Volume 8, November 2020

GLOBAL CYBER EXPERTISE MAGAZINE

ENABLING CAPACITY BUILDING

KNOWLEDGE ACCESS AND SHARING ONLINE

- page 66 -

African Union

GFCE

OAS More rights for more people

Volume 8, November 2020

Global Cyber Expertise Magazine

Editorial

On behalf of the Editorial Board, I am pleased to welcome you to Issue 8 of the Global Cyber Expertise Magazine! As COVID-19 cases continue to soar around the world and we are unable to meet in-person as a global community, we have published this edition at our first ever GFCE Annual V-Meeting in a virtual conference venue.

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 edition, we see a number of articles addressing the impact of COVID-19 on digital transformation, cybersecurity and capacity building activities. As we begin to accept this new normal in the (post) COVID-19 era, governments and organizations are actively finding ways to overcome new challenges in this domain, such as shifting capacity building activities to the virtual space.

From Asia & Pacific, find out more about the GFCE Pacific Hub in an interview with our new GFCE Pacific Liaison. Learn more about CERT NZ's awareness campaigns and APNIC Foundation's projects in the Pacific and in Southeast Asia.

From Africa, read about how the GFCE is building on its collaboration with the AU to address cyber capacity needs in the region. An article on the OCWAR-C project gives insight on ECOWAS' collaboration with the EU to strengthen cyber resilience in West Africa and another article looks at protecting digital Africa.

From Europe, the European Commission shares how they went digital overnight as a result of COVID-19 and find out more about the National Cyber Security Index (NCSI). Also, learn about the impact of the pandemic on the cybercrime landscape and what this means for such capacity building projects.

From the Americas, the Organization of American States outlines how governments in the region are looking to revise and redefine their cybersecurity priorities in the wake of the pandemic and what 5G means for cybersecurity in the region. Mexico also shares their stance on cybersecurity looking at recent experiences and challenges ahead.

From the global development section, read about how Cybil Knowledge Portal can support your capacity building efforts, the impact of the Cybersecurity Capacity Maturity Model for Nations (CMM), and the GFCE's ambitions towards 2021.

We thank our guest writers for their valuable contributions to the eighth edition of the Magazine and we hope you enjoy reading the Global Cyber Expertise Magazine!

On behalf of the Editorial Board,

David van Duren
Director of the GFCE Secretariat

Interview

CHERIE LAGAKALI, GFCE PACIFIC LIAISON

Written by: GFCE Secretariat

In October 2020 the GFCE appointed Cherie Lagakali as its first regional Pacific Liaison, to lead the scoping and design of a new GFCE Pacific Hub. Cherie's appointment follows the outcomes of the GFCE's first regional Pacific meeting, held in Melbourne in February 2020. This regional meeting identified a need to strengthen cyber capacity building communication, coordination and knowledge sharing among Pacific Island countries, regional donors and project implementers.

As Cherie begins to engage the Pacific ecosystem on what and how a GFCE Pacific Hub can support the region, we took the time to talk to Cherie, hearing her thoughts on the cyber capacity building challenges the Pacific region faces and what overriding objectives a GFCE Pacific Hub will need to prioritize

Q: What challenges has and does the Pacific face when it comes to cyber capacity building?

A: I have been in this role for a month, speaking to stakeholders in the region about some of the difficulties the Pacific is facing on cyber capacity building and finding out where a GFCE Pacific hub could fit in. These discussions have identified that there is a continuing duplication of effort and a need for balance. For example, an organization frequently arrives in the pacific region to undertake cyber capacity building and then a week later another organization comes in to do the exact same thing. This can be exhausting for Pacific Island countries as it takes up a lot of resources and countries are caught between whether to commit or not, as the work is still seen as important.

Figure 1. Cherie Lagakali, GFCE Pacific Liaison.

> "There is a need for proper facilitation."

There is a need for proper facilitation. There are a lot of trainings in the region but these would be a hundred CERT 101 trainings –all the basics, while there is an actual need for mid-level and advanced trainings so that there is progress.

> "There has to be a balance."

Rather than making the Pacific a dumping ground of cyber capacity building projects, there could be proper coordination looking into what work an organization is coming to do, its priorities and where it could best align, based on the needs of the Pacific. This would ensure that the same work is not done over and over again and that there is a balance. This is important because in the Pacific, human resource is scarce, there are very small communities with only few people in the field and these are the people that end up being burnt out and exhausted because they have to do so many things.

Q: What must the GFCE carefully consider in designing and launching a new GFCE Pacific Hub? How do we make sure that we don't become part of the problem?

A: The GFCE must figure out a coordination and information sharing functionality for the Pacific. The GFCE could step in with its Clearing House function to be able to properly match the work that is being done in the Pacific, with Pacific needs. There must be a correct match and I'm hoping that this scoping process will find out what those needs are, what work organizations are doing and find the organizations that can come and fit in right away.

"Communication between the donor community and the needs of the Pacific is essential."

From the consultations, I am finding that Donors need to be communicating and collaborating amongst each other first as there are situations where one donor has its set of implementers coming to do one set of work, then the next week another implementer from a different donor comes in to do that same work. A Hub could coordinate the work between donors by having a list of donors, their implementers, their priorities and the needs in the Pacific and then match these.

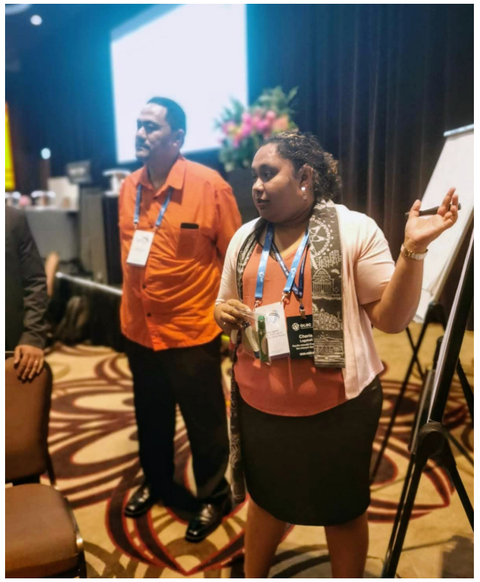


Figure 1. Cherie Lagakali at the GFCE Pacific Regional Meeting in 2020.

Q: How does the GFCE avoid your quote of being 'another actor in an already crowded field'?

A: As there is a lot of work being done in the region, the GFCE, as an organization from outside the region coming into the region, must have the buy-in of Pacific Island Governments. It will need to establish relationships and a level of trust. The scoping process is currently an introductory stage for the GFCE in the Pacific, outlining our background, role and offer of support for the region.

There is a lot of good work being done regionally as well as locally. The Samoa Information Technology Association (SITA) is doing community awareness and e-learning during COVID-19 , Tonga CERT is doing community awareness running workshops weekly. There is also Women in IT Solomon Islands (WITSI), IT Solomon Islands (ITSSI) and Tonga Women in ICT(TWiICT). PacSON is also running trainings, recently collaborating regionally with the CERTS on a Cyber Smart Pacific 2020 awareness program. The GFCE must establish relationships with these and other actors already operating in the Pacific. It will have to work out what they are doing, what their needs are and where it can enhance activity. In doing this, the GFCE will gain community support as well as country support, because it will have taken the time to understand and work with current national and regional initiatives and mechanisms.

Finally, the GFCE could aim to grow the role of the Cybil Portal and Clearing House function in the Pacific, enabling stakeholders in the region to gain access to updated lists of where and how work has been done, whether successful or not readily available for Pacific Island countries, as a reference aide to deciding what future projects to take on.

Figure 3. Pacific participants at the GFCE Pacific Regional Meeting in 2020.

Q: What do you believe to be the GFCE Pacific Hub's primary objective?

"The ultimate priority for the hub has to be by the Pacific and for the Pacific"

A: The ultimate priority for the hub has to be by the Pacific and for the Pacific. We are coming into the Pacific to do work with and for the Pacific so it would be good to have the Pacific's input. We have heard that there's a lot of scoping projects - Organizations come and take all the information from the Pacific and then go away. There is a need for continuity. To have the Pacific Island Countries communicating with each other (knowledge sharing). There is knowledge sharing within the different organizations and the networks that are already there, the GFCE hub will enhance it. The GFCE hub should not be bias to a particular implementer or donor because it is for the Pacific, the priorities for the hub need to be – the Pacific!

STRENGTHENING TECHNICAL COMMUNITIES IN APAC: EXPLORING NEW APPROACHES TO TECHNICAL CAPACITY BUILDING

Written by: Sylvia Cadena, Head of Programs, APNIC Foundation

Searching for better ways to build technical capacity in the Asia Pacific, the APNIC Foundation is exploring new approaches to add to the already strong technical content delivered, where a customized and evidenced based approach, rooted in community consultation processes and scoping, are key elements of training design and delivery. The APNIC Foundation is working on implementing two projects funded by the Australian government's Cyber Cooperation Program to strengthen this capacity through training and technical assistance, engaging with multiple stakeholders across different industries to capture local context while dealing with the challenges of a COVID-19 climate. However, there are still challenges to be faced and improvements to be made.

A fit for purpose approach

In over two decades, APNIC (Asia Pacific Network Information Centre) has learnt that technical content is only one element of building technical capacity for Internet network operators across the Asia Pacific. Increasingly, the ability to build confidence in people to tackle technical challenges and tailoring training delivery based on community needs (and targeting underserved groups) are as important, as demand for ubiquitous, faster, safer, reliable, stable and affordable Internet access grows.

Not all technical training is created equally. Vendor-provided training is often overly specific to particular hardware or software and directly linked to sales targets, meaning it often isn't offered to disadvantaged communities. Vendor-neutral approaches — advocated for by APNIC — help to make informed decisions, test other available options (including low-cost open source implementations) and guide the procurement process; however, they require a different business model.

There isn't yet a dataset that tells us how many engineers and technical staff work to plan, deploy, operate and maintain Internet networks worldwide, let alone in the Asia Pacific. We know the percentage of people connected per economy, we also know (roughly) that a skills gap exists and that there are enormous shortages in less developed economies for technically skilled network operators. It is also not very clear what the diversity challenges are that need to be tackled to make it more representative of the communities they serve, more inclusive and balanced.

Figure 1. Participants and trainers at the "PNGTRAINING WS # 9 - Information Security for System Administrators" workshop held in Lae, Papua New Guinea from 3-5 July 2019.

> "The ability to build confidence in people to tackle technical challenges and tailoring training delivery based on community needs (and targeting underserved groups) are as important [as [technical content] as demand for ubiquitous, faster, safer, reliable, stable and affordable Internet access grows."

The more we rely on Internet infrastructure, the more important having the 'right' technical capacity becomes for every organization and individual, especially as strong investment backing the deployment of submarine cables, satellites and other connectivity initiatives accelerates the digital transformation in developing economies.

An evidence-based approach

A one-size-fit-all approach to build capacity will not improve the Internet experience for the billions of existing users across the Asia Pacific while addressing the needs of those that are getting connected for the first time. In this changing and demanding context, it is evident we must have a better understanding of who, why, what for and how to deliver technical training and open minds to innovate and explore blended learning.

In collaboration with APNIC, the APNIC Foundation is working towards an evidence-based approach to tackle the development of technical capacity. Where community consultation and scoping are key elements of design and delivery, where learning pathways help technical staff progress in their learning, and virtual labs help them to simulate configurations and troubleshooting, to boost confidence in their practical skills to do live deployments.

A key element of the design of the community consultation is the engagement of multiple stakeholders across different industries, to capture not only the complexity of the local context and assess technical training needs but to also foster the buy-in of human resource departments, managerial staff and policymakers.

In that context, we are working on the implementation of two projects trying to address the issues raised above, by incorpo-

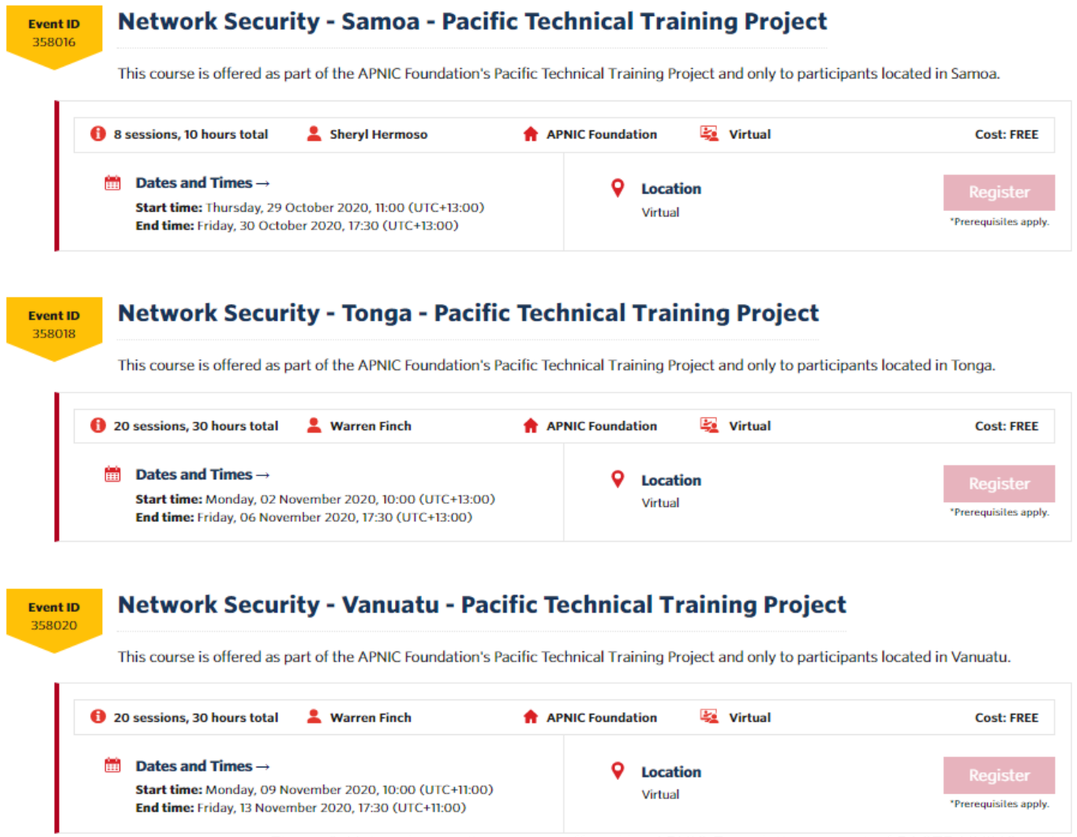


Figure 2. Network security courses offered by APNIC Foundation as part of PACTRAINING project.

rating community consultation and scoping processes to the planning and delivery. The projects are funded by the Australian government, under the Cyber Cooperation program and are expected to be completed by December 2021. These two projects represent over USD 600,000 in investment.

The Pacific Technical Training Project – PACTRAINING

The project team developed a Training Plan based on a detailed community consultation process conducted from August to December 2019, which involved a series of face-to-face interviews and an online survey for network operators (mobile operators and Internet Service Providers), universities, banks, government agencies as well as other organizations from the Solomon Islands, Tonga, Fiji, Vanuatu and Samoa.

This comprehensive plan is intended to guide future investments in technical training, as top priorities across seven technical topics were identified and opportunities to complete self-paced online courses using the APNIC Academy, attend webinars, practice using virtual labs and receive online technical assistance are made available.

The first event targeted the Solomon Islands community and took place from 19 to 23 October, focusing on routing with RPKI. A series of network security courses are scheduled for 2020 and more will come for 2021 for each economy.

SWITCH SEA: Fostering diversity and gender empowerment in technical leadership of the Internet industry in Southeast Asia

The project aims to improve the knowledge and skills of 100 women and LGBTQI+ technical staff working on Internet network management and operations in Viet Nam, Thailand, The Philippines and Cambodia. The project will use a gender responsive and inclusive approach to improve project participants' knowledge and skills across the following two areas and topics:

- **Network operations**: Internet routing; network security; crisis/disaster management; and research.
- **Leadership and professional development**: Project management; management skills; strategy and growth; negotiation; and public speaking

The project originally included face-to-face networking and training events, as well as fellowships that involved international travel. In response to the COVID-19 challenges, an updated project strategy will combine a range of online education, training and mentoring to support the ambitions of women and LGBTQI+ staff working in the sector and increase the visibility and recognition of their contributions to network operations research and development. The project will support 20 high-performing participants to receive additional support around technical research and publications.

The consultation process is ongoing. It involves identifying the 100 people that will join us in this adventure and co-create their training plans and support their professional development.

Impact of COVID-19

Before COVID-19, getting together at a training venue provided hours of interaction and engagement between trainers and participants, to get to know each other, and feel comfortable enough to ask questions about deploying improvements on their networks or network monitoring and analysis, while at the same time pushing trainers to learn more about the challenges that network operators experience in the field.

COVID-19 has disrupted implementation of these two projects, as online learning was initially conceived as a complementary part of the learning process. After a few months of review and adjustment project plans are now focusing on full online delivery.

There are many untested parts of that approach. We have many questions about what this change means and how can we learn and adapt.

Monitoring and evaluation mechanisms to learn from the different capacity building approaches each project has envisioned have gained a renewed and more critical role. Traditionally, the main focus of post-event surveys was on measuring satisfaction and effectiveness but integrating them with the consultation process also helps to understand better technical community needs in each economy in terms of skills, diversity, priorities, and preferred delivery mechanisms, in addition to local knowledge that may impact how effective the training actually is.

Will this fully online approach be fit for purpose, inclusive and effective? Will we be able to digest feedback quickly enough so that improvements can be incorporated, knowing what we know now about the additional costs, resources and time needed for a full online delivery?

But what type of motivation might be needed for participants to support the trainers and complete the prerequisites?

Will it possible to keep the energy and attention of participants during full-day sessions as the costs to accommodate half-day sessions almost doubles the commitment for trainers and will make delivery more expensive than face-to-face training? Will their connectivity support it? How will this work with the distractions of their daily job, or working from home demands, like children?

Will these online approaches strengthen collaboration among the community? Or are we losing sight of how we could support new and existing NOGs and other types of professional associations to continue to develop the Internet industry in each economy?

Many questions remain. We are open to learn and committed to improve on what we do. If you are based in any of these nine economies, join us for the ride and help us to make it work! For more information, contact foundation@apnic.net.

SUPPORT BUSINESSES TO OPERATE SECURELY ONLINE

Written by: Rob Pope, Director, CERT NZ

CERT NZ was established in 2017, with the aim of being a national CERT for all New Zealanders - businesses, organisations and individuals. As well as helping New Zealanders and businesses affected by cyber attacks, CERT NZ runs communication campaigns to provide everyday New Zealanders with information about the cyber landscape and how they can keep themselves and their businesses cyber secure. In response to the COVID-19 pandemic, in conjunction with New Zealand government agency Consumer Protection, CERT NZ launched the Trade Smart Online/Buy Smart Online campaign. The campaign promotes key actions to support more secure online transacting, to assist small-to-medium enterprises (SMEs) and consumers. With the first tranche completed, CERT NZ Director Rob Pope tells us more about the campaign, results and next steps.

A growing threat to business

In New Zealand, as was the case around the world, COVID-19 restrictions drove many businesses used to bricks-and-mortar trading suddenly online. Haste to create a website and get dollars in the door meant some were not taking the precautions they needed. In addition, the cyber security threat from attackers was increasing.

The challenge for CERT NZ was to act quickly to give businesses the tools to keep their data and finances safe online. Our experience with rapidly creating high profile campaigns targeting businesses has allowed us to learn a number of lessons which we are keen to share more broadly.

Scams and frauds proliferate during COVID-19

The alarm bells went off in the second quarter of this year, during the height of the COVID-19 lockdown in New Zealand. At this time, we saw a 229% increase in scams and frauds reported to CERT NZ from the previous three months. This shows a very real picture of opportunistic offending by criminals, taking advantage of businesses and consumers at a time of high stress and uncertainty. Buying, selling or donating goods online was the second highest type of scam or fraud in that category.

Overall across the first half of 2020, CERT NZ saw a 42% increase in reporting from the same period last year. Alongside anecdotal evidence from our engagements with banks, local chambers of commerce, key partners, and others, it was clear there is an urgent need to raise awareness of the risks amongst consumers and businesses, particularly as more

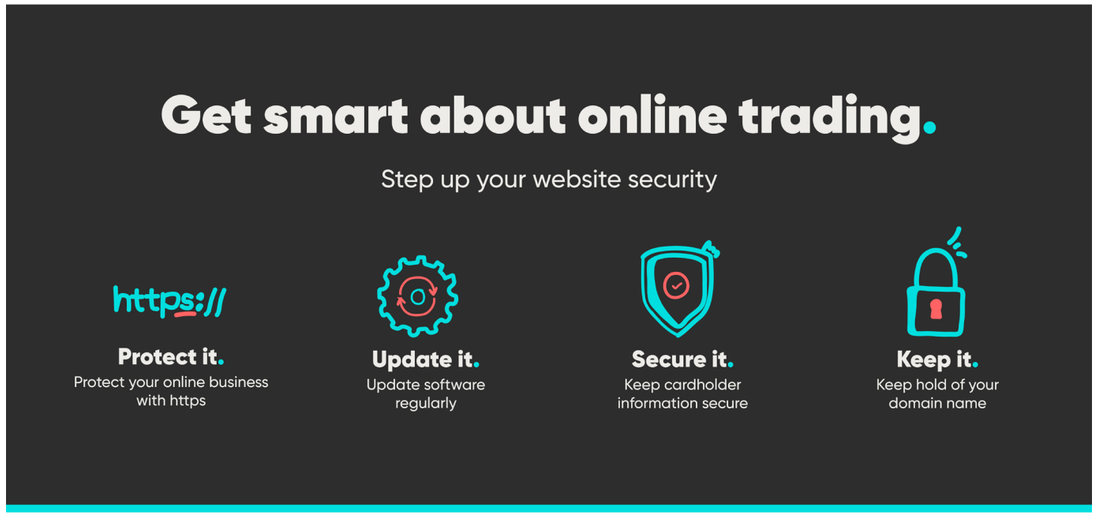


Figure 1. CERT NZ's Trade Smart Online campaign banner.

people grow their online presence, and many businesses set up online platforms for the first time.

In order to validate the reports we were seeing, we commissioned a survey amongst New Zealand small-to-medium businesses (SMEs), which gave us insight into how businesses were operating online and their levels of cyber security. The survey showed 46% of respondents already had a business website. More were in the process of setting one up or adding payment facilities. Around three-quarters of SME websites already collected or accepted some form of customer information.

Prior to Covid-19, 35% of online stores owners believed their website accounted for more than half of their turnover. This increased to 41% since the pandemic began. Despite the vital role websites play delivering sales, many businesses are not taking basic precautions to safeguard this important asset and their customers. While 83% of SMEs feel it's important to protect their websites from cyber security attacks, only 47% of those with websites have protective processes in place.

The campaign

We wanted to remind SMEs that cyber security needs to be prioritised as more online trading takes place, especially with the shift for many retailers happening so rapidly.

To bring about change we knew we needed to reach both businesses and consumers. We developed a joint Trade Smart/Buy Smart Online campaign with our colleagues at Consumer Protection, who have responsibility for consumer affairs in New Zealand.

We know the increased environment of trading online comes with risks and creates a need for business owners and their staff to understand these and to know how to reduce them. Most SME's don't have internal technical support and are reliant on third party providers. We understand the conflicting demands to maintain business operations while at the same time being faced with potentially expensive cyber security investment. Our approach has been to provide a level of assurance to business owners that good cyber security doesn't

need to cost the earth. However through a combination of awareness of key risks and maintaining a set of simple steps they are going a long way to protecting their livelihood and the interests of their customers.

With that in mind, the Trade Smart Online campaign focused on simple but impactful steps to securing the business's website. The key messaging had four calls to action for business website owners:

- Protect it – enable https to give the website added security and privacy.
- Update it – keep your software and devices updated.
- Secure it – make sure you are PCI DSS compliant if you accept online payments.
- Keep it – auto-renew your domain to protect it from expiring.

These actions not only help businesses protect themselves, but protect customer data which we know is incredibly valuable to cyber attackers.

"We wanted to remind SMEs that cyber security needs to be prioritised as more online trading takes place, especially with the shift for many retailers happening so rapidly."

Putting it into action

Partnering with another government agency meant we could combine budgets and utilise television media for the first time.

The campaign is being run twice; the first tranche ran mid-July until the end of August in response to the significant increase in online trading and shopping. The second tranche is due to kick off at the beginning of November, throughout the lead up to the holiday period when a lot of people are transacting online.

We ran 15 and 30 second advertisements featuring four key messages and directed website owners to cert.govt.nz to get more information. While most of the budget was spent on television, a small amount was also used for digital media.

Results

We were very pleased with the results from the first tranche of the campaign.

We reached over two million people with our television ads and delivered against all our targets. The most telling point was that visitors to the website campaign page which provides detailed information on the four steps, spent

Figure 1. CERT NZ's Cyber Smart Week 2020 banner.

on average over seven minutes viewing the page. This tells us that the information was well read and resonated with our audience.

The challenge continues

As we are all aware, when it comes to increasing cyber security awareness there's always more we can do. This October, we carried on the momentum with our annual Cyber Smart Week (CSW) campaign. CSW also focuses on four key, actionable steps not only businesses but individuals can take to make themselves more secure online.

For all the campaigns CERT NZ runs, we ensure we utilise a multi-stakeholder approach as we know when trying to enact any kind of behaviour change it takes a joint effort. By partnering with government agencies, Internet service providers and retail businesses we amplify our messages to reach an even wider audience. We provided free resources for our partners to share and promote through their channels.

"For all the campaigns CERT NZ runs, we ensure we utilise a multi-stakeholder approach as we know when trying to enact any kind of behaviour change it takes a joint effort."

Having learned so much from our global partners' initiatives, this year a big focus of the CSW campaign has been sharing our messages further to build capacity and increase awareness.

For example, we had the pleasure to work with the PaCSON (Pacific Cybersecurity Operational Network) Awareness Raising Working Group to collaborate on a regional effort around International Cyber Awareness Month. The group proposed and voted on a theme and tag line, agreeing to "Cyber Smart Pacific" and "Step up your digital safety and security." To assist, CERT NZ shared our Cyber Smart Week collateral with our Pacific partners to utilise and tailor for their campaigns and it has been great to see the local efforts to improve our collective cybersecurity taking off across the region.

What we've learned

From our reporting data and insights and engagement with our partners, we are continuing to build our understanding of New Zealand's cyber threat landscape, through our various campaigns we have distilled a few core approaches that help guide our cyber awareness efforts:

- **Know your audience:** While the core actions many of us look to promote may remain similar, tailoring our messaging and approach to specific audiences has been key. Whether it's developing natural language reporting tools or producing technical and non-technical versions of our advisories, we are constantly looking to better understand the needs and motivations of our community.
- **Keep it simple:** We have focused our campaigns on clear calls to action with straight forward actions that have the biggest impact.
- **Partnership:** We are lucky in New Zealand to have a rich ecosystem of organisations working on and around cyber issues, partnering together we can ensure that we a leveraging each other's expertise and reaching further afield helps us amplify our message and reach different sectors and audiences that we might not otherwise reach.
- **Sharing:** The importance of working together on raising awareness and building capability for cyber security is at the forefront of the work we do here at CERT NZ.

Having gained so much value and collaboration from the wider community, we are keen to share our own experiences and efforts. We look forward to continuing the conversation and are excited to have recently joined the GFCE Working Group D Awareness Raising Toolkit project team.

Our second flight of the joint Trade Smart/Buy Smart Online campaign will run from 1 November to 5 December. You can find more information about our Trade Smart Online campaign here.

GFCE Working Groups

DRIVING FORCE OF THE GFCE

THE WORKING GROUPS ARE THE DRIVING FORCE OF THE GFCE

DELHI COMMUNIQUÉ

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

1 CYBER SECURITY POLICY & STRATEGY

2 CYBER INCIDENT MANAGEMENT & CRITICAL INFRASTRUCTURE PROTECTION

3 CYBERCRIME

4 CYBER SECURITY CULTURE & SKILLS

5 CYBER SECURITY STANDARDS

CLEAR IMPACT

OUTCOMES AIM TO HAVE A CLEAR IMPACT FOR THE GFCE COMMUNITY

SHARING PROJECT INFORMATION FOR DECONFLICTING WORK AND/OR COOPERATION

A FLAGSHIP CYBER CAPACITY BUILDING PROJECT

SHOWCASING PARTNERS' EXPERTISE THROUGH WEBINARS, TRAININGS & WORKSHOPS

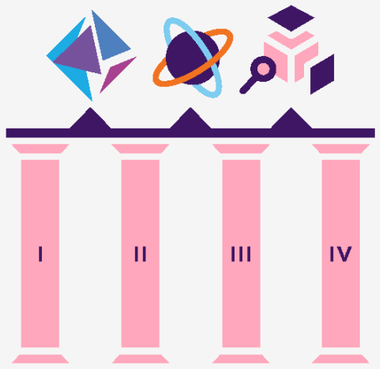
COMMUNITY DRIVEN

MULTI-STAKEHOLDER COLLABORATION IN THE WORKING GROUPS IS COMMUNITY DRIVEN

COMBINING 4 PILLARS

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

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



ANNUAL WORK PLAN

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

GET IN TOUCH

VISIT THE WEBSITE OR EMAIL US!

THEGFCE.ORG
CONTACT@THEGFCE.ORG

GFCE

GLOBAL FORUM ON CYBER EXPERTISE

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

Written by: Moctar Yedaly, Head of Information Society, African Union Commission

Following their earlier collaboration in organizing the GFCE Annual Meeting in Addis Ababa, the African Union and GFCE have decided to engage in a two-year collaborative project with support from the Bill & Melinda Gates Foundation. The project aims at mapping the current projects & programs and cyber capacity gaps in Africa, developing cyber capacity knowledge modules and sharing these modules via online in-person and online methods.

Introduction

According to various national cyber security assessments (i.e. by ITU, AUC, GCSCC, etc.) there is a vital need for most African countries to improve their cybersecurity capacities. There appears to be a significant gap in recognizing, understanding and responding to cyber threats due to a lack of awareness, infrastructure (e.g. national/sectoral CERTs), institutions and enforcement capabilities. Therefore, there is an urgent need to connect Africa's digitalization efforts with ongoing global efforts to improve cybersecurity.

"There is an urgent need to connect Africa's digitalization efforts with ongoing global efforts to improve cybersecurity.""

Earlier collaboration between AU & GFCE

The Global Forum on Cyber Expertise's (GFCE) large and diverse multi-stakeholder community has extensive expertise and experience that could be valuable for the African region. Various GFCE members and partners are involved in large cyber capacity programs in Africa. This was a key reason to organize the GFCE Annual Meeting 2019 in Addis Ababa with the support of the African Union (AU). Under the coordination of the GFCE, multiple organizations sponsored the participation of nearly 80 participants from over 40 African countries. The GFCE Working Groups organized workshops on key cyber topics. Additionally, GFCE side-meetings were organized, bringing together donors, implementers and regional organizations to discuss how they could improve coordination and avoid the duplication of efforts in the African region.

To build on the success of the Annual Meeting 2019 and the continuous efforts of the AU, the GFCE Secretariat and the AU seek to strengthen cyber resilience in the African region in close collaboration with all relevant stakeholders.

Figure 1. Participants of the GFCE Annual Meeting 2019 in Addis Ababa.

"With support from the Bill & Melinda Gates Foundation, the GFCE, in partnership with the AU, aims to develop cyber capacity building knowledge to enable African countries to better understand cyber capacities and support them in strengthening their cyber resilience."

Two-year collaborative project

With support from the Bill & Melinda Gates Foundation, the GFCE, in partnership with the AU, aims to develop cyber capacity building knowledge to enable African countries to better understand cyber capacities and support them in strengthening their cyber resilience. Through a two-year collaborative project, the GFCE and AU aims to achieve the following outcomes:

- Grow a trusted community of cyber leaders from the different African countries;
- Identify relevant cyber capacity gaps on a national and sub-regional level in African countries;
- Enable African countries to prioritize, address and communicate their national cyber capacity needs; and
- Foster coordination and increasing international collaboration between (existing) cyber capacity building efforts in Africa.

The project will build on and utilize existing cyber structures, plans, expertise and capacities within the AU, as well as within the multi-stakeholder and international GFCE Community. The GFCE Secretariat and the AU will be responsible for the coordination of the program. A GFCE regional liaison will be part of the AU team to align the coordinating efforts of the AU and the GFCE Secretariat.

Desired deliverables

In order to meet the above-mentioned outcomes, the AU will work closely with the GFCE community on a number of deliverables that are outlined below:

Mapping the current projects & programs and cyber capacity gaps

As a starting point of the project, the AU in collaboration with the GFCE will draw and build on data provided by Cybil – the CCB Knowledge Portal, to create an overview of previous, planned and ongoing projects and programs on cyber capacity building in the African region. The support of the GFCE community and the AU network will be key in this mapping exercise. Simultaneously, through desk research, surveys and interviews, an overview will be developed on current cyber capacities as well as capacity gaps in the African region. The stakeholders that are identified in these two deliverables will be encouraged to join the regional GFCE Africa group that will meet every few months to share updates for enhanced coordination and collaboration on capacity efforts in the region.

Development of cyber capacity knowledge modules

The GFCE community can offer support on key cyber capacity needs due to the vast amount of expertise available within the network. Knowledge sharing and awareness raising are key components of the cyber capacity knowledge modules that are aimed to be developed in collaboration with the GFCE Working Groups on the different cyber capacity topics with an African regional focus. Additionally, knowledge modules will be developed on "Communicating the impact of CCB" and "Reducing the gender gap in cybersecurity leadership". The aim of the knowledge modules is to raise awareness on the different cyber capacities and to provide concrete tools and steps to be taken to implement these in the experts' own countries.

In-person and online knowledge sharing opportunities

To support the rolling out of the online knowledge modules, a six-month program will be planned with a maximum of three participants per African country. The participants will be selected based on their national cyber capacity needs and the aim is to train the participants to enable to identify and address their country's needs on cyber capacities. During this six-month program, there will be formal and informal knowledge sharing opportunities during in-person and/or online meetings. The aim is to organize at the start and at the end of the program in-person meetings in Addis Ababa for the African participants and regional and global stakeholders. However, due to the current situation with COVID-19 and possible travel restrictions throughout 2021 and 2022, it is possible that alternatives need to be sought for the in-person meetings. In this manner, the program supports the growth of a trusted community of cyber leaders from the different African countries.

Tailor-made support in spin-off projects

After the six-month program if countries require further support on certain cyber capacity needs, they are invited to join the GFCE community where they are assisted in writing a tailor-made clearing house request for potential spin-off projects. Either existing programs and projects in Africa can support the needs or support for these countries can be sought with the support of the GFCE and broader cyber capacity building community.

Collaboration AU & GFCE community

The AU and GFCE are looking forward to work with the GFCE community and other relevant stakeholders on this project to enable African countries to identify and address their cyber capacity needs. The project can only be successful with the support and expertise from the GFCE Members and Partners. The project will start in the beginning of 2021. More information on the project will soon be available on the GFCE website.

"The GFCE community can offer support on key cyber capacity needs due to the vast amount of expertise available within the network."

OCWAR-C: PARTNERING TO BUILD A RESILIENT CYBER ECOSYSTEM IN WEST AFRICA

Written by: Folake Olagunju, Program Officer Internet & Cybersecurity, ECOWAS Commission, and Co-chair GFCE Advisory Board; and Raphael Koffi, Ag. Director Digital Economy & Post, ECOWAS Commission

Eleven of the fifteen Member States in West Africa are classified as Least Developed Countries (LDC), highlighting the need to implement initiatives that can create a positive socio-economic effect. Over the last decade, ECOWAS Member States have recorded growth in the use and development of ICTs, unfortunately though, this growth has also led to a rise in cyber related crimes and activities. In order to ensure a coordinated regional approach in dealing with cybercrime issues, the ECOWAS Commission launched a cybersecurity Agenda aimed at securing the common digital market for growth in West Africa and is partnering with the European Union (EU) to put in place building blocks for a more resilient West Africa, thereby building bridges between the Global North and South.

Herculean task

Undisputedly, strides have been made in the use and development of Information and Communication Technologies (ICTs) in West Africa with an estimated 47.4% internet penetration rate as of the end of 2019. Furthermore, the average E-Government Development Index (EGDI) for ECOWAS Member States has moved from 0.2882 in 2016 to 0.3574 in 2020 and will continue to grow as many West African countries have embraced digital transformation to facilitate economic recovery during and post COVID-19 pandemic.

This growth has gone hand in hand with the rise in cyber related crimes and activities with individuals and Member States participating unknowingly and sometimes knowingly. In response to this, individual Member States are at varying stages of implementing solutions that can make their environment more secure.

Considering the geopolitical nature of cyber issues and given that the Economic Community of West African States (ECOWAS) was set up to foster the ideal of collective sufficiency for its Member States, it is important that an arbitrary approach is not applied when considering challenges such as lack of appropriate laws, low cyber workforce capacity, resource mobilisation and infrastructure inefficiencies facing the region. Hence the need for a regional framework to avoid duplication of efforts and maximise resources.

With this in mind, ECOWAS launched its cybersecurity Agenda for securing the common digital market for growth in West Africa.

Leveraging on established partnerships to address these challenges and support the implementation of the ECOWAS cybersecurity Agenda, the European Union (EU) and the ECOWAS Commission are implementing the "Organised Crime: West African Response on Cybersecurity and fight against Cybercrime" (OCWAR-C) project.

Figure 1. Participants at a working session of an OCWAR-C workshop.

"The OCWAR – C project aims to improve security in ECOWAS Member States in two ways: by providing support to improve the resilience and robustness of information infrastructure in Member States and by increasing capacities of relevant stakeholders of Member States in charge of the fight against cybercrime."

With a global view to ensure that the development of the region is on the right trajectory and with positive impacts delivered, the OCWAR–C project aims to improve security in ECOWAS Member States in two ways: by providing support to improve the resilience and robustness of information infrastructure in Member States and by increasing capacities of relevant stakeholders of Member States in charge of the fight against cybercrime.

Levelling the playing field

In February 2019, the OCWAR-C journey commenced with a cybersecurity maturity level assessment of Member States. The results were not surprising, with the following numbers to hand - five Member States with an existing national cybersecurity strategy, six with a Computer Security Incidence Response Team (CSIRT) and six with the presence of a Digital Forensics Laboratory (DFL). From a legal perspective, most Member States have a prevailing legal framework in place and in line with the ECOWAS regional Acts, with a number of Member States signing and ratifying continental (Malabo) and international (Budapest) conventions. Concerning critical infrastructure, only a handful of Member States have these mapped out and most do not have any explicit laws regarding their protection. Finally, evidence of limited awareness, skills and cyber related training were also noted.

Limited resources and the numbers above illustrate why a concerted coordinated approach that allows Member States to think through the challenges/issues at the national level through a regional lens is being taken to increase community immunity. Therefore, working on the premise that Cyber Capacity Building (CCB) is holistic and multi-layered

Figure 2. Participants of a cyber defense workshop at the de l'Institut africain de cybersécurité (African Institute of Cybersecurity).

covering human capability, policy, technology and legal activities, two regional instruments: *the regional cybersecurity and cybercrime strategy* and the *regional Critical Infrastructures Protection Policy* have been prepared waiting for formal adoption by the ECOWAS Council of Ministers.

The regional cybersecurity and cybercrime strategy speaks to how to improve the level of national cybersecurity and cybercrime mechanisms as well as encourage cooperation and mutual assistance between Member States, whilst the regional Critical Infrastructures Protection Policy outlines how to ensure resilience and security of the region's infrastructures and essential services. Both regional instruments will be adapted at the national level of member states thus enhancing the necessary integration of national efforts. To bolster robustness, the project will also support selected members states in establishing either a CSIRT or DFL provided the minimum prerequisites or commitment of national authorities to sustain such a structure is in place.

To tackle the critical mass of cybersecurity workforce currently lacking in the region, a three tier (few, many and all) approach to capacity development is being deployed. On the few tier, the OCWAR-C project will conduct Train the Trainer events for identified persons from key stakeholder groups at the national level. This approach has proven successful in other projects such as the GLACY+ (Global Action on Cybercrime Extended) conducted for ECOWAS. The many tier will involve Member States sensitising their key organisations that handle cyber related issues and finally the all tier will improve cyber hygiene through awareness and sensitisation campaigns that cut across entire member states and across borders.

"To bolster robustness, the project will also support selected members states in establishing either a CSIRT or DFL provided the minimum prerequisites or commitment of national authorities to sustain such a structure is in place."

Figure 3. Participants of a cyber defense workshop at the de l'Institut africain de cybersécurité (African Institute of Cybersecurity).

Takeaways

The COVID-19 pandemic has increased rate of digital transformation in the region, regardless of how limited it may appear in some Member States. This can be viewed positively, as conversations around cybersecurity issues are now being considered as part of national and regional priorities.

To thrive, the region needs to be able to handle cyber-attack incidents. Therefore, it is expected that when the OCWAR-C project draws to a close by early 2023, the region will see considerable changes with Member States working from similar milieus with a level of trust that encourages information sharing to coordinate their actions, promote self-reliance and to create within themselves a good capacity for intervention and reaction. Recognising that the OCWAR-C project cannot have all the answers and due to limited sources of funding, ECOWAS and Member States need to continue to work closely to:

- Strengthen infrastructure inefficiencies
- Address gaps in legal & regulatory frameworks
- Fulfil the obligation to strengthen capacity in order to build resilience
- Garner political will/commitment/influence to push cybersecurity to the top of national agendas.

PROTECTING DIGITAL AFRICA

Written by: Abdul-Hakeem Ajijola, Chair, African Union Cybersecurity Experts Group (AUCSEG), and Chair of GFCE Working Group B

The article calls for Africa to take a whole of society approach to cybersecurity so that it can leverage it as an enabler that empowers members of the society to advance. Beyond the often-discussed technical threats, Africa must consider the ramifications of the Fragmentation of Technology as some nations are weaponizing interdependence. This presents challenges for African leadership to seek ways to thread their way between contenting geopolitical cyber related situations and powers. The article brings attention to election interference via influence operations targeting the electorate and operations against the technical infrastructure of election processes. The author also calls on African nations to leverage Women as Information Security power players and advises on the need to develop a generation of "cyber diplomats" to engage in ongoing global Norms development processes.

Cyber threats

The accelerated usage of, and increasing dependence on, digital technologies across Africa is a double-edged set of swords. While it portends great advancements in socio-economic empowerment, education and human wellbeing, there are also threats which we must understand, build resilience against, and mitigate across digital and analogue value chains.

It is imperative that we take a whole of society approach to cybersecurity and leverage cybersecurity as an enabler that empower members of the society to advance; opportunity to create a national profit centre; create wealth, job creation plus revenue generation, improve supply chains to secure global competitive advantage and foster resilience to ensure the survivability of key societal institutions, cultural perspectives, and values.

Cyber threats are becoming more diverse and complex and endangering the technical integrity of the digital world heightened by the digitalization of organisations that makes the emerging African digital economy more vulnerable to cyberattacks, not only from states but also from criminal organizations and other nonstate actors. Threat agents cut across a wide spectrum ranging from curious neophytes, show-offs, cyber-criminals to state-sponsored actors with assorted ego, financial and political motives. Furthermore, the dynamic nature of the cyber threat landscape is driven by factors including available tools to exploit vulnerabilities, the knowledge base of available resources and vulnerabilities, and the skill requirements to place an attack – which is becoming easier due to the freely available, ease to use, tools online.

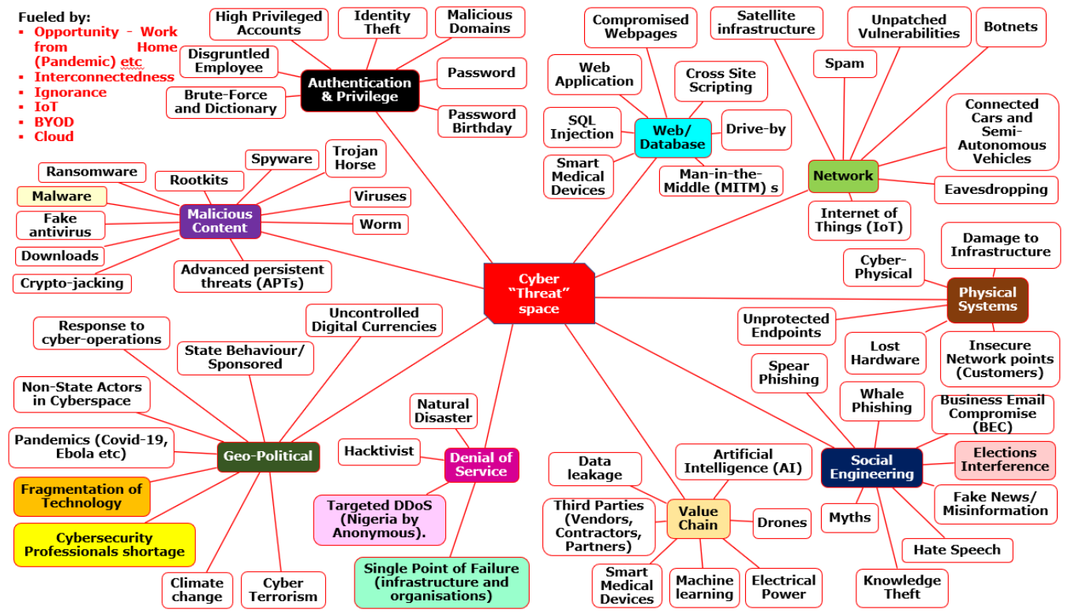


Figure 1. Mind map of the Cyber "Threat" Space.

Cyber threats are becoming more diverse and complex and endangering the technical integrity of the digital world heightened by the digitalization of organisations that makes the emerging African digital economy more vulnerable to cyberattacks, not only from states but also from criminal organizations and other nonstate actors. Threat agents cut across a wide spectrum ranging from curious neophytes, show-offs, cyber-criminals to state-sponsored actors with assorted ego, financial and political motives. Furthermore, the dynamic nature of the cyber threat landscape is driven by factors including available tools to exploit vulnerabilities, the knowledge base of available resources and vulnerabilities, and the skill requirements to place an attack – which is becoming easier due to the freely available, ease to use, tools online.

> "The success of bad actors is fuelled by the exponential growth of the threat surface as technology becomes ubiquitous and pervasive and exacerbated by the spectre of COVID-19."

The success of bad actors is fuelled by the exponential growth of the threat surface as technology becomes ubiquitous and pervasive and exacerbated by the spectre of COVID-19. Opportunities are driven by new models of business and social interactions. This is compounded by increased interconnectedness with over one billion new users expected to move online over the next few years, many of whom are from the global south and Africa in particular. Add to the mix is the ignorance of many end users and intermediate organisations and providers. Technical advisory groups across the world, like the African Union Cybersecurity Experts Group (AUCSEG) view the increasing the cyber threat surface with concern and advocate for enhancing the need for Cyber-hygiene as a foundational defence at home, remote or other access end points and as a component of national security.

Cyber Risks

In addition, the cyber-risks that are regularly discussed, Africa needs to be fully cognisant of the following, namely:

1. **Fragmentation of Technology** as manifest in:

a. Independent initiatives by Russia (RuNet), China (Great Firewall) and Iran (national Internet for Iran) to create independent network infrastructure with separate Domain Name Systems and relate architecture.

b. Coercion by some nations to ban, raise tariffs or domesticate ownership of foreign technology providers, products (equipment) and services such as infrastructure from Huawei and Apps such as Tik-tok – retaliation to such sanctions has motivated the development of alternative, possibly incompatible, models, standards, and pathways. African Union member states risks being caught out as unwary victims in a potential China-USA, USA-Europe, USA-Russia and/ or China-India geopolitical and cyber-warfare battle space.

c. Africa, must thread its way across the multipolar world of technology by:

i. Building proficiency in monitoring and proactively navigating complex and varied economic, commercial, technology, privacy, and connectivity relationships as they relate to cyberspace.

ii. Motivate indigenous research, development and innovation and employ indigenous technologies and solutions to minimise total dependency on any single external party.

iii. Develop and implement robust vetting mechanisms when integrating software, hardware or networking solutions and segment operations across multiple pathways, organisations, and technologies to minimize exposure to single points of failure.

4. **Elections Interference:** Elections are foundational to the liberal democracy that several African nations are endeavouring to practice for the well-being of their inhabitants and long-term stability of those nations.

a. Some State and non-state actors are adopting tactics to interfere with and affect election outcomes. This is particularly important as African societies embrace digitisation such as social media and as the election process itself becomes more dependent on digital technologies for election management and related processes. The misuse of social media has in effect presented and opportunity for bad actors to "hack" the electorate and impact the outcomes of elections. This is compounded by the potential to undermine the digital technology that is used to support the election process ranging from illegal monitoring of members of the opposition as alleged in 2015, when it was reported that at least four Nigerian State Governors were alleged to have "illegally" acquired technologies that allowed them conduct mass surveillance and intercept communication to eavesdrop on the conversations their political peers and rivals. The alleged widespread failure and manipulation of electronic voting support systems in the 2017 Kenya Presidential elections lead to a re-run.

b. African nations must evolve mechanisms that:

i. Ensure appropriate incident response and recovery plans that include communications strategies to inform all relevant stakeholders on the scope of any incidents and address false narratives on cyber-attacks before they spread.

ii. Encourage political parties to conduct self-assessments to determine which assets may represent the most valuable targets for threat actors seeking to steal sensitive campaign data.

iii. Address the scourge of fake news, hate speech and related misinformation.

3. **Getting Women and youth into IT Security and evolving them into Power Players is a critical societal security issue.**

a. No Society/ Economy can make significant headway if it does not leverage 50% of its population (Women) and stifles another 47% (Male Youth) of its population.

b. It is in our strategic self-interest to encourage our ladies, wives, sisters & daughters to become cybersecurity power players.

c. Cyber activities provide flexibility for people to work from home within the boundaries of our traditional values systems.

d. It is important to ensure that female African cybersecurity pioneers are visible to inspire a new generation of women into the profession.

Figure 2. Female African power players in cybersecurity.

Way forward for Africa

1. **The global south must be careful about "Digital Colonization"** as we do not make much input into any alternative sources of digital technology or technology value chains. Thus, the imperative over the long-term is to build indigenous capacity that sustainably empowers us to participate in technology value chains on our own terms based on a robust, realistic, and implementable Cybersecurity Preparedness Strategy and Plan.

2. **African needs to immediately and deliberately optimally mix and match equipment based on open standards and interoperability, thus spreading risk and reducing reliance on any single source organisation or country.** This will impact all imminent and future technology provisioning contracts, and loan discussions, across the continent.

3. **Africa must build its human resources capacity.** For example, Cryptography (not Quantum Cryptography) and the development of algorithms followed by software development are not as equipment intensive as other opportunities. Indigenous cryptographic algorithms can be quickly developed by empowered Africans. Though they will not immediately solve all cyber challenges and related problems, such solutions will diminish the capacity of others to access and decipher the content of our transmissions. Collaboration with capacity building entities like the Global Forum on Cyber Expertise (#GFCE) is a good place to start.

4. Africa, supported by the AUCSEG and other support entities, must initiate, and sustain capacity development of people, processes, and technology. **We must encourage and facilitate the private sector as the prime driver of technology development and deployment while Governments ensure fair play, equity, and regulatory compliance.** While appreciating that corruption is a challenge, it is uncertainty, principally arising from inconsistent policy implementation, that is the arguably bigger problem for private sector facilitated development in Africa.

5. Given the ongoing United Nations (UN) Group of Governmental Experts and UN Open Ended Working Group among several international discussions such as the aimed at establishing global cyber norms, **Africa needs to develop a generation of savvy "cyber diplomats."** Our Cyber Security Policies and Strategies must safeguard that African nations do not lose out in ongoing global cyber norms development processes and remain relevant given that norms (soft laws) are likely to evolve in to international (hard) laws which impact our continental and national cybersecurity postures.

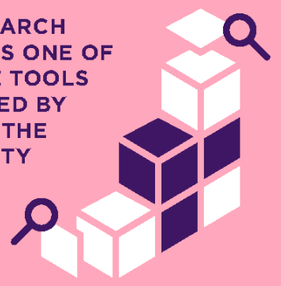
6. **Africans and their governments must continually ask themselves about what factors will impinge on our cyber-survivability and the threats that they (we) are not considering**, be aware of or are not yet invented, but are just over the threat horizon. Colloquially speaking we need "torch-light" like mechanisms to peer into the darkness ahead of us. On the technological side, the African Union can learn from, partner with and co-develop predictive cyber threat models as initiated by the Association of South-east Asian Nations (ASEAN).

There are no clear, easy, or obvious answers, and these are conversations that African, and societies in the global south need to engage in immediately.

Global CCB Research Agenda

GFCE TOOLS

THE RESEARCH AGENDA IS ONE OF THE GFCE TOOLS DEVELOPED BY AND FOR THE COMMUNITY



RESEARCH COMMITTEE

THE RESEARCH COMMITTEE PROVIDES EXPERT SUPPORT FOR THE DESIGN, DELIVERY AND IMPLEMENTATION OF THE AGENDA

AIM OF THE RESEARCH AGENDA

ADDRESS EXISTING KNOWLEDGE GAPS ON CCB

HELP THE CAPACITY BUILDING COMMUNITY DESIGN AND RUN MORE EFFECTIVE PROJECTS

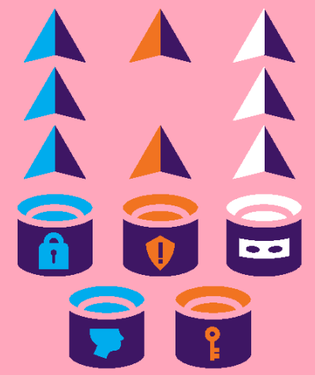
THE PROCESS

AN ANNUAL, COMMUNITY-DRIVEN PROCESS

1. HARVESTING & REFINING IDEAS
2. AGENDA SETTING
3. COMMISSIONING RESEARCH
4. DELIVERING RESEARCH

HARVESTING IDEAS

KNOWLEDGE GAPS AND RESEARCH IDEAS ARE IDENTIFIED IN THE WORKING GROUPS



AGENDA SETTING

THE GFCE COMMUNITY WILL BE INVITED TO PRIORITIZE RESEARCH NEEDS INTO A RESEARCH AGENDA ONCE A YEAR

RESEARCH OUTPUTS

OUTPUTS MUST BE ACCEPTED BY THE REQUESTING WORKING GROUP BEFORE BEING PUBLISHED ON THE CYBIL PORTAL THESE CAN BE:

GUIDE WITH ILLUSTRATIONS

IN-DEPTH STUDY

REPORT WITH RECOMMENDATIONS

RESEARCH OUTPUTS WILL PROVIDE ACTIONABLE DATA

GET IN TOUCH

VISIT THE WEBSITE OR EMAIL US!

THEGFCE.ORG
RESEARCHCOMMITTEE@THEGFCE.ORG

GFCE

GLOBAL FORUM ON CYBER EXPERTISE

HOW COVID-19 SPURRED CYBER AWARENESS WITHIN THE EUROPEAN COMMISSION

BEST PRACTICES IN A SUPRANATIONAL ENVIRONMENT

Written by: Ann Mennens, Corporate Cyber Aware Programme Manager, European Commission

Literally overnight, the European Commission has taken up the challenge of teleworking for all staff in March. Internal awareness raising guidance was adapted in consequence, focussing on ensuring a secure digital workplace from the home environment, security proofed business processes and tooling, and upskilling staff in cybersecurity. Every staff member has a responsibility in protecting the Commission, its systems and assets. The corporate Cyber Aware programme provides updated information, education and advocacy, preparing the staff to be the Commission's first line of defence against the cyber threats it is facing.

"Digitalisation and Cybersecurity are two sides of the same coin." - President Von der Leyen

The digital Commission

The European Commission under the leadership of Ursula Von der Leyen has the ambition to be a truly digital Commission that will drive a Europe fit for the digital age. The roadmap defines digital targets related to connectivity, skills and digital public services, focussing on the right to privacy and connectivity, freedom of speech, free flow of data and cybersecurity. The same principles apply to the daily organisation and running of the Commission. Applying in practice what we preach to the Member States, the European Commission (EC) Digital Strategy sets a vision for the Commission to become a digitally transformed, user-focused and data-driven administration by 2022. Cybersecurity is an essential component for the effective functioning of such modern, high-performing digital public administration, enabling the Commission to operate in a secure and trustworthy environment, and safely deliver its political priorities.

"Cybersecurity is an essential component for the effective functioning of such modern, high-performing digital public administration, enabling the Commission to operate in a secure and trustworthy environment, and safely deliver its political priorities."

This digital transformation comes with new working modalities, such as cloud, mobile, Internet of Things, big data, machine learning, social media. Along with the advantages they bring, come inherent cybersecurity challenges, widening the 'attack surface' and exposing the Commission to an increasing number of cyber-attacks.

How does this impact its staff? Since mid-March, the 32.000+ workforce had been propelled into a truly digital workplace, able to work at any moment, from any place, coordinating, sharing information and documents, preparing the decisions shaping Europe's future. Earlier resistance to change was overtaken by the sudden urgent need for this change to happen. Colleagues across the Commission willingly adopted new processes and tools, making the Digital Workplace an everyday reality. It was accompanied by guidance to make the shift in a cybersecurity proof manner.

Figure 1. The Cyber Aware team.

The corporate Cyber Aware programme

The awareness raising guidance has been produced as a part of the Commission programme for cyber awareness raising: Cyber Aware. Launched in 2016, it gradually developed into a highly effective programme providing the backbone for the establishment of a true cybersecurity culture amongst the Commission staff.

The key principles shaping the success of Cyber Aware:

Embedded in strategy

The establishment of a security culture with the staff, reinforcing the work of the IT security services protecting the Commission, is part of the vision for the organisation and reflected in its strategy and yearly management and working plans.

Tone at the top

Cyber Aware has the support from the highest level, including the personal commitment of Commissioners and VIPs leading the way. Their personal cyber stories showcase that anyone can become victim of a cyber scam and promote a cyber aware behaviour.

Attributed resourcing for the programme combined with an appropriate governance structure ensure that it is here to stay and grow as needed.

Targeted communication

Cyber Aware knows it's 'clients' and has a message tailored to every target audience, be it end-users, IT professionals, senior management and VIP or any specific group like newcomers, trainees or developers.

Variety of training

Cyber Aware uses different training methods and material, acknowledging the force of blended learning. The regularly updated offer includes events and campaigns, classroom and online courses, e-learning, videos as well as gamified content like quizzes, platforms with challenges, and simulation exercises to learn by doing, like fake phishing campaigns.

Flagship is the internal Cybersecurity Training Programme, launched in 2020 to attract more women and reduce the skills gap in cybersecurity.

Shared responsibility

The Commission is equipped with the latest high tech tools assisting the IT security expert teams in the protection of the organisation against cyber attacks, monitoring, detecting cyber threats and managing incidents. Technology alone does not suffice, the human needs to be present in this chain fencing off attacks through cyber hygiene and a safe online experience.

Continuous Improvement

Cyber Aware receives input from several services and colleagues in the Commission regarding new threats, ongoing phishing campaigns, types of incidents, flaws in user behaviour, questions to the helpdesk. This feeds the communication to users and the content programming for the training and exercises, including the fake phishing campaigns. Combined with best practices identified with peers, it ensures that content is topical and relevant for the different target audiences. The latter's feedback is essential to keep at pace with expectations.

Choose your Dream Team

Cyber Aware has an enthusiastic team with diverse talents, combining skills in management, communication, graphical design, training and education, video production, languages, and yes, also some knowledge in EU affairs and IT security. We happen to be all ladies, happy to contribute to the gender balance in the IT Security Directorate, composed predominantly of men.

Never walk alone

Cyber Aware is a team of four, addressing a 32000+ Commission audience. It can count on experts in the different Commission services dealing with cybersecurity, the Cyber Aware Operational Team. It also works together with different networks to ensure a wide spreading and reach of the information (e.g. training and communication services, Local Informatics Security Officers, etc.).

Figure 2. The Interinstitutional kick-off of the European Cyber Security Month (ECSM) 2020 was a hybrid event with some participating in person and others via videoconference.

Join forces: cooperate with your peers

Worldwide, the community of experts in cyber awareness raising is growing day by day. Exchanging ideas, experience, thoughts and best practices with people who are confronted with the same challenges, can be very rich and comforting. Don't be shy, just do it. It will feel great and you will learn a lot. No need to reinvent the wheel, where possible, exchange not only ideas and experiences, also share your material and resources. It is for the greater good, to better spread the word on how to be cyber aware.

European Cyber Security Month (ECSM)

The yearly highlight in cyber awareness raising happens in October. Cooperation started in March with peers in the EU Member States, Europol and ENISA, to decide on the themes, exchange experience and put together the material for the campaign: videos, posters, infographics and more, publicly available in all official languages of the EU. With the motto 'Think Before U Click', ECSM 2020 focused on two themes to help people recognise and handle online threats: Digital Skills and Cyber Scams.

Cyber Aware organised the interinstitutional kick-off for ECSM2020, marking this important campaign with a joint event of EU institutions (EU-I). Objective was to raise awareness on cyber scams, particularly in the light of COVID 19, putting the spotlight on the role every individual can play to stop cyber related crime. The cybercriminals quickly adapted their modus operandi to the changing situation, but the EU-I also reacted swiftly to counter them. Watch here how Commissioner Hahn opened the event, passing the ball to high level speakers from the different EU-I .

The best is yet to come

The coming years foresee an intensification of the Cyber Aware programme, both in depth and width, reaching out to the Commission population at all levels. Information and training will be further diversified, professionalised and shaped according to identified needs, using novel methods and technologies. The spotlight however remains on the small things each and every staff member can do, should do, to ensure the protection of their information and privacy and of the Commission assets, against malicious attackers: to be cyber aware!

"Each and every one of us can do a lot to make the European institutions more cyber secure."
- Johannes Hahn, European Commissioner for Budget and Administration

HOW PREPARED ARE COUNTRIES IN THE FACE OF A CYBERATTACK? THE NATIONAL CYBER SECURITY INDEX REVEALS

Written by: Merle Maigre, Senior Expert on Cyber Security, e-Governance Academy (eGA)

Safeguarding our digital way of life and maintaining cyber security capacities is a challenging task for both governments and businesses. How prepared are countries in the face of a cyberattack? How do we evaluate success? These questions are regularly asked by many governments. Several international standards and guidelines exist for developing the cyber security of a single organization. Yet, there is a lack of comprehensive tools for developing and measuring cyber security at the national level. The National Cyber Security Index (NCSI) created and maintained by the e-Governance Academy is designed to fill that gap. It is a comprehensive tool for cyber capacity building as it provides cyber security maturity assessments for governments. The decision about where you want to go must start with a recognition of where you are. Similarly, the NCSI takes national decision makers on a cyber capacity development journey starting with mapping the situation and setting strategic goals.

The importance of cyber security

Since COVID-19 forced offices and schools to close, the web has remained the main lifeline enabling us to work and educate our kids. The number of people relying on online security has skyrocketed. At the same time, the accelerated spread of various online tools for accessing sensitive governmental and corporate IT systems has increased the potential for security incidents. Around the globe, phishing scams, ransomware, DDOS attacks, malware and data stealing apps have increased. This emphasizes the importance of cyber security for both governments and businesses, and the need for a comprehensive tool for cyber capacity building.

NCSI: a unique comprehensive measuring tool

The National Cyber Security Index (NSCI), created and maintained by the e-Governance Academy, is a comprehensive tool for capacity building on cyber security. Spanning across 160 countries surveyed, the index is one of the world's most detailed cyber security assessment tools. It provides a transparent assessment methodology on how national cyber security could be understood and managed by policy makers. Based on publicly available data, it also offers an opportunity for all to review the sources by which the country's assessment is based on.

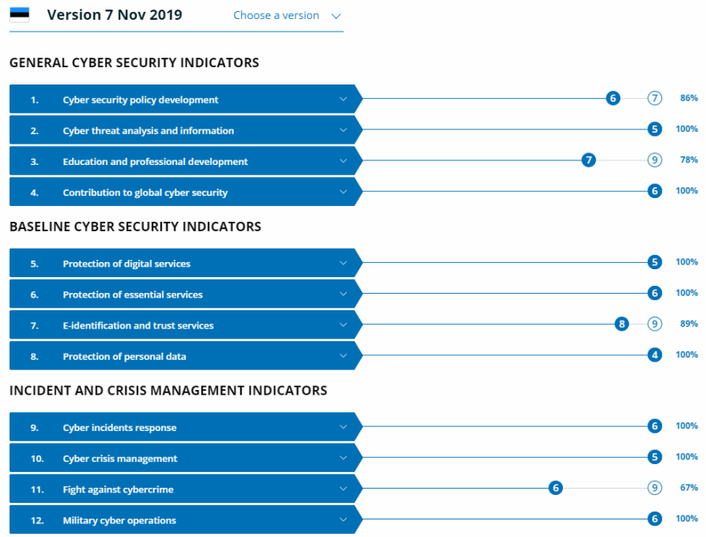


Figure 1. Estonia's assessment based on the NCSI's 12 identified capacities.

Cyber security can only be guaranteed through a wide range of cyber capacity building measures. Cyber security also needs to be approached with humility – it is important to realize that cyber security incidents can never be completely prevented. Rapid development of technology and its accelerated spread raises the likelihood of security incidents. Therefore, in addition to preventing incidents, the focus must also be on cyber resilience; that is, the control and reduction of damage caused by incidents. This requires two types of action: first, proactive measures aimed at preventing incidents, and second, reactive ones to control and reduce damage.

When assessing cyber capacity, both proactive and reactive categories must be covered. The NCSI measures preparedness to prevent cyber threats, as well as readiness to manage cyber incidents, crime and large-scale cyber crises. It analyzes traditional government tasks, such as drafting legislation or designating responsible institutions, as well as assesses other various cyber capacity building activities, such as curricula at different school levels or a public-private partnership. Inter alia, the index maintains that the existence of a reliable digital identity and capable technical means for identification are also elements of a country's cyber security, as the use of personalized e-services requires that these services are used only by a given person to whom access is granted.

Overall, measurable activities are divided into 12 capacities. Each cyber capacity contains multiple indicators. For example, the capacity of cyber security policy includes four indicators that assess whether a country has a cyber security policy unit, formats of cooperation, as well as a cyber security strategy and a plan for its implementation. The other 11 capacities are similarly quantifiable. The index includes 46 indicators in total.

The unique feature of the NCSI is that its data is continuously updated. Unlike other indices, which generally publish assessments once a year, the Index updates data on a rolling basis – as soon as new country data becomes available and is reviewed by experts. The NSCI country pages additionally serve as a database of hundreds of links and documents. Thus, NCSI is a valuable free source of shared information detailing how countries are building their cyber capacity.

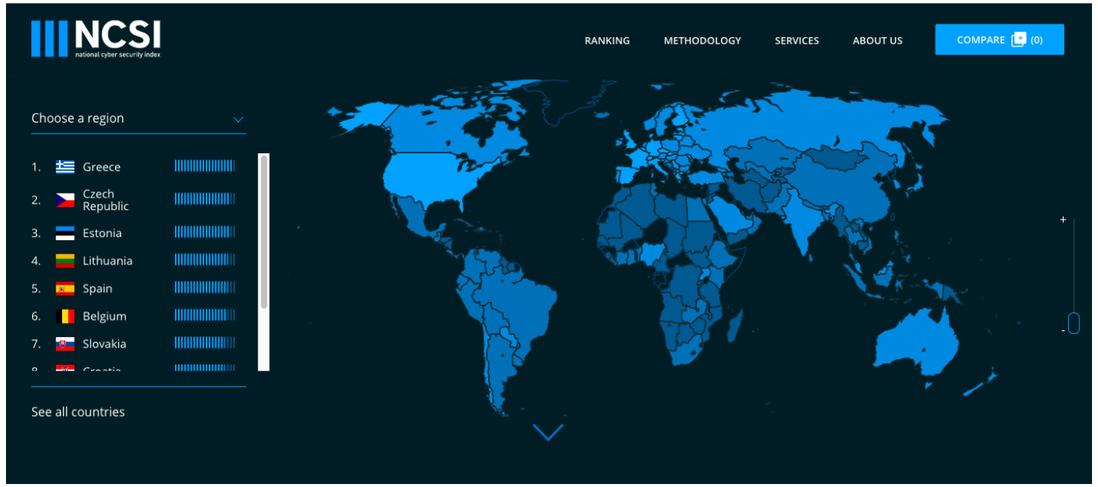


Figure 2. The homepage of the NCSI website.

Useful benchmark for countries

A world map and a ranking of countries is displayed on the homepage of the NCSI website (https://ncsi.ega.ee). It allows countries to compare their rankings globally, at a regional level or within international organizations. It also offers an option to see how a country's position in the index has changed over time. For each individual country, the index provides an overview of its position based on other commonly used digital indicators such as the International Telecommunication Union's ICT Development Index, the Global Cybersecurity Index and the World Economic Forum Network Readiness Index.

The advantage of the NCSI is that it evaluates countries' digital security and at the same time, helps governments have a common understanding of their situation, identify capacity gaps and improve their positions. For example, Finland and Georgia have used the NCSI index as an official benchmark to assess and improve their national cyber security. The index also confirms the claim that cyber security supports the country's overall digital development. This means that the indicators of developed digital nations are balanced as they also focus on developing cyber security.

"The advantage of the NCSI is that it evaluates countries' digital security and at the same time, helps governments have a common understanding of their situation, identify capacity gaps and improve their positions."

What is the e-Governance Academy?

The NCSI is managed and updated by the Estonian e-Governance Academy (eGA). Founded in 2002, the eGA is a non-profit organization that creates and transfers knowledge and best practices in the area of public sector digital transformation. The mission of eGA is to increase the competitiveness of societies through digital transformation, transparency and openness. For this purpose, eGA transfers Estonian and international best practices to governments and other stakeholders around the world. eGA's activities are organized under the programs of Smart Governance, e-Democracy, Technology and Cyber Security.

Based on its 18-years of worldwide experience, eGA maintains that a nation's cyberspace, its digital society and e-services

Figure 3. Cyber security experts of Finland and Estonia, Janne Järvinen, Kimmo Ruosku and Epp Maaten, sharing experiences on how to benefit from the use of NCSI. Photo by Raigo Pajula.

form a complex environment that cannot safely exist without solid cyber security protection. As governments begin to build an information society, they typically focus on providing more digital services and creating various service environments. Cyber security for a society will only receive more thought after an extensive or damaging security incident. At the same time, cyber security is an integral part of an information society. Electronic services such as e-banking or e-tax administration are of no use if their functioning and the confidentiality of the data transmitted is in doubt.

There are many threats in cyberspace and the measures to counter them are also numerous. This raises the question of where a state should begin in order to better protect itself in cyberspace. True cyber security also means that a country has effective measures in place to prevent, detect, and react to cyber incidents. To limit disruption, countermeasures should be planned, discussed and agreed on before a cyberattack even occurs. Above all, the decision about where you want to go must start with a recognition of where you are. The NCSI takes national decision makers on a cyber capacity development journey starting with mapping the situation and setting strategic goals.

"The NCSI takes national decision makers on a cyber capacity development journey starting with mapping the situation and setting strategic goals."

BUILDING CAPACITIES ON CYBERCRIME IN TIMES OF COVID-19

Written by: Matteo Lucchetti, Programme Manager Cybercrime, GLACY+ Project, Council of Europe; Giorgi Jokhadze, Programme Manager Cybercrime, CyberEast Project, Council of Europe; and Nina Lichtner, Programme Officer, Cybercrime@Octopus Project, Council of Europe.

The COVID-19 pandemic had a direct impact on the cybercrime global landscape, with malicious actors exploiting vulnerabilities of individuals in a period when criminal justice authorities were facing increasing challenges due to the mutated priorities and the different working conditions. In such a scenario, capacity building was deemed useful as long as it could provide concrete responses and usable solutions to the emerging necessities and the related requests. Programs in the field were able to support by reassessing the needs of the beneficiaries, adapting the work plan and redesigning efficient delivery methods.

COVID-19 and the cybercrime landscape

It is undeniable that the COVID-19 pandemic has been amplifying vulnerabilities and exposures of individuals and society in all respects.

During the crisis, we all have been relying more than ever on computer systems, mobile devices and the Internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. And this has been increasingly exploited by malicious actors to their own advantage.

In fact, a surge of COVID-themed online threats was noted, hitting especially in the first months of the pandemic, as for example:

- Phishing campaigns and malware distribution through seemingly genuine websites or documents providing information or advice on COVID-19, used to infect computers and extract user credentials.
- Ransomware shutting down medical, scientific or other health-related facilities where individuals are tested for COVID-19 or where vaccines are being developed in order to extort ransom.
- Attacks against critical infrastructures or international organizations, such as the World Health Organization.
- Ransomware targeting the mobile phones of individuals using apps that claim to provide genuine information on COVID-19 in order to extract payments.
- Fraud schemes where people are tricked into purchasing goods such as masks, hand sanitizers, but also fake medicines claiming to prevent or cure SARS-CoV-2.
- Misinformation or fake news are spread by trolls and fake media accounts to create panic, social instability and distrust in governments or in their health authorities' measures.

In this respect, a huge increase of cases of online child sexual exploitation and abuse was reported, as well as an increased number of successful DDoS attacks, increased attempts to recruit online money mules due to the uncertain employment context, and increased vulnerability of organizations due to the use of remote working environments on unsecured devices. The impact on the criminal justice system

A survey was conducted by the Council of Europe among selected countries in Europe, Asia-Pacific, Latin and Central America and Africa, to assess the impact that the COVID-19 crisis had on the criminal justice sector in charge of cybercrime cases.

Under the legislative perspective, it acted as a catalyst to advance on promulgating regulations, and in a few cases even laws, to facilitate collaboration with service providers in emergency situations, as well as to limit the spread of fake news on the pandemic. This called for an even stronger focus on the need to provide legislative advice through capacity building initiatives.

But the COVID-19 crisis also revealed and reinforced some of the constraints that criminal justice authorities had already been facing in the management of criminal cases related to cybercrime and electronic evidence.

In many countries, law enforcement officers, irrespective of their specialization, were reassigned to contribute to the enforcement of emergency rules (e.g. lockdowns, curfews, border controls) despite the already increased workload of cybercrime investigations. In some cases, prosecutors were also detached to support law enforcement in implementing such measures in the field. This created a shortage of human resources available to handle cybercrime investigations and prosecutions.

The judiciary's capacity to fulfil its role has also been hindered in many countries. Courts have been reported to function with limited capacities due to restrictions related to physical meetings. During this period, only urgent hearings were held in most of the affected countries, while the general workload was deferred to a later stage.

While prosecuting cybercrime cases has been reported to be difficult in this context, a stronger focus was placed on technical responses, such as the prompt take-down of malicious websites. In cases of fake news, some authorities have been issuing official disproving statements while at the same time initiating investigation and prosecution processes, with the primary scope of discouraging such behaviour.

> "While prosecuting cybercrime cases has been reported to be difficult in this [COVID-19] context, a stronger focus was placed on technical responses, such as the prompt take-down of malicious websites."

The need for capacity building, standard operating procedures and infrastructure

With prosecutors and judges largely resorting to remote work during the pandemic, the need to manage a greater amount of case files and accompanying evidence (including oral evidence taken by remote links, electronic court hearings, etc.) increased.

Against applicable restrictions in which access to and use of "traditional" types of evidence, such as witness testimony or crime scene examination, could be limited, the importance of proper electronic evidence as data which could be accessed, obtained and processed remotely in many situations should not be underestimated as well. Even more importantly, electronic evidence as a type of admissible proof in criminal cases requires specific handling skills and respect of the chain of custody on behalf of the criminal justice authorities.

This emphasized the importance of regularly conducting judicial trainings on electronic evidence, targeting judges and prosecutors, but also all the relevant staff working in the criminal justice system, to the extent possible.

Developing and sharing guidelines on online investigations for prosecutors, including instructions on making requests for data to Internet Service Providers, was remarked as a priority for support to be possibly provided by capacity building initiatives,

in order to streamline processes and facilitate faster case handling at the national level.

Developing standard operating procedures (SOP) for criminal justice process in times of crisis is another necessity in this respect. The SOPs should outline the roles, responsibilities and means of communication and cooperation between the authorities involved in the criminal justice process during the crisis response. In the process of drafting, applying and revising such documents, the Council of Europe Standard Operating Procedures on Electronic Evidence could be used as general guidance.

In terms of infrastructure, countries that had already started working on the digitalization of their criminal justice system reported that the current crisis is accelerating this process, while other countries are now prompted to open the debates on possible electronic solutions. However, the feasibility of such measures is largely dependent on the national Internet infrastructure, with some countries reporting difficulties for their LE and judiciary staff in carrying out their duties remotely due to the limited connectivity.

Challenges and opportunities for capacity building programs

As always in times of crisis, consolidated practices may suffer major challenges if resources are reduced or refocused on different priorities. And this is what happened also for capacity building initiatives and projects on cybercrime in times of COVID-19 pandemic.

Issues that were experienced on the national level were related to both the increased workload of national counterparts and the changed working conditions, and they included:

- Maintaining the focus on project-related issues despite reduction of dedicated staff and changed priorities;
- Keeping the criminal justice community united and engaged in cooperating with each other;
- Reliance on technical infrastructures often with diverse levels of stability and accessibility, beyond the implementing entity's control.

On the project side, the main challenges that arose were related to:

- Reassessing new needs and priorities of supported countries and reshaping the work plan accordingly;
- Readapting training courses and materials to make them fit for remote delivery;
- Measuring the impact of activities conducted online and identifying ways to maximize it.

But the new working conditions and the shift to online delivery also allowed to seize a few opportunities for enhancing the impact of capacity building activities through a more efficient and cost-effective organization of multiple meetings with multiple counterparts, thus developing the overall agenda at a faster pace.

Redesigning the capacity building agenda – the GLACY+ example

In consideration of the altered scenario, capacity building initiatives conducted by the Cybercrime Programme Office of the Council of Europe underwent a thorough revision, aimed at reassessing the new priorities for the supported countries, identifying what practical and concrete contribution could have been brought in the current conditions and defining the most effective delivery strategies.

One example can be provided by the GLACY+ (Global Action on Cybercrime Extended) Project, the flagship initiative of the European Union and the Council of Europe in the field of cybercrime capacity building.

Starting from March 2020, GLACY+ activities have been re-organized for online implementation due to travel restrictions and lockdown measures implemented worldwide to contain the spread of the COVID-19 pandemic. In this period, five categories of activities were implemented:

- **Webinars,** at global, regional and national levels. These were one-to-many fully online sessions, with up to 400 participants from all over the world, lasting maximum 2 hours and focusing on some topic of general interest. Webinars resulted to be very useful to reach out to a large number of countries at once and aggregate a global community of committed criminal justice practitioners;
- **Online workshops**. Result-oriented events usually implemented on a country-specific basis and composed of several sessions over a few days. Attended by a restricted number of participants, these workshops are focused on specific tasks, such as drafting cybercrime bills or discussing national policies, as for example the High Level Workshop on Cybercrime Legislation in Congo;
- **Remote delivery/ hybrid approach**, either in-country or regional. This is a hybrid way of conducting activities, where participants and national trainers gather in a venue with a stable connection and in full respect of sanitary measures in place in that specific country (e.g. social distancing, use of masks, hand sanitizers, etc.), and international facilitators/ trainers intervene from remote. Direct interaction between participants is therefore made easier, so it was the preferred mode for training activities. An example of such delivery mode is the Introductory course on Cybercrime and Electronic Evidence for Ghanaian criminal justice sector;
- **E-Learning**. Trainees are engaged in a program that lasts a number of weeks, which is organized as a university course, with weekly modules composedof webinars/ presentations/ sessions to attend, tests to pass and readings to do. For such training, a dedicated platform has to be used, which hosts all the contents of the different modules and allows trainees to consume materials at their own pace. This way of delivering training requires a long-term commitment from the participants, which were limited in number to a few units per country, but it allowed a longer and more structured exposure to contents and therefore it constituted a learning experience providing deeper knowledge. An example of e-learning provided to police forces of GLACY+ countries is represented by the E-Evidence Boot Camp Training Course organized by INTERPOL;
- **Desk studies and reports**. In order to provide usable tools and reply to the increasing request for policy and legislative support from countries worldwide, a number of desk studies/ reports were also completed. A relevant example in this regard is the Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence.

Figure 2. The front cover of the Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence, published by INTERPOL and the Council of Europe, in the framework of the GLACY+ Project.

Conclusions

The COVID-19 pandemic was exploited by cybercrime actors to increase the attack surface and to take advantage of vulnerability and exposure to online threats of individuals and the society.

Criminal justice authorities working in the field faced a number of challenges due to the increasing number of cases and workload, a general reduction of the staff with redefined priorities, and changed working conditions.

Prompt cooperation with foreign criminal justice authorities and with the private sector became even more relevant, as well as knowledge and capacities to handle it.

This scenario highlighted once again the need and the relevance of capacity building initiatives in this area and the capability to quickly adapt to the evolving situation became crucial for those programs, in order to keep providing effective support to countries worldwide.

Reassessing priorities of action, adopting a flexible and tailored approach to reshape the work plan, and defining a plethora of delivery options proved to be an efficient way to continue building capacities and it allowed to consolidate an even stronger sense of belonging to a global community, united and equally committed in the global fight against cybercrime.

Cybil

Cybil
Knowledge
Portal

GLOBALLY OWNED

CYBIL IS THE GLOBALLY OWNED KNOWLEDGE PORTAL ON CCB BY:

- GCSCC
- ASPI
- NUPI
- FIRST
- GFCE
- DIPLOFOUNDATION

INFORMATION SOURCES

ALL INFORMATION RECEIVED FOR CYBIL IS FIRST SHARED AND CURATED BY THE GFCE WORKING GROUPS

WHAT IS ON CYBIL

A UNIQUE REPOSITORY OF INTERNATIONAL PROJECTS, TOOLS, PUBLICATIONS, ACTORS AND EVENTS RELATED TO CCB

- CYBER SECURITY POLICY & STRATEGY
- CYBER INCIDENT MANAGEMENT & CRITICAL INFRASTRUCTURE PROTECTION
- CYBERCRIME
- CYBER SECURITY CULTURE & SKILLS
- CYBER SECURITY STANDARDS
- TRENDING TOPICS

WHO IS CYBIL FOR

- GOVERNMENTS
- INDUSTRY/ PRIVATE SECTOR
- CIVIL SOCIETY/ ACADEMICS
- IMPLEMENTING AGENCIES & ANYONE INTERESTED IN CCB

CYBIL IN NUMBERS

- 665 PROJECTS
- TOOLS
- 105 PUBLICATIONS
- 581 ACTORS
- 21 UPCOMING EVENTS
- 1000+ VISITORS A MONTH

WHAT TO DO ON CYBIL

- SHARE KNOWLEDGE TO SUPPORT CYBER CAPACITY BUILDING EFFORTS
- FIND OUT WHO IS DOING WHAT AND WHERE
- LEARN FROM GOOD PRACTICES AND EXPERIENCES
- CHOOSE RELEVANT TOOLS FOR YOUR NEEDS
- PUT EVENTS ON YOUR RADAR

GET IN TOUCH

VISIT THE WEBSITE OR EMAIL US!

CYBILPORTAL.ORG
CONTACT@CYBILPORTAL.ORG

Global Cyber Security Capacity Centre
International Cyber Policy Centre
Norwegian Institute of International Affairs
FIRST
GFCE
DiPLO

CAPACITY BUILDING AND INCREASING INTERNET ACCESS: CYBERSECURITY REALITIES IN LATIN AMERICA AND THE CARIBBEAN AMIDST COVID-19

Written by: Gabriela Montes de Oca, Cybersecurity Program Officer, Organization of American States Inter-American Committee Against Terrorism; and Valentina Uribe, Intern, Organization of American States Inter-American Committee Against Terrorism

The global pandemic has increased our reliance on the internet and other digital avenues for performing daily activities. Shopping, studying, working, and even meeting with friends has moved online. This increased dependence on being digitally connected all the time, and for almost everything, has made us more vulnerable to cyber-attacks. In Latin America, the reality is mixed: as the whole region seeks to find solutions to the pandemic, governments have also taken this opportunity to revise and redefine what cybersecurity means for them and to prepare for upcoming challenges.

Latin America's digitalization: A work in progress

In recent decades, the world has experienced a growing process of digitalization. New technologies such as machine learning, artificial intelligence, and 5G, among others, have emerged, radically transforming the way our societies operate. Technical infrastructures and support systems have been updated to keep up with new sectors moving their operations online. Even against this backdrop of rapid digital developments, this digitalization has accelerated because of the global pandemic. According to Accenture Research, we saw three years of digital and cultural transformation from April to June of this year. COVID-19 has become the catalyst for rapid change, bringing new challenges and opportunities for governments.

One of the biggest challenges for cybersecurity, brought by the global pandemic, is the sharp increase in vulnerability to cyberattacks. Even though organizations and governments have been preparing to detect, respond, and recover from cyberattacks for some time now, many were surprised by the surge of these attacks. According to a report developed by Interpol on the impact of COVID-19 on cyber threats, in Latin America and the Caribbean, during the first months of the pandemic, there was an increase in COVID-19 themed phishing and fraud campaigns. Moreover, as many companies implemented teleworking, cybercriminals increasingly targeted employees to gain access to corporate networks to steal sensitive information.

According to Insight Crime, Brazil, Mexico, and Colombia have been the countries most affected by cyber threats during the pandemic. One study in the region revealed that 56% of the cyberattacks registered until September 2020 had targeted users and infrastructures in Brazil.

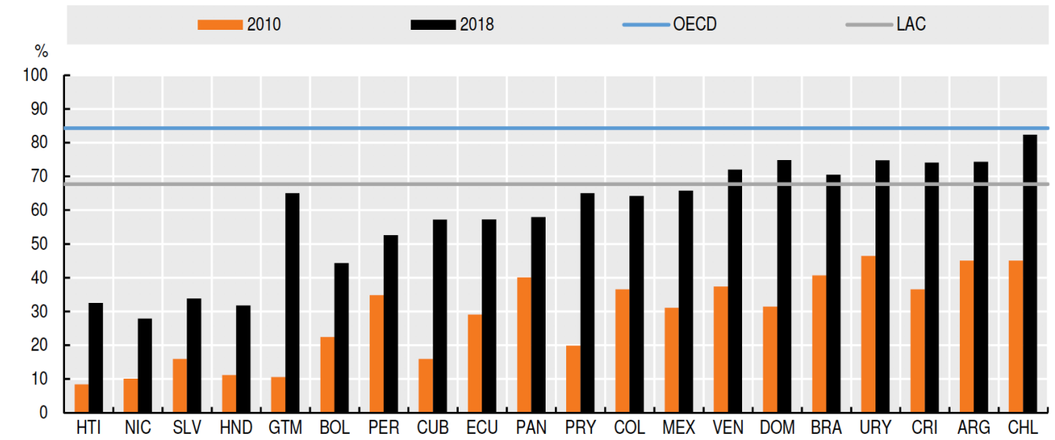


Figure 1. Percentage of Internet users in selected Latin American and Caribbean countries, 2010-2018. ECLAC.

At the beginning of the pandemic, in February, Mexico's Ministry of Economy was victim to the country's second highest profile attack, after the national oil company Pemex suffered a ransomware attack in which hackers demanded $5 million in bitcoin. In Colombia, cyberattacks increased by 59% during the pandemic, compared to the previous year. Many of these attacks were successful and caused various degrees of damage, highlighting the need to strengthen cybersecurity capabilities.

The COVID-19 crisis also confronts us with one of the most significant issues in the region: the gap in internet access. According to a report by ECLAC, 67% of Latin America's population uses the internet. However, there are strong differences between countries in the region. In countries that are considered "well-connected," internet penetration in rural areas only reaches 40-50% of the population, and in in "poorly-connected countries" that number drops to 10%. The effects of this digital divide have been even more egregious during the pandemic as individuals without internet access have not been able to continue with their education, work responsibilities, or perform other activities that have moved online. As a result, governments in the region have become more aware of the need to invest more in internet access and cybersecurity.

Even before the pandemic, Latin America and the Caribbean already faced many challenges regarding cybersecurity when compared with other regions. According to a recent report published by the OAS with the Inter-American Development Bank's (IDB) support, Latin America and the Caribbean is still at a start-up stage regarding its cybersecurity maturity level. Many countries still do not have National Cybersecurity Strategies, and economies depend mostly on small and medium enterprises (SMEs), which do not always have adequate protection against cyberattacks. On the bright side, some countries have developed capacity building initiatives and programs to strengthen their cybersecurity capabilities, but there is still a lot of work to be done.

> "Addressing cyber challenges, especially during a pandemic, requires a strong commitment to cybersecurity."

Providing solutions for the region: How the OAS has adapted to the current pandemic and continues to provide cybersecurity knowledge and best practices

Addressing cyber challenges, especially during a pandemic, requires a strong commit-

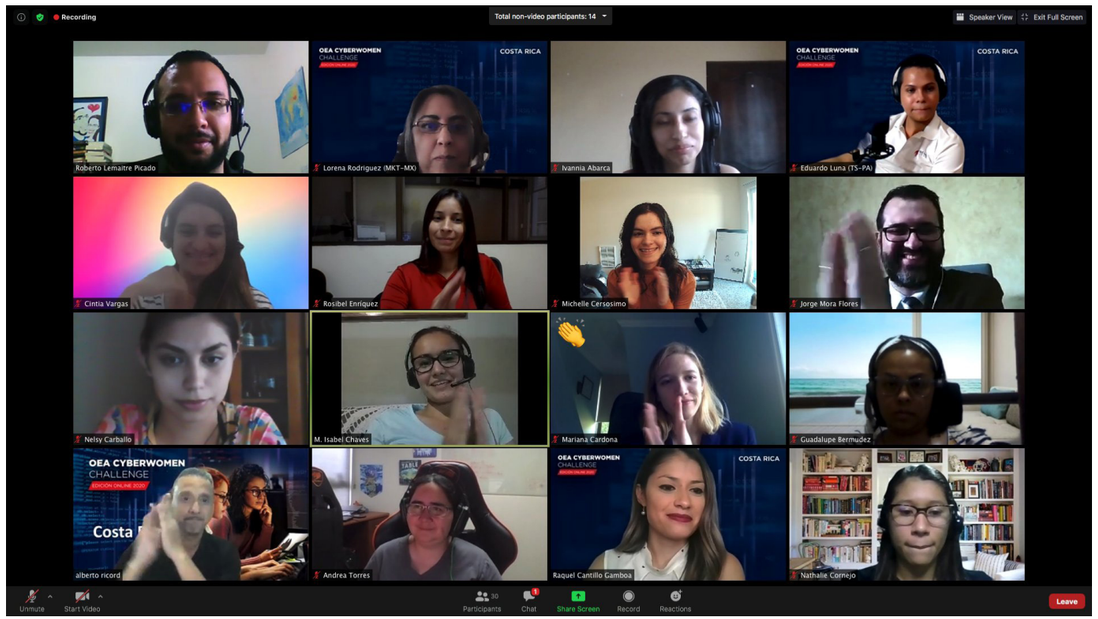


Figure 2. The OAS and TrendMicro Cyber Women Challenges have been carried out since 2018 to contribute to a more diverse and gender-inclusive cybersecurity workforce. In 2020, due to the pandemic, all challenges have been conducted online and have counted with the participation of more than 350 women in Latin America.

ment to cybersecurity. For this reason, since the beginning of the pandemic, the Cybersecurity Program of the Organization of American States has quickly adapted to the new digital reality to continue offering member states workshops and training in cybersecurity, promoting access to relevant information, and supporting the development of National Cybersecurity Strategies.

During the pandemic, the OAS Inter-American Committee against Terrorism's Cybersecurity Program has adjusted the format of different events, such as the Cybersecurity Symposium and the Cybersecurity Summer Bootcamp, among many other capacity-building activities, including the Cyber Women Challenge and the "Creating a Career Path in Cybersecurity" workshop, done in conjunction with private sector partners. Likewise, the program has published multiple reports such as "Cybersecurity Education, Planning for the Future Through Workforce Development" with Amazon Web Services and "Cybersecurity. Risks, Progress, and the Way Forward in Latin America and the Caribbean" with the IDB, to disseminate relevant information about cybersecurity gaps, opportunities and the need to create a more prepared workforce to face upcoming challenges.

Similarly, to address the increased interest from the public, the OAS Inter-American Committee against Terrorism's Cybersecurity Program has also organized more than 10 webinars and panels, which involved the participation of more than 5,000 people since March 2020. The topics have included strategies to stay cyber secure while transitioning to remote work, cybersecurity for families and women in cybersecurity.

National governments have also understood the urgency and started to focus on developing their National Cybersecurity Strategies to respond to the heightened digital threats during the pandemic. Consequently, the OAS Inter-American Committee against Terrorism's Cybersecurity Program has supported countries such as Belize, Barbados, Guyana, and Jamaica in the development, update and/or launch of their National Cybersecurity Strategies this year. To date, 13 countries in the region have developed their own strategies.

CSIRTAmericas, the OAS' hemispheric network of computer security incident response teams (CSIRTs), has also played an essential role during these times by promoting information exchange within the Americas, which is critical to manage and respond to cyberattacks. During the first semester of 2020, CSIRTAmericas organized three regional virtual meetings, sent more than 20 notifications and alerts related to COVID-19, shared more than 15 technical reports, and trained more than 60 incident responders in collaboration with the OAS Inter-American Committee against Terrorism's Cybersecurity Program.

Conclusions

During this process, the Organization of American States has learned key best practices to continue strengthening cybersecurity capacities in the region:

1. National Cybersecurity Strategies are now more important than ever: Although the COVID-19 crisis is primarily related to health institutions, the sharp increase in cybersecurity attacks can bring significant costs to a country's economy, services and critical infrastructures. In this sense, the development, update and continuous work around national cybersecurity strategies can serve as a main framework to rally different sectors of society and mitigate the costs and consequences of cyber-attacks.
2. Regional collaboration means regional capabilities: Although the region presents different realities, Latin American and Caribbean countries can benefit from continuous collaboration and the exchange of information and participation in regional forums, such as those organized by the OAS.
3. Respond to local realities: Although there is a growing amount of information and advice on the crisis from a cybersecurity standpoint, countries must advance legislation, policies and initiatives that respond to their own reality and from a multi-stakeholder approach. In Latin America and the Caribbean, it is important to recognize that cybersecurity must be paramount in guaranteeing and improving internet access for all.

The COVID-19 crisis increased our reliance on the Internet, and with that, our vulnerability to cyberattacks. Because of the unique reality of the Americas, it also provided governments and institutions with opportunities to strengthen their cybersecurity capabilities, and to look at their strengths and areas of opportunity from a different standpoint. The different ways in which the pandemic has affected the cybersecurity of various countries highlights, now more than ever, the importance of maintaining and reinforcing the commitment to upholding cybersecurity as a shared responsibility.

Figure 3. In 2019, the OAS and Cisco created the Cybersecurity Innovation Councils to support the creation of new solutions to cybersecurity problems in the region. This year, both organizations have organized three virtual councils in Mexico, Colombia and Chile, bringing together representatives from the private, civil and public sectors to discuss national cybersecurity issues.

"The pandemic [...] highlights, now more than ever, the importance of maintaining and reinforcing the commitment to upholding cybersecurity as a shared responsibility."

MEXICO´S STANCE WITH REGARDS TO CYBERSECURITY: RECENT EXPERIENCES AND CHALLENGES AHEAD

Written by: Isaac Morales Tenorio, Coordinator for Multidimensional Security, Multilateral Desk of the Secretariat of Foreign Affairs Mexico; and Valeria Solis Rivera, Director for Cybersecurity and Drug Policy Issues, Multilateral Desk of the Secretariat of Foreign Affairs Mexico

Information technologies and the expansion of the development possibilities that they bring with them are a prioritized area for governmental, industrial, social and even ethical spheres today. By recounting recent developments in Mexico regarding cybersecurity and cyberspace governance, this article emphasizes the importance of materializing a balance between security concerns and opportunities for development and the protection of human rights, in a country which is confident of multilateral fora as the best and more comprehensive way to address these issues.

A global challenge

The technological evolution must go hand in hand with rapidly evolving policies to keep up with new trends and establish strategic guidelines that allow for better harnessing of opportunities and better forecast of the associated risks and cross-cutting challenges.

Mexico has always considered cybersecurity challenges as a global issue which requires a combination of local, national, regional and international efforts. In this regard, Mexican authorities are confident that discussions on the applicability of international law and multilateral pathways would help to better address and find long term commitments. The ultimate goal of participating in international fora is to put national priorities, needs and inter-ests on the table, while aiming at echoing international best practices and lessons learned through internal policies and programs.

Mexico has been actively engaged with the UN, OAS and other cyber stability and capacity building oriented international fora. This includes the Global Forum on Cyber Expertise (GFCE), where Mexico, as one of the first Latin American members of the GFCE, has found a perfect platform to share concerns and ideas to respond to the most important cyber needs and challenges.

> "The ultimate goal of participating in international fora is to put national priorities, needs and interests on the table, while aiming at echoing international best practices and lessons learned through internal policies and programs."

At the national level, Mexico does not currently have a central or unique national authority to address cybersecurity issues. The national model is based on inter-agency coordination, giving a national specialized inter-agency Committee a key role. At the moment, there are some legislative discussions aimed at improving national structures and norms to respond to cybersecurity challenges. Based on Mexico's experience, decisions related to international cooperation, should consider confidence building measures and capacity building opportunities.

> "Based on Mexico's experience, decisions related to international cooperation, should consider confidence building measures and capacity building opportunities."

Figure 1. The office building of Mexico's Secretario de Relaciones Exteriores (Secretariat of Foreign Affairs).

Mexico's National Cybersecurity Strategy

This recent experience points to the first National Cybersecurity Strategy which was drafted and developed through quite an innovative approach. This approach involved the support and advice of the OAS/CICTE Cybersecurity Program, and an open dialogue with all the relevant stakeholders in the process (government, private sector, academia, civil society and the end-user). This approach was considering to be quite unique globally, regionally and nationally, and has turned out to be both innovative and beneficial in the medium term.

Mexico became the fifth Latin American country to draft a National Cybersecurity Strategy in 2017. Mexico's strategy consisted of 5 strategic objectives, along with 3 guiding principles and 8 cross-cutting pillars that aligned with the 5 dimensions of the global Cybersecurity Capacity Maturity Model (CMM): i) cybersecurity policy and strategy; (ii) cyber culture and society; (iii) cybersecurity education, training and skills; (iv) legal and regulatory frameworks; and (v) standards, organizations, and technologies.

In executing this enormous drafting effort, not only did Mexico have to coordinate a significant number of agencies and actors, which shared big stakes in the matter, but it also had to articulate a correlated responsi-

bility of end-users, conservatively estimated at around 70 million people (from a total population of 124.8 million). With this, Mexico achieved a cybernetic foundational base, which also highlighted the many challenges ahead, specifically at the national level.

Challenges ahead

The number of cybersecurity challenges has not and will not stop increasing, due to the growing dependence on technologies in the economic, social, political and technical realms. In the very particular case of Mexico, much still needs to be done from within. Some first crucial steps have been taken and we can be sure that the appetite for achieving a much more consolidated approach towards cybersecurity is a reality.

We must now strive towards ensuring that its relevance permeates all the multiple dimensions of the political agenda for it to grow in importance exponentially. That is why Mexico is always looking to balance at least three elements: a) to identify all the peaceful uses and potential of cyberspace and digital technologies to promote development, universal access to them and bridge inequalities; b) to protect fundamental freedoms in cyberspace and guarantee the exercise of human rights online; c) to promote a secure cyber environment where the rule of law and stability are preserved. The way ahead should allow us to:

1. Issue new relevant legislation in order to strengthen and allocate appropriate resources for local norms and structures;

Figure 2. Mexico continues to contribute to international cybersecurity efforts.

2. Further advance efforts to investigate and prosecute new and emerging cybercrimes, and to better register digital evidences and data protection, collection, and preservation of information in the systems;

3. Achieve more institutionalized and continuous dialogue with private sector, civil society and the research and academia sector, including the involvement of the private sector and internet service providers with regards to their obligations to keep track of IP addresses;

4. In order to develop a further skilled workforce to deal with current and future cyber challenges, increase the formation and capacity building in cybernetic and information technologies as well as engineering careers and curricula related to cyber and telematic issues, all this with a gender perspective;

5. Define both the wider digital transformation and wider cybersecurity agendas, to include developments in the fields of Artificial Intelligence, Digital Forensics, and Machine Learning;

6. Consolidate programs aimed at increasing "digital opportunities", bridge gaps and ensure greater capabilities for all citizens, considering their needs according to age, gender and socioeconomic status;

7. Implement better awareness campaigns aiming to promote safe-use habits, to develop and expand the culture of protecting information systems amongst all users.

Capacity building is fundamental to address challenges in order for national agendas to work. Although both nationally and internationally, the issue might seem to be an "a la carte" one, where we make decisions according to our needs, it is increasingly becoming a core issue where key rules must apply and intertwine both at the physical and cyber realm. Furthermore, gradual progress needs to be made in a coordinated way together with the respective and precise capability development, since the lack of digital or cybernetic skills can also limit the adoption of digital or cybernetic tools.

In addressing challenges, Mexico also recognizes the important value of continuing to launch initiatives in the cyber realm considering three basic degrees of technical cyber knowledge. The first relates to ensuring inclusive digital access for all users or potential users of digital technologies, with the aim to raise awareness for safer use. The second relates to current users who need to sustain safe online and digital habits while exercising their informed and consented right to privacy with regards to their own data. The third corresponds to more advanced technology users who can comfortably encrypt their own information and even respond to potential minor cyber threats, which will consequently need more specialized and advanced skills to become innovative and competitive in the digital and cybernetic world and even within an eventual national cyber industry.

"Capacity building is fundamental to address challenges in order for national agendas to work. Although both nationally and internationally, the issue might seem to be an 'a la carte' one, where we make decisions according to our needs, it is increasingly becoming a core issue where key rules must apply and intertwine both at the physical and cyber realm."

5G IN LATIN AMERICA: MORE THAN A NEW MOBILE TECHNOLOGY

Written by: Gabriela Montes de Oca, Cybersecurity Program Officer, Organization of American States

The deployment of 5G around the world has increasingly gained momentum and become a reality for different countries. The discussion around its benefits usually centers around increased connectivity and economic growth, with a specific focus on its potential to improve communications and create jobs. The Latin American and Caribbean region is no exception, but as it prepares to advance and deploy this technology, cybersecurity considerations need to be at the forefront of such discussions, ensuring a digital transformation that results in safer lives for all citizens.

Mobile connectivity in Latin America: A reality of its own

According to the Organization for Economic Cooperation and Development, by 2017, 62% of the Latin American and Caribbean population were connected to internet, with around 200 million people offline. Despite significant infrastructure and deployment developments, the quality of the internet at that time, and today, continues to be limited and unreliable across many parts of the region. This reality separates the region from many others in the world and is especially relevant when considering the impact of mobile technologies for millions of people.

In terms of mobile penetration, the numbers are considerably higher. By 2019, GSMA highlighted there were 422 million unique mobile subscribers across Latin America, or 67% of the total population. The industry is also growing exponentially, and just in 2018, their services generated 5% of GDP in Latin America, a contribution that amounted to around $260 billion in economic value added. However, mobile technologies are adopted very differently in every country in the region. According to the Open Signal's State of LTE Report, the availability of fourth generation (4G) wireless technology ranges considerably in Latin America, with high levels in countries such as Peru and Mexico, which have more than 80% coverage, and very low levels in countries such as Venezuela, where the political conditions affect the reach of these technologies.

In the context of this growth, the race for 5G has already begun, as discussed by the Inter-American Development Bank's report "5G The Driver for the Next-Generation Digital Society in Latin America and the Caribbean". In 2019, Uruguay became the first Latin American country to make the first 5G call on a commercial network through ANTEL, the Uruguayan state-owned telecommunications operator. Similarly, Brazil has already made agreements with partners such as the European Union, the United States and South Korea on 5G support. Colombia, Mexico, Argentina, Ecuador, Dominican Republic and Chile have also signed memorandums of understanding with private and public sector partners and have begun conducting tests.

According to GSMA, 5G adoption in Latin America will reach 7% by 2025, with Mexico, Brazil, Colombia and Uruguay, leading this development. However, due to the COVID-19 pandemic, it also highlights that the

Figure 1: Latin American governments have already scheduled bidding and deployments of 5G technologies in the region in accordance with local regulations and objectives. Source: Competitive Intelligence Unit (2020).

4G is set to become the region's dominant technology by 2020

% of connections (excluding licensed cellular IoT)

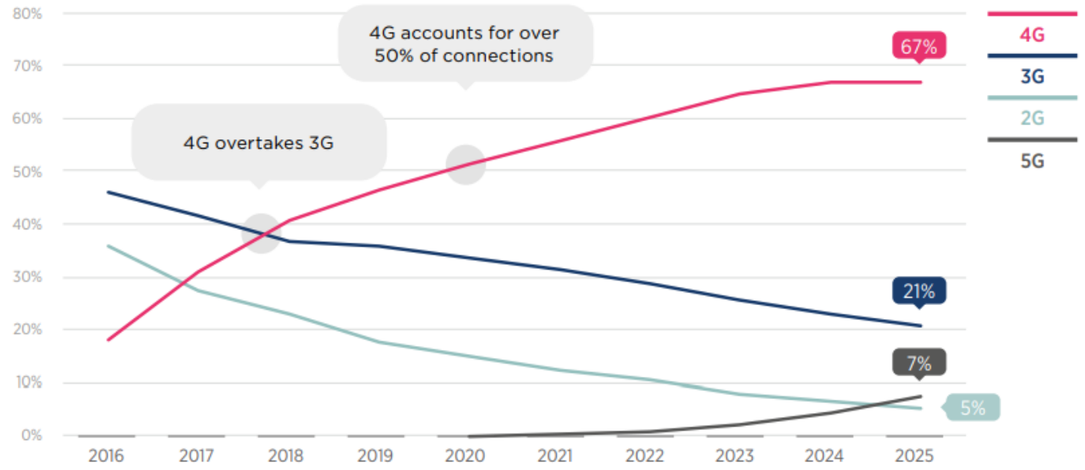


Figure 2: Convergence of mobile technologies in Latin America (2016 to 2025). Source: GSMA (2019).

deployment of 5G has also been affected. In particular, "5G spectrum auctions could potentially be delayed as operators weigh the risk of long-term investments across the region against current financial developments caused by the crisis." 5G's cybersecurity lessons from around the world

5G's cybersecurity lessons from around the world

As mentioned before, one of the main concerns about the development of 5G in Latin America and around the world refers to its associated infrastructure, deployment and maintenance, especially in a region where COVID-19 has severely affected the economy. However, as with any other new technology, Latin American countries must consider the associated cybersecurity risks that come with 5G. In particular, they can benefit from the expertise provided by the European Union and the United States, among others, on how to identify and mitigate risks.

First, the National Cybersecurity Agency (CISA) of the United States has identified that 5G implementation can introduce vulnerabilities in the following areas:

- Supply chain: Specifically, malicious or unintentional introduction of risks like malicious software and hardware, counterfeit components, among others.

- Deployment: Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to disruption and manipulation.

- Network Security: Existing vulnerabilities in 4G LTE networks that contain unresolved vulnerabilities may affect 5G equipment and networks even with additional security enhancements. This is especially relevant for the region, especially as GSMA predicts that 4G and 5G

- Competition and Choice: Despite the development of standards that encourage interoperability, some companies are building proprietary interfaces into their technologies, limiting customers' choices to use other equipment. This lack of interoperability limits the ability of trusted ICT companies to compete in the 5G market.

"As private companies and the general population prepare for and anticipate the development of new mobile technologies, such as 5G, policymakers must be proactive in the creation of regulations that respond to their associated threats."

Similarly, the European Union created a toolbox titled "Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures", which recommends the following measures to mitigate these risks:

- Strengthen security requirements for mobile network operators;

- Assess the risk profile of suppliers;

- Apply relevant restrictions for suppliers considered as high risk, including necessary exclusions for key assets; and

- Ensure that each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier and avoid dependency on suppliers considered high risk.

Case Study: Colombia's 5G Plan

In June of 2020, Colombia released its 5G Plan , which addresses the benefits and opportunities that the deployment of 5G might bring to the Colombian population in the long term. The document also highlights that just like with any other technology, 5G needs to be assessed carefully in terms of cybersecurity. In particular, the document highlights that "Security risks and threats to security and privacy will be a point of crucial importance to consider both in planning, enlistment, provisioning and assurance of services, all the more because its special characteristics will allow an immense flow of exchange of data, not only between users but between things (IoT), among which could be immersed those of malicious type or those of malicious access or those used for extraction of fraudulent data."

As recognized by this plan, the deployment and transition from these 3G to 4G and 5G, as well as the threats they present, are framed within two guidelines created by the National Council for Economic and Social Policy. The first guideline (CONPES 3701), created in 2011, serves as the main source on cybersecurity and cyber defense, and serves as the main policy document related to Colombia's national cybersecurity strategy. Additionally, in 2016, the government approved the National Digital Security Policy, which includes risk management as a key component to tackle digital security.

Although 5G was not a possibility when these two guidelines and laws were created, the government has noted that they represent a starting point for tackling new technological developments, and for upholding the country's main cybersecurity priorities when discussing the details of 5G deployment in charge of certain companies and local operators.

As private companies and the general population prepare for and anticipate the development of new mobile technologies, such as 5G, policymakers must be proactive in the creation of regulations that respond to their associated threats. Specifically, as some countries are updating or creating their national cybersecurity strategies, it is recommended that they reflect the state of mobile developments in the country, considering the cybersecurity threats that 5G might enable and resolving past vulnerabilities that could hinder its possible benefits. Similarly, these laws should also reflect the new realities pertaining data access and surveillance.

Although the digital divide in Latin America and the Caribbean persists, mobile deployments will continue and spread the opportunities of the digital revolution in the region. With cybersecurity in mind, its deployment will bring a safer and more stable cyberspace for all.

COORDINATING A GLOBAL NETWORK FOR CYBER CAPACITY BUILDING

Written by: Kathleen Bei, Advisor, GFCE Secretariat

As the GFCE celebrates its 5th Anniversary in 2020, the GFCE Secretariat looks back at the GFCE's achievements and ambitions towards 2021. To enhance the GFCE's efforts in coordinating a global network for cyber capacity building and strengthen the GFCE ecosystem to support the practical implementation of cyber capacity building, the GFCE seeks to increase its regional focus, enhance collaboration, and secure high-level political recognition for cyber capacity building.

Five Years of the GFCE

In recent years, we have seen a growing global consensus on the importance of cyber capacity building and the need to improve coordination of capacity building efforts. The COVID-19 pandemic has brought about a rapid shift online in many aspects of our lives, further amplifying the importance of cybersecurity, and consequently the need to strengthen cyber capacity and expertise globally.

It was for precisely this reason that the Global Forum on Cyber Expertise (GFCE) was established five years ago; anticipating the need for a global pragmatic coordinating platform for international collaboration on cyber capacity building. To achieve its mission, the GFCE has focused on the following strategic goals:

- Coordination: avoid duplication and fragmentation of CCB efforts globally by supporting coordination activities;
- Knowledge sharing: make relevant CCB knowledge and expertise available on a global scale;
- Matchmaking: match requests of cyber capacity needs from GFCE members with offers of support.

Over the last five years, with the input and participation of its multi-stakeholder community, the GFCE has met some significant achievements:

- Growing the GFCE network from 42 members (2015) to over 120 members and partners today;
- On the ground presence in the Pacific, Africa, Europe, Asia, and the Americas, with the GFCE Community representing all continents;
- Developing and endorsing the 2017 Delhi Communique on a GFCE Global Agenda for Cyber Capacity Building;

Figure 1. Growth of the GFCE ecosystem in five years.

- Establishing the five GFCE Working Groups, the driving force of the GFCE;
- Supporting several countries with their request for assistance on, for example, National Cybersecurity Strategy, Critical Infrastructure Protection or Cybercrime Legislation through the GFCE Clearing House;
- Making practical knowledge and proven solutions available to the global community through Cybil, a dedicated CCB knowledge portal (www.CybilPortal.org);
- Developing a Global Cyber Capacity Building Research Agenda process, to address knowledge gaps with data and evidence;
- Establishing the GFCE Foundation and the Foundation Board, adding a strategic entity to the existing GFCE structure; and
- Organizing over 50 global and regional events around the world in the last five years.

Figure 2. The six strategic building blocks for the GFCE towards 2021.

What's next?

Based on the input of the GFCE Community during a series of virtual consultations in May this year, the GFCE Foundation Board has formulated six strategic building blocks for the GFCE. These building blocks give strategic direction for 2021, to enhance the GFCE's efforts in coordinating a global network for cyber capacity building and strengthen the GFCE ecosystem to support the practical implementation of cyber capacity building.

Increase regional focus and support practical implementation

Global coordination is important to amplify capacity building efforts and ensure greater effectiveness and efficiency. The GFCE's efforts to build regional nodes and further increase its regional focus in 2021 is an efficient approach to realizing global coordination, as this highlights regional perspectives and priorities for capacity building. In 2020, the GFCE held two regional meetings in Europe and in the Pacific. Other regional meetings for Africa, Southeast Asia and the Americas had to be postponed due to the COVID-19 pandemic. The GFCE aims to hold more regional meetings in 2021, exploring possibilities of hybrid or virtual formats if traveling remains a challenge.

> "The GFCE's efforts to build regional nodes and further increase its regional focus in 2021 is an efficient approach to realizing global coordination, as this highlights regional perspectives and priorities for capacity building."

Africa has been an important region full of potential for the GFCE and its work on coordinating cyber capacity building, as various GFCE members and partners are involved in cyber capacity building projects in the region. Therefore, the GFCE has partnered with the AU on a 2-year project, supported by the Bill and Melinda Gates Foundation, to develop cyber capacity building and support African countries in strengthening their cyber resilience (read more: page 18). The GFCE has also partnered with Microsoft on a dedicated program within the GFCE Secretariat to increase cyber capacity building efforts in the region.

As a result of the Pacific Regional Meeting, the GFCE has also recently begun work on a scoping assessment for a future GFCE Pacific Hub, led by new GFCE Pacific Liaison, Cherie Lagakali (read interview: page 4). The future Hub would aim to fill gaps in specific areas of capacity building and improve coordination and information sharing between Pacific Island countries, regional and international donors and implementers.

Enhance collaboration

Towards 2021, the GFCE also aims to enhance collaboration within the GFCE community to better connect and strengthen the GFCE ecosystem. The GFCE tools, which have been refined and developed over the course of 2020, are important for the GFCE to support the practical implementation of cyber capacity building through coordination, knowledge-sharing and match making. These tools are the Cybil Knowledge Portal (read more: page 66), the GFCE Clearing House and the new Global Cyber Capacity Building Research Agenda. In 2020, the GFCE is testing the first development of the Global CCB Research Agenda process and has collected and prioritized 15 research ideas for the draft Research Agenda 2021.

> "The GFCE tools, which have been refined and developed over the course of 2020, are important for the GFCE to support the practical implementation of cyber capacity building through coordination, knowledge-sharing and match making."

Build awareness and securing political recognition

In order to continue multiplying the successes of the GFCE and enlarge the pool of international resources for cyber capacity building, the GFCE notes that it is necessary to create greater awareness on and secure high-level, political recognition for cyber capacity building. The GFCE seeks to connect and cooperate with other important platforms and processes in the field, such as the UN OEWG, and has submitted comments to the OEWG initial pre-draft as well as the capacity building discussion questions during the 3rd round of informal meetings. The GFCE also calls on the UN to address integrating cyber capacity building into UN development agendas, as this alone could have a tremendous impact on the prioritization and funding for cyber capacity building.

During the GFCE Annual V-Meeting 2020, the GFCE community will also explore the idea of the GFCE convening a high-level political conference in 2021 in collaboration with states, development organizations and others, to raise the profile and allocation of resources for cyber capacity building and encourage global coordination and cooperation between existing entities.

Share your needs and ideas

As we continue to look for ways to strengthen the GFCE ecosystem and support global cyber capacity building efforts, it is important for the GFCE Community to continue voicing its capacity needs, and ideas on how we can bring greater awareness to the GFCE's work and support international efforts both within and outside the community. If you have any ideas, suggestions or questions, please get in touch with the GFCE Secretariat by emailing contact@thegfce.org.

COLLABORATIVE EFFORTS FOR EMPIRICAL CAPACITY BUILDING

Written by: Kate Pacalt-Shady, Head of Marketing and Communications, Oceania Cyber Security Centre (OCSC); Dr James Boorman, Head of Research and Capacity Building, OCSC; Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Centre (GCSCC); and Dr Enrico Calandro, Co-Director, Cybersecurity Capacity Centre for Southern Africa (C3SA).

The COVID-19 pandemic has accelerated digital transformation at a pace that often exceeds the time required to appropriately manage risk. Some of the well-known benefits of digital transformation include reducing cost and increasing accessibility of services; creating new ways to work, trade and learn; and connecting people to new and existing communities. At the same time, digital transformation brings about risks that need to be managed both in terms of securing information and understanding threats to interacting online. When building capacity to manage risk and respond to cyber threats it is important to understand the situation, the operating environment and the outcomes. In other words, what works, what doesn't work and why.

The CMM and its impact

While efforts by the global community to proactively address cybersecurity problems are valuable, there is little empirical research on whether they achieve their intended objectives. Many capacity-building initiatives happen in siloes, may duplicate efforts and lack evidence of impact (see Creese, Esteve-González, Shillair, Dutton (2019). Cyber Security Capacity Building: A Cross-National Empirical Study). In response to this problem the Global Cyber Security Capacity Centre (GCSCC) together with its strategic and regional partners has been focusing on developing, deploying and refining a cybersecurity capacity maturity framework for understanding what works, what doesn't work and why. Since 2015 reviews based on the Cybersecurity Capacity Maturity Model for Nations (CMM) have been completed more than 110 times in 84 countries, including two regional studies by the Organization of American States (OAS) and 26 reviews in cooperation with or by the World Bank. The findings and recommendations from these CMM reviews have provided governments, funders and implementers a baseline to guide capacity building and investment. In response to technological changes and policy trends, the CMM has been reviewed and updated through two consultation processes with leading academics and cybersecurity experts from around the world. The third version of the CMM will be launched early 2021.

"For participating countries, the CMM reviews have played a key role in determining the status of capacity maturity; identifying gaps; assisting in decision making on future capacity building and investments; and enabling coordination of efforts."

For participating countries, the CMM reviews have played a key role in determining the status of capacity maturity; identifying gaps; assisting in decision making on future capacity building and investments; and enabling coordination of efforts.

A 2020 external study commissioned by the UK Foreign, Development & Commonwealth Office (UK FCDO) found that CMM reviews "drive enhanced awareness and capacity-building in the area of cybersecurity, provided a foundation for the national cybersecurity strategy development and improved credibility of the cybersecurity agenda within governments."

Countries from all parts of the world also expressed that "the CMM helped to define roles and responsibilities within government, resulted in increased funding for cybersecurity capacity-building and underpinned capacity building programmes by international partners."

The Global Constellation

In order to increase the impact of the global research project, to assure a sustained and contextualised application of the CMM, and to build regional expertise on cyber capacity research, the GCSCC began the process of building a Constellation of Regional Research Centre partnerships.

The Oceania Cyber Security Centre (OCSC) a not-for-profit collaboration of eight Victorian Universities in Melbourne Australia, funded by the State Government of Victoria for a four-year engagement became the first foreign government alliance in the Constellation in 2017.

In 2020 the Cybersecurity Capacity Centre for Southern Africa (C3SA) was established at the University of Cape Town (UCT) as a consortium between the GCSCC, UCT's Department of Information Systems, Research ICT Africa, a digital-policy think tank based in Cape Town, and NUPI. C3SA is funded by the Norwegian Ministry of Foreign Affairs for a two-year engagement.

"[The] CMM Review clearly showed not only the shortcomings of existing frameworks [of cybersecurity capacity used in country], but also interconnections between these areas." Government representative from European country, survey response

"It [the CMM Review process] created awareness and opportunity for different stakeholders to take ownership of the topic." Government representative from Pacific country, interview

"[The CMM] is a very, very good tool that governments can use to guide their efforts around cybersecurity … we're looking forward to the next review." Government representative from African country, interview

"[The CMM Reviews] improved the collaboration and coordination between Government agencies to attend [to] the issue of cybersecurity." Government representative from Latin American & Caribbean country, survey response.

"The Constellation Partners lead the deployment of the CMM in their respective regions and provide a point of contact for international partners and regional governments seeking to engage in the CMM review process."

The Constellation Partners lead the deployment of the CMM in their respective regions and provide a point of contact for international partners and regional governments seeking to engage in the CMM review process. They offer a localised presence and promote international relations, contextualised capacity building, project engagement and coordination of implementation.

This positioning contributes to a deeper local understanding of what constitutes cybersecurity capacity at a national level and collectively is a cornerstone for regional cybersecurity capacity building and national security.

Further, this regional know-how contributes to GFCE's efforts in reducing duplication in resource allocation and efforts in enhancing global coordination and collaboration.

The Constellation's Strategic Partners

The uptake by nations and the support from strategic partners and other implementers in the development and deployment of the CMM has been critical to the success of the CMM reviews and their impact on capacity building across the world including: the World Bank; the Organization of American States (OAS); the International Telecommunication Union (ITU); the Commonwealth Telecommunications Organisation (CTO); the Asia Pacific Network Information Centre (APNIC); the Asia Pacific Telecommunity (APT); NRD Cyber Security, the Norwegian Institute of International Affairs (NUPI); GIZ Germany; and the GFCE.

The commitment of governments and the Global Constellation's strategic partners has been trifold;

1. to provide funding to operationalise the CMM review project with the nation, in country;
2. to adopt, prioritise and implement the CMM's multi-dimensional recommendations with and for the nation; and
3. to use the evidence-based recommendations as a baseline for every dimensional capacity building project and re-assessments driving continual improvement.

This collaborative approach being key in supporting the global cybersecurity capacity agenda and efforts.

The CMM Research and COVID-19

The CMM reviews continue to provide recommendations for host nations to strengthen their cybersecurity capacity and build resilience, while providing essential data for research. Initial correlation analysis of the CMM data across the world so far enhances empirical support to international efforts aimed at building cybersecurity capacity, further illustrating that the level of capacity building in most nations is at the very early stages of development. These findings reinforce the case that more initiatives are needed to bolster cybersecurity capacity, with greater attention aimed at decreasing the divide between low- medium and high-income nations.

CMM reviews in numbers:

119 CMM reviews
84 countries assessed
35 reassessments

Region:
Africa: 25
Asia: 10
Europe: 10
Latin America and the Caribbean: 32
Oceania: 7

*Development Status**:
High-Income Economies: 14
Upper-Middle-Income Economies: 31
Lower-Middle-Income Economies: 25
Low-Income Economies: 14

Population:
<1 million: 21
>1 million <10 million: 29
>10 million <100 million: 29
>100 million: 5

GFCE members: 50
ODA recipients: 71

* https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups

"Despite the global pandemic, the Global Constellation's priority remains: to conduct CMM reviews and contribute to the global cybersecurity capacity building agenda through high-quality research."

As with the rest of the world COVID-19 has had implications on the Global Constellation centre's operations and changes in operating environments have resulted in new opportunities. The C3SA and GCSCC piloted an online CMM in Uganda providing an interim solution in the delivery of CMM's to recipient nations (article about the lessons learnt "Reviewing cybersecurity capacity in a COVID-19 environment"). In the Oceania region the OCSC is preparing to do the same, returning to face-to-face reviews when safe to do so.

Despite the global pandemic, the Global Constellation's priority remains: to conduct CMM reviews and contribute to the global cybersecurity capacity building agenda through high-quality research.

Visit:
https://gcscc.ox.ac.uk/
https://ocsc.com.au/
http://www.c3sa.uct.ac.za/

Follow the Constellation on Social Media:
@CapacityCentre
@oceania_cyber
@C3SA_UCT

For more information on all projects that the Global Constellation partners are involved in, visit CYBIL: https://cybilportal.org/projects

ENABLING CAPACITY BUILDING THROUGH KNOWLEDGE ACCESS AND SHARING ONLINE

Written by: Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Centre (GCSCC)

Since 2019, Cybil, the cyber capacity knowledge portal, supports the GFCE's ambition to provide a neutral and open platform to access and share practical knowledge and best practices in cyber capacity building. As the COVID-19 pandemic spotlights cybersecurity risks, the need for countries to intensify their cyber capacity building efforts has become even more evident. It also changed the way of work due to global lockdowns and the cancellation of physical meetings and conferences. These developments highlight the important role that Cybil can play for knowledge sharing and supporting the effective use of resources by the global community. Owned and curated by the global community, Cybil offers easy access to a comprehensive collection of best practices, guidelines and other resources for actors to plan, implement and coordinate cyber capacity building in the thematic areas covered by the GFCE Working Groups while targeting evolving issues such as COVID-19. With these offerings produced by the GFCE and other key actors in the field on a publicly available online platform, Cybil can help to fill knowledge gaps on the 'what' and 'how' of cyber capacity building but also acts as an important way to disseminate knowledge.

A One-Stop Knowledge Hub for Cyber Capacity Building

The impact of the COVID-19 pandemic on our online experiences has reiterated the pressing need for securing networks and online services. It has also drawn the attention of governments around the world to gaps in countries' capacities, as well as the need for planning and implementing cyber capacity building (CCB) effectively. Besides sufficient resources, this requires knowledge and access to expertise and best practices, as well as the ability to cooperate and coordinate actors in the global community.

Actors in CCB are facing a number of challenges when planning, setting up, or analysing CCB programmes and projects. Beneficiary governments who want to better understand their needs, or who have already identified areas for capacity building with need for assistance, are looking for potential funders and experts in best practices to inform their agenda. On the other hand, funders might seek new opportunities to support countries in their efforts to build capacity, reduce the risks for local users, and strengthen global structures. Implementors of CCB, including GFCE members, knowledge partners, or implementors are also looking for collaborators, existing capacities, and activities to harmonise CCB activities. Last but not least, many researchers need data and resources for examining the impact of CCB and ways to improve it.

CYBIL PORTAL CATEGORY	What do you find?	What you can do?
Cyber capacity projects from around the world	**Who is doing what and where, and who is funding it?** A repository of over 660 past and present international cyber capacity building projects. This extends from national projects funded by external governments or organisations and implemented by one organisation, to multi-donor projects which cover a region or set of beneficiary countries. Project information is provided by the project owners and/or the beneficiaries or funders of activities, and/or is publicly available.	• Apply one or more filters such as geography, beneficiary group, actor type (beneficiary, funder, implementer or funder), status, GFCE themes and topics, date of update, and title (A-Z); • Export the repository in a single spreadsheet for project planning or research purposes; and • Submit projects online with a single spreadsheet
Tools to help develop your cyber capacity	**How is it done and what is best practice?** A collection of resources to help design and deliver international CCB projects. These are submitted by members of the GFCE community and curated by the GFCE Working Groups and include resources such as toolkits, best practice guides, and online resources – all of which can help in the design and delivery of international CCB projects. Outputs of the GFCE Working Groups can also be found here.	• Apply one or more filters such as GFCE themes and topics, actors, date of update and title (A- Z); • Export the collection in a single spreadsheet.
Lessons and best practices	**What was the outcome and what are lessons learnt?** A library of papers, articles, and reports analysing cyber capacity building activities and providing lessons learnt, outcomes and research for and about international CCB. Also, outputs of the GFCE Working Groups can be found here.	• Apply one or more filters such as GFCE themes and topics, actors, type of publication, year of publication, date of update. and title (A-Z); • Export the library in a single spreadsheet.
Actors and stakeholders to collaborate with	**Who is doing what in cyber capacity building?** Profiles of governments, companies, regional and international organisations, and other actors involved in international CCB as beneficiaries, funders, implementers or analysts of CCB activity.	• Apply one or more filters such as GFCE themes and topics, geography, group membership, actors, date of update, and title (A- Z); • Export the database in a single spreadsheet

Table 1.

Supporting this global CCB community is the main target group of CYBIL. The portal provides easy access to practical knowledge and best practices in CCB, as depicted in *table 1*.

From the Global Community, for the Global Community

Cybil was developed by the GFCE Knowledge Partners, the Australian Strategic Policy Institute (ASPI), DiploFoundation, FIRST, the Global Cyber Security Capacity Centre (GCSCC), and the Norwegian Institute of International Affairs (NUPI). Under the leadership of the GCSCC, these partners worked together to establish a platform which provides access to CCB knowledge to a diverse global community on different levels of capacities and various foci of work. To ensure community members can find content relevant to them, a "Getting Started Guide" on Cybil signposts users to the relevant sections on Cybil.

Since its launch at the GFCE Annual Meeting 2019 in Addis Ababa, Cybil has become a valuable resource for actors in the global CCB community to use for project proposals, identify potential partners and funders, and share knowledge and information about their activities. The GFCE community provided a constant flow of new content and updates, which is carefully curated and governed by the GFCE Working Groups and the GFCE Secretariat, who together monitor the relevance and accuracy for the needs of the community (see Cybil Curation Processes):

- GFCE members and partners contributed new project information and updates to the repository: for instance, the World Bank's Global Cybersecurity Capacity Programs I+II used Cybil to share the details of each specific country-level intervention;
- Cybil became a place for organisations analysing and conducting CCB to share reports, lessons learned, and articles. One example is the report Making Gender Visible in Digital ICTs and International Security by Global Affairs Canada;
- Outputs developed by the GFCE Working Groups were published first on Cybil An example is Lessons Learnt on Cyber Incident Management Capacity Building, which was developed by the GFCE WG B Task Force Cyber Incident Management;
- Cybil was instrumental in coordination and clearing house activities of the GFCE. In preparation of the GFCE Regional Meetings in Europe and the Pacific, for example, the Cybil repository was used as the primary source for identifying activity in the regions, and provided a starting point for coordination; and
- the Portal became the hub for documents, tools and publications presented at the GFCE V Meeting April-June 2020, including cybersecurity resources for addressing the consequence of COVID-19.

The overall aim and principle for Cybil's governance is to be as inclusive and comprehensive as possible. Therefore, several channels were introduced to enable more participants to easily submit content. For instance, a special spreadsheet guides what information is relevant for the project repository and can be uploaded easily. All content can also be sent to the GFCE Secretariat on a contact form. . Alternatively, users may email contact@cybilportal.org. These different tools increase the accessibility of the platform.

Fostering and Enabling Knowledge Sharing in COVID-19 and Beyond

The commitments of the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building 2017 are even more crucial in times when CCB and resilience become a higher priority for governments. It demands action from those funding, developing and implementing CCB in areas such as the development and promotion of good practice; identification of knowledge, developing technology and expertise gaps in the community's response; narrowing the gap between nations' CCB needs and the available resources; avoiding duplication of efforts given limited resources; identifying ways for increasing cooperation with the private sector and civil society in CCB; mapping global and regional progress in building the necessary capacities; and sharing information among stakeholders in a timely and effective manner. But during the pandemic, these efforts face increased challenges in the absence of opportunities to engage face-to-faceactivities of the CCB community moved online. One of the first examples were the online GFCE V-meetings from April – June 2020, which replaced the GFCE Working Group meetings in The Hague. The Cybil knowledge hub was used to share resources that were presented and mentioned, such as tools for governments' response to the cybersecurity implications of COVID-19. Cybil was able to prove its flexibility and the ability to respond to evolving needs of the GFCE community.

Going forward, Cybil will be developed further by the GFCE, which took over the management of the Portal from the GCSCC in September 2020. The Portal Advisory Group, which has evolved into the Cybil Steering Committee, continues to provide input and strategic advice on the future direction of CYBIL. In 2020, a digital marketing strategy will be implemented to foster CYBIL's reach within but also beyond the GFCE community. New features will be soon introduced such as an interactive map to find projects around the world, visualisations of networks and thematic coverage, an area for webinars, and multi-language access.

These efforts all contribute to the principles set out in Cybil's objectives: providing easy access to practical knowledge and best practices in CCB, neutral and open in all its work, avoiding duplication, owned and curated by the global community, meeting needs of the global community, fostering more effective use of resources among GFCE community and greater harmonisation of efforts.

How to get invovled in Cybil

- Submit your projects – past and ongoing https://cybilportal.org/submit-your-cyber-capacity-building-projects or on the contact form.
- Regularly inform Cybil about any relevant updates and developments (contact form).
- Share your publications and other outputs on Cybil (contact form).
- Let Cybil know about your events (contact form).
- Contact the Portal Steering Committee or participate in its meetings to give feedback (contact form).
- Provide funding to support Cybil (contact form).
- Email contact@cybilportal.org for more information!

Volume 8,
November 2020
Global Cyber Expertise Magazine

Colophon

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

Global Cyber Expertise Magazine

AU • EU • GFCE • OAS
contact@thegfce.org

Issue 9 submission deadline:
26 February 2021