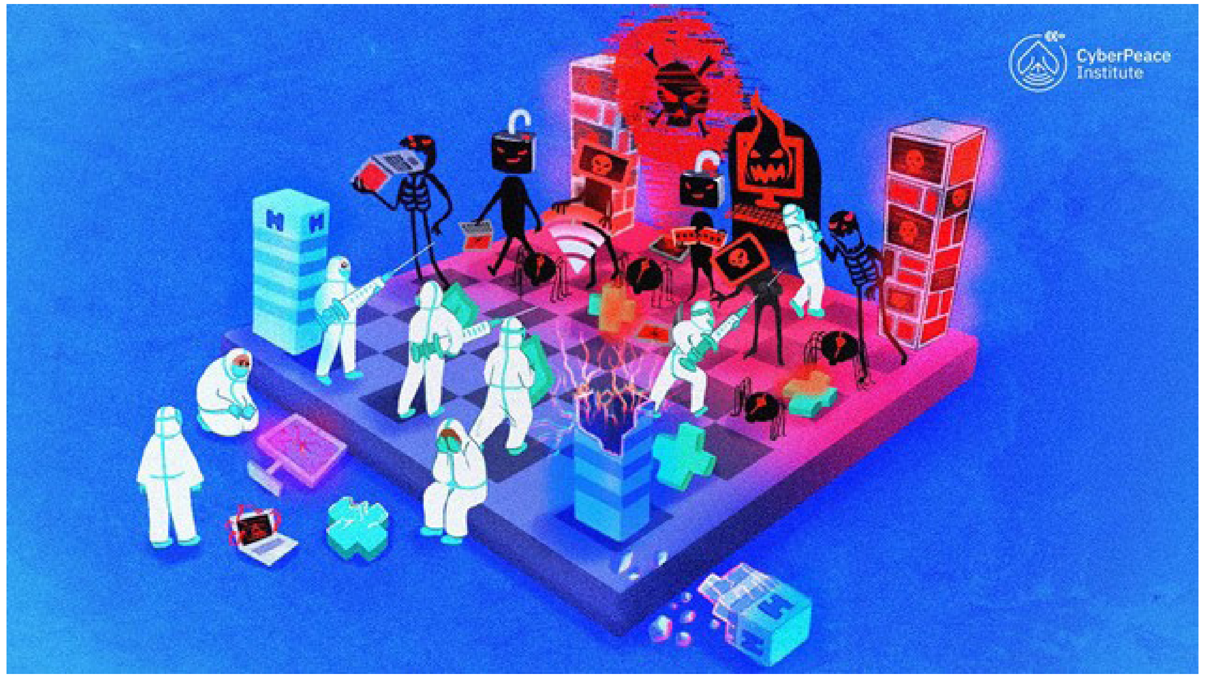


Figure 2. As the healthcare sector depends on digital systems and devices, it becomes increasingly vulnerable to attacks and malicious activities.

Cybersecurity capacity building strives to tackle these challenges by addressing the vulnerabilities of the technology in use, by creating stronger regulatory regimes and by promoting security best practices for end users. The first two fall within the macro-level of state actions and responsibilities. States are indeed expected to afford protection by declaring the entire healthcare as vitally critical infrastructure. This enhances information exchange and reinforces the enforcement of protection mechanisms under international law. The third aim is implemented at a more local level in accordance with contextual specificities to empower vulnerable communities. Our approach is based on practical, evidence-led analysis conducted in the healthcare sector. We are confident, however, that similar high-level considerations can also be applied to other critical civilian infrastructure sectors.

A Paradigm Shift for Cybersecurity Capacity Building

Cybersecurity capacity building activities seek to support and empower individuals, communities and governments by reducing security-related risks emerging from access and use of information and communication technologies. CCB is essential to fostering the development of skills, human resources, policies and institutions to increase the security and resilience of States directly, and indirectly, of all.

Too often, CCB has focused on providing top-down assistance at the national level through exchange of legal and administrative best practices, and providing access to technology with the goal of increasing national cybersecurity capacities. Such efforts focus primarily on the macro state level and fail to comprehensively capture and evaluate the complexity of the victims involved or the specificities and needs of vulnerable communities affected. Indeed, cybersecurity cannot be achieved without effectively empowering those communities that do not have the necessary means to access capacity building programs.

> “Capacity building activities must imperatively be available at the micro level of vulnerable local communities to have a more holistic and successful impact.”

By successful impact of CCB, we mean community-level change that creates value for and is acknowledged by beneficiaries and all others affected. In the realm of cybersecurity, such value can be translated into awareness, education, security, and protection at the national level. How can we measure the impact of cybersecurity capacity building on individuals and vulnerable communities? Research may index States' efforts and commitments to cybersecurity but the real impact remains unquantifiable. Therefore, while CCB improvement should be based on better coordination mechanisms among projects and initiatives, there is a pressing need to focus on quantifying the cyber resilience and cybersecurity maturity of local communities.

While there is almost global consensus that cybersecurity capacity building is necessary for the achievement of a safe and stable cyberspace, there can be no peace nor stability if victims and vulnerable communities are not systematically included in the solution. To achieve sustainable cyberpeace, cybersecurity capacity building activities must:

- **be evidence-led** and assess the specific needs of the reality on the ground and in context;
- **involve all stakeholders,** especially civil society organizations, in the documentation of attacks and in fostering accountability mechanisms;
- **involve people on the ground** to empower local populations and vulnerable communities.

The CyberPeace Institute has embraced the shift towards empowering vulnerable communities in its mission to address global challenges in the protection of critical civilian infrastructure. **At the CyberPeace Institute, we put individuals at the center, seeking to empower them for a more sustainable and long-term cyberpeace.** With an initial focus on the healthcare sector, the CyberPeace Institute has launched the Cyber 4 Healthcare program to assist healthcare professionals, analyze attacks and advance policies to protect the sector.

This is supported by a Call to Governments to join forces in the promotion of cyberpeace in the healthcare sector and the delivery of direct operational support to healthcare. The approach starts from the victim and builds knowledge and resilience around the specificities of the organization and the affected communities. The healthcare sector is the first focus area, other critical infrastructure sectors will follow. **As a chain is no stronger than its weakest link, cybersecurity capacity building activities must start focusing on empowering people to ensure successful, long-term impact that leaves no one behind.**

THE GFCE'S REGIONAL APPROACH

Written by: Kathleen Bei, Advisor, GFCE Secretariat

Over the last two years, the need for a regional approach in the GFCE has become undeniable. By increasing regional focus, the GFCE is able to more accurately identify needs, discover best practices, and amplify regional efforts to the global level; which is in line with its efforts to maintain a demand-driven approach to capacity building. 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.

GFCE's Regional Focus

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. The GFCE's ongoing efforts to bolster its regional focus is outlined in the Strategic Building Blocks document that was presented during the GFCE Annual V-Meeting last year. Some key milestones towards 2022 that are linked to these efforts include connecting and cooperating with regional organizations, organizing regional coordination meetings and increasing awareness of the GFCE.

> "A regional approach is favorable because countries within a region tend to share similarities in priorities and are seen to be able to reach a common understanding, agreement or way forward more easily than in other multilateral fora."

A demand-driven approach

Over the last two years, the need for a regional approach in the GFCE has become undeniable. A regional approach is favorable because countries within a region tend to share similarities in priorities and are seen to be able to reach a common understanding, agreement or way forward more easily than in other multilateral fora . Furthermore, a regional approach can be instrumental in improving regional collaboration and knowledge sharing amongst stakeholders in the region. In placing a greater emphasis on the regional approach, the GFCE aims to not only better understand and meet the regional needs and demands, but also to support the GFCE Community with bringing their expertise and know-how to the region. By increasing regional focus, the GFCE is also able to more accurately identify needs, discover best practices, and amplify regional efforts to the global level; which is in line with its efforts to maintain a demand-driven approach to capacity building.

> "As capacity building requires trust between implementers and the beneficiary community, to ensure sustainable and long-term impact, the GFCE is connecting and collaborating with regional organizations to support its regional efforts."

Collaboration with Regional Organizations

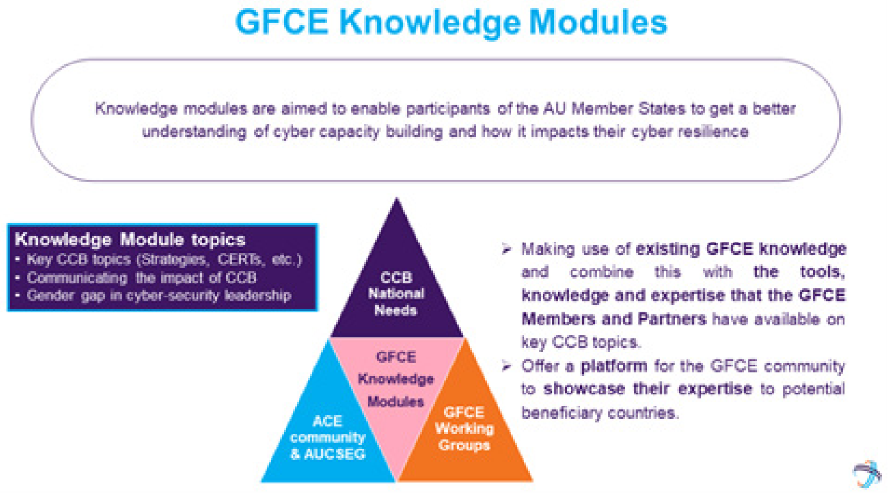
As capacity building requires trust between implementers and the beneficiary community, to ensure sustainable and long-term impact, the GFCE is connecting and collaborating with regional organizations to support its regional efforts. By doing so, the GFCE taps into platforms that have built long-lasting, trusting relationships with their respective member States, and that can help the GFCE tailor its approach in the respective regions. Many regional organizations also already have a clear overview of regional perspectives and capacity needs and can therefore work with the GFCE to translate them into specific activities to support capacity building. In turn, the GFCE is a valuable partner for regional organizations as it provides access to a global multistakeholder implementing network and a platform to share good practices and lessons learnt across regions. Furthermore, the GFCE aims to support existing regional organizations and structures in their cyber capacity building efforts to avoid duplication.

GFCE Regional Meetings and Engagements

The GFCE also plans to hold more regional meetings in 2021, to bring together relevant stakeholders (donors, implementers and beneficiaries) of the region to discuss, learn and find solutions to capacity building challenges. Through these regional meetings, the GFCE can fortify its coordination role, and more effectively match needs with offers for support. These regional meetings also increase the regional visibility and awareness of the GFCE and its work on cyber capacity building, and can lead to increased knowledge transfer to the region. Besides discussing capacity building needs, it is also important to gather stakeholders to share regional good practices and initiatives to promote greater knowledge-sharing. The entire second day of the GFCE Consultation Meeting 2021 is dedicated to regional meetings to give participants a better understanding of the GFCE's as well as its Member and Partner's efforts on a regional level. Read more about the GFCE's planned and ongoing efforts in the different regions:.

Africa

Following the success of the GFCE Annual Meeting 2019 and based on the input of the Community, the GFCE has given additional emphasis on its engagement in Africa. Many GFCE members and partners are interested in or already working on capacity building in the region, and the GFCE has extensive expertise and experience that would be valuable to share. In 2021, the GFCE Secretariat therefore welcomed two new members to the team – Mr. Moctar Yedaly and Dr. Martin Koyabe – to support its efforts through a two-tier approach. Mr. Moctar Yedaly is involved in outreach to new members and partners in the region, executing a GFCE-Africa Strategy in order to better coordinate capacity building efforts. Dr. Martin Koyabe is focused on the two-year AU-GFCE collaboration project which aims to expand African countries' cyber capacity building knowledge to better understand, identify and address their national cyber capacity needs. Over the two-year period, this project will map cyber capacity building priorities in the region, establish a multi-stakeholder Africa Cyber Experts (ACE) Community to strengthen knowledge sharing, and develop knowledge modules based on the expertise of the GFCE Community. These efforts will enable the GFCE to better understand and address the capacity building needs of African countries, enhance cooperation and knowledge sharing between stakeholders, and facilitate the GFCE Community in bringing their knowledge and expertise to the region through the GFCE Knowledge modules. Africa


GFCE Knowledge Modules

Knowledge modules are aimed to enable participants of the AU Member States to get a better understanding of cyber capacity building and how it impacts their cyber resilience

Knowledge Module topics
- Key CCB topics (Strategies, CERTs, etc.)
- Communicating the impact of CCB
- Gender gap in cyber-security leadership

➢ Making use of **existing GFCE knowledge** and combine this with **the tools, knowledge and expertise that the GFCE Members and Partners** have available on key CCB topics.

➢ Offer a **platform** for the GFCE community to **showcase their expertise** to potential beneficiary countries.

Figure 1. GFCE Knowledge Modules on key capacity building topics will be developed and delivered as part of the AU-GFCE project.

The Pacific

The GFCE Pacific Regional Meeting in February 2020, held in the margins of the OCSC-GCSCC Global Cyber Capacity Conference, was the GFCE's very first engagement in the Pacific region. During the meeting, donors, implementers and beneficiaries in the region came together to share perspectives and learn from each other's invaluable insights, highlighting the need for greater peer-to-peer sharing. A key takeaway from the meeting is that capacity building initiatives in the region were most effective when designed with an awareness of the local ecosystem and needs. In an effort to address the demands and needs that were discussed during the meeting, the GFCE appointed Ms. Cherie Lagakali as the first GFCE Pacific Liaison to conduct a comprehensive scoping assessment and explore how a GFCE Pacific Hub can best support and coordinate capacity building in the region while facilitating greater knowledge sharing. By appointing Ms. Cherie Lagakali, a local who can build relationships with those on the ground, the GFCE ensures that the needs of the Pacific are most accurately identified and will lead to a long-term solution that the Pacific community can be confident of. As of June 2021, the scoping assessment is now complete, and the next step is to validate the design options for a GFCE Hub with the Pacific Community Stakeholders.

Latin America and Caribbean

In collaboration with the Organization of American States (OAS), the GFCE held its first event on cyber capacity building in Latin America and Caribbean (LAC) in March 2021. The aim of the meeting was to introduce the LAC Community Stakeholders to the GFCE and demonstrate how the GFCE can support the implementation of cyber capacities. The GFCE-OAS partnership was formally announced during the meeting, with the OAS acting as the GFCE's regional hub in LAC and Ms. Kerry-Ann Barrett as GFCE-OAS Liaison. The GFCE-OAS Hub will be the linking pin between the GFCE Community and regional stakeholders, improving support and visibility to LAC while coordinating and enhancing knowledge sharing of initiatives, and functioning as a point of contact for various activities including the GFCE Clearing House.

Southeast Asia

Since the GFCE held its Annual Meeting 2018 in Singapore, the GFCE has sought to improve representation from the Southeast Asian region to better understand the needs of the region and the existing capacity building efforts. At present, four out of eleven ASEAN countries are already GFCE members. As plans to hold an in-person Southeast Asia regional meeting in 2020 fell through due to travel restrictions, the first GFCE Southeast Asia regional meeting was announced during the GFCE Consultation Meeting 2021. The meeting, organized in collaboration with Cyber Security Agency (CSA) Singapore, will take place in the margins of the Singapore International Cyber Week (SICW) in October 2021. As ASEAN member states have increasing placed an emphasis on cybersecurity and creating trust in information and communications technology (ICT) infrastructure, the GFCE is looking forward to strengthening engagement and better coordination of capacity building efforts in the region.

Europe

The GFCE held its first regional meeting in Lille, France in January 2020. During the meeting, the mapping of European capacity building projects on the Cybil Knowledge Portal was presented and discussed. Given that a large number of implementers within the GFCE Community are European or Europe-based, European stakeholders have pointed out the importance of active knowledge and expertise sharing, while focusing on addressing a country's capacity building gaps and weakness. The GFCE hopes to connect with other multi-stakeholder platforms and actors in the region to organize an in-person European meeting later in 2021.

Figure 2. Speakers at the GFCE-OAS Meeting for the LAC region presenting the GFCE Toolbox.

Volume 9, June 2021
Global Cyber Expertise Magazine

Colophon

Editorial Board:

Adil Sulieman (AU)
Georgiana Macovei (EU)
Belisario Contreras (OAS)
Kathleen Bei (GFCE)

Guest Editors:

Daniela Schnidrig
Cyber4Dev Communications Team
Mariana Jaramillo
Louise Marie Hurel
Ka Man Yip
James Boorman
Siim Alatalu
Giouli Lykoura
Stéphane Duguin

Artwork & Design:

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

Chief editors:

Kathleen Bei (GFCE)
Anna Noij (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 10 submission deadline:
10 October 2021