Volume 11, September 2022

GLOBAL CYBER EXPERTISE MAGAZINE

THE GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING (GC3B): MAKING 2023 THE YEAR OF CYBER RESILIENCE FOR DEVELOPMENT

- page 12 -

African Union

GFCE

OAS More rights for more people

Volume 11,
September 2022

Global Cyber Expertise Magazine

Editorial

On behalf of the Editorial Board, I am pleased to welcome you to Issue 11 of the Global Cyber Expertise Magazine! We are proud to present this edition during the GFCE Annual Meeting 2022.

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

In this edition, our cover story takes a look at how the Global Conference on Cyber Capacity Building is making 2023 the year of Cyber Resilience for Development. Also under the global developments section, we learn about how why the resilience of NGOs in cyberspace should be a top priority and the role of the CyberPeace Builders in achieving this. Following this, we delve into how regional multistakeholder cyber capacity building is being advanced through the Global Cyber Policy Dialogues.

From the Americas, learn about the need for cyber capacity building and the cybersecurity situation of the region. Then take a look into how the region is responding specifically to the shortage of cybersecurity professionals through education, training and capacity-building opportunities.

From Europe, we have an article highlighting how the UK's Digital Access Programme offers a holistic approach to building and sustaining cyber capacity. Additionally, we have an article on strategies for cyber diplomacy capacity building.

From Africa, read about the developments of the Africa Cyber Capacity Building Committee, in addition to how African students' strategic thinking on cybersecurity is being developed through cyber policy competitions such as the Cyber 9/12 Strategy Challenge.

From Asia and Pacific, we have an article reflecting on some cyber incidents that affected the Pacific in the past year, and how these inform the role of the GFCE in supporting the Pacific's cyber capacity building efforts.

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

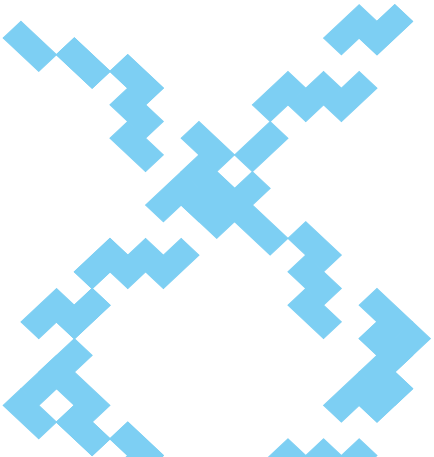
On behalf of the Editorial Board,

David van Duren
Director of the GFCE Secretariat

WHY NGO RESILIENCE SHOULD BE OUR TOP PRIORITY IN CYBERSPACE

Written by: Adrien Ogee, Operations Manager, CyberPeace Institute; Alexis Alley, Community Manager, CyberPeace Institute.

Non-governmental organizations (NGOs) are a growing target in cyberspace due to their expanding digital footprint and structural difficulties to build cyber capabilities. Cybercriminals and state actors are well aware that NGOs hold valuable assets with access to funds, trusts and valuable data.These malicious online actors are not shy to attack these vulnerable groups even if that puts orphans or migrants at risk. Beyond the collective responsibility to protect the most vulnerable - capacity building programmes for NGOs are a must if we are to preserve and build a safer cyberspace.



In the Fall of 2021 on a late Saturday evening, we received a call from a non -governmental organization (NGO) supporting orphans, globally. An on-going ransomware attack struck the NGO's files of children at risk in over 120 countries. The CEO had been notified and panicked when faced with the daunting ransome of one million euros to decrypt the information. Files, pictures and personal data of these children held by these attackers who in reality did not know they were targeting an NGO. Yet, the financial objective remained and a discount was offered in the end.

Figure 1. CyberPeace Builders.

Unfortunately, this is not an isolated incident. The majority of NGOs under attack do not report the incidents they face. However, in the last two years over 200 different NGOs have reported cyberattacks. Potentially lacking in scale or knowledge, cybersecurity becomes subordinate when comparable priorities can be a clean water source or food security.

"The majority of NGOs under attack do not report the incidents they face. However, in the last two years over 200 different NGOs have reported cyberattacks."

In 2021, Roots of Peace came to the CyberPeace Builders for help following $1.3M stolen in USAID funding intended to support Afghan farmers to grow crops on fields cleared of landmines. In 2022, over 1 billion people rely on NGO services and care. The International Committee of the Red Cross was breached leading to the loss of personal data from over 500,000 vulnerable refugees and migrants. In a reality where scarcity already affects the majority; the Philadelphia Food bank also had one million dollars stolen from them that was planned to feed part of the 10% living under the poverty line in the United States.

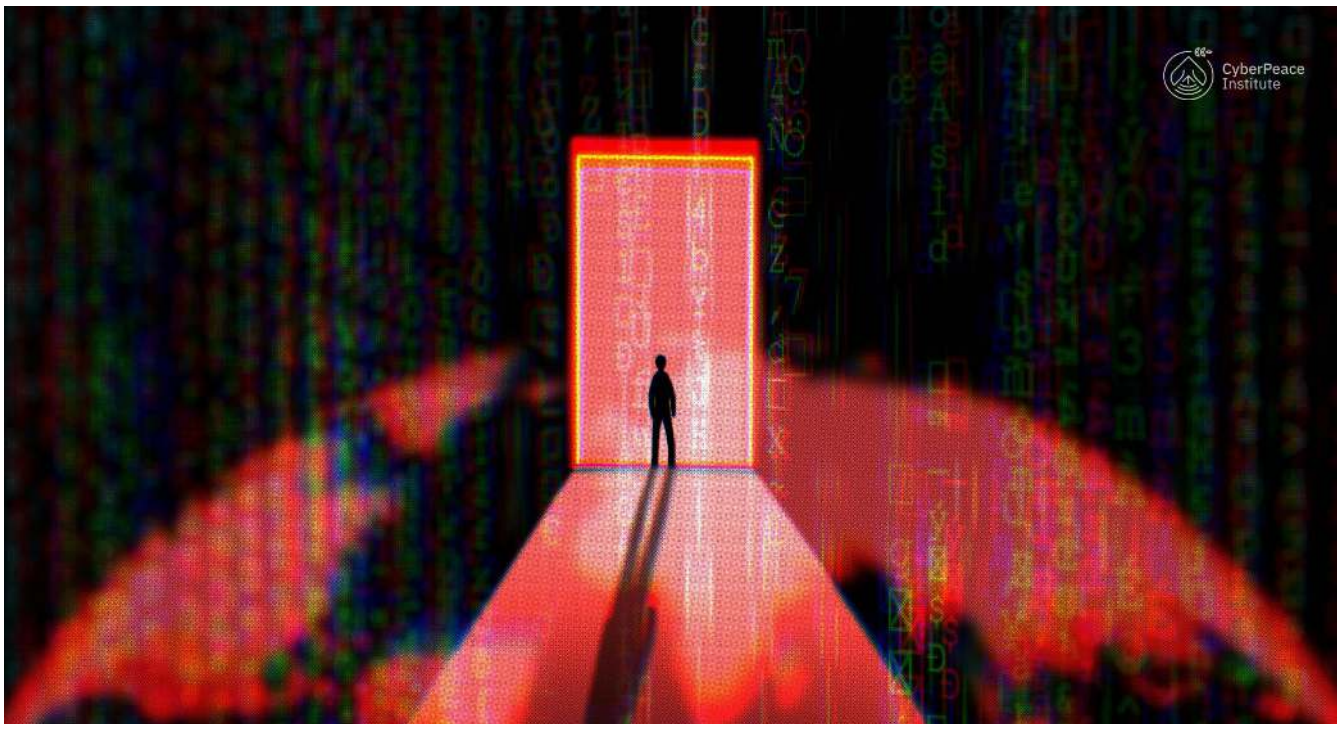


Figure 2.

These are mere examples of a growing and disheartening trend. Most NGOs have started their digital transformation in the last decade and are unable to invest sufficiently in cybersecurity. Only 1 in 10 NGOs train its staff on cybersecurity matters and only 1 in 5 monitor its networks. Yet, the entire non-profit industry raises on average, 1 trillion dollars annually. An expanding digital footprint, structural inability to invest in cybersecurity, as well as limited cooperation with law enforcement make NGOs a prime target for cybercriminals. State actors are also interested either in the data that NGOs gather, or in discrediting their work by disrupting their services. The asymmetry between the limitless resources of state actors and the limited resources of NGOs makes for an explosive mix.

"An expanding digital footprint, structural inability to invest in cybersecurity, as well as limited cooperation with law enforcement make NGOs a prime target for cybercriminals."

Figure 3. CyberPeace Builders.

Figure 4. CyberPeace Builders' logo.

At The CyberPeace Institute, we launched the CyberPeace Builders program in November 2019 as a haven for NGOs. Providing concrete assistance through a capacity building programme that connects humanitarian NGOs to cybersecurity volunteers through an innovative portal. We build on the lessons drawn from helping the most vulnerable, NGOs and those they protect, evaluating the information collected to provide concrete solutions to decision-makers. To date, the CyberPeace Builders have helped over 70 NGOs across 4 continents with overwhelmingly positive feedback as they gain access to free, trusted cybersecurity advisors from industry experts in a simple and fluid manner. Additionally, we have developed elaborate mechanisms to create a compelling value proposition for the volunteers and the companies they work for. By the end of 2022, our programme will have helped over 100 NGOs and by the end of 2025, over 1000.

NGOs are not just on the frontline of the most complex social challenges - they are on the very forefront of cyber warfare. If we do not help them, we must accept that the internet will become a space that tolerates and mobilizes extreme violence against the vulnerable. Past this, the Internet will no longer be a place for progress and connection but rather competition and threats. Helping NGOs continue their critical work is the single most important issue that industry and policy makers must address today.

GLOBAL CYBER POLICY DIALOGUES: ADVANCING REGIONAL MULTISTAKEHOLDER CYBER CAPACITY BUILDING COOPERATION

Written by: Anneleen Roggeman, Senior Program Manager, Observer Research Foundation America; Abagail Lawson, Associate Fellow & Program Manager, Observer Research Foundation America.

In 2020 the Observer Research Foundation America, in partnership with the Ministry of Foreign Affairs of the Netherlands, launched a series of regional dialogues to address key cyber challenges, strengthen multistakeholder networks and increase coordination among regional capacity building initiatives. These meetings are intended to complement ongoing international cyber processes at the United Nations and other forums on a normative framework for cyber stability by engaging groups of states and stakeholders that have not been as involved in international conversations on cyberspace governance. Over the course of the project, several themes have emerged that transcend regional boundaries and offer insights for global efforts on cyber capacity building to implement the international framework for cyber stability.

The *Global Cyber Policy Dialogues* is an ongoing project led by the Observer Research Foundation America (ORF America) in partnership with the Ministry of Foreign Affairs of the Netherlands.

The project convenes regional dialogues to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity building initiatives. The goals of the initiative are to:

- Increase understanding of the impact of international cyber policy on national and regional priorities, particularly in countries and regions which have not been as engaged in international cyber discussions.

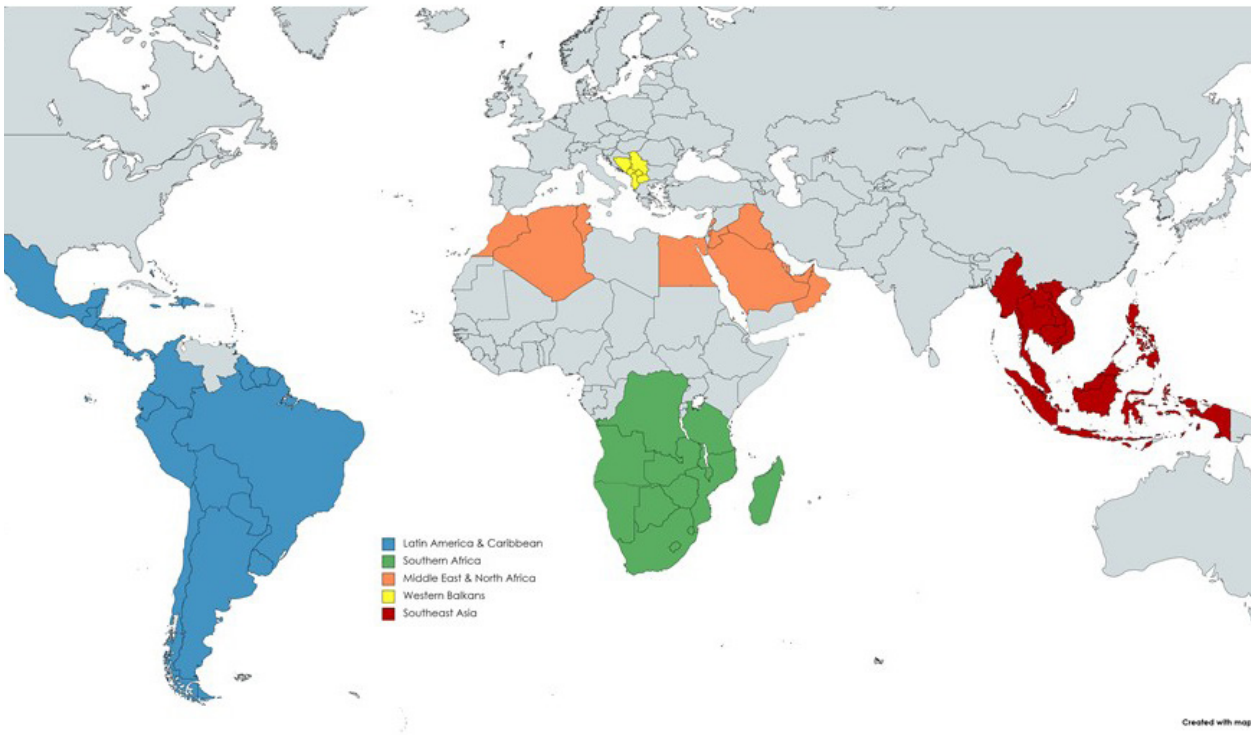


Figure 1. Map of participating regions and countries.

- Create intraregional networks on cyber issues and build trust among stakeholders and countries.
- Help shape the results of relevant United Nations processes and facilitate implementation of outcomes, including the work of the Open-ended Working Group, Group of Governmental Experts, potential Programme of Action, Ad Hoc Committee on Cyber Crime, and the Secretary-General's Roadmap for Digital Cooperation.
- Strengthen regional multistakeholder cyber cooperation and improve cyber capacity building to be more recipient-led and aware of other complementary ongoing efforts, including encouraging collaboration with the Global Forum on Cyber Expertise (GFCE) and its community as well as promoting the GFCE as a key cyber capacity building platform.
- Increase North-South engagement on cyber issues, by laying a foundation for long-term relationships between project partners and regional and national actors.

ORF America has convened six virtual preparatory meetings focused on five regions: Southeast Asia, Southern Africa (a second meeting was held in October 2021), Western Balkans, Latin America & Caribbean, and the Middle East & North Africa. Each meeting is co-hosted with the Ministry of Foreign Affairs of the Netherlands and a partner ministry from the respective region, as well as a local civil society organization, and brings together multistakeholder participants and speakers from government, civil society, academia, and the private sector. The virtual meetings have served to lay the groundwork for eventual in-person roundtables and develop and strengthen relationships among regional partners and constituents.

Figure 2. Overview of virtual meetings, topics and partners.

Figure 2 provides an overview of the meetings held so far, including topics and partners.

In the next phase, in-person dialogues will be held in the different regions. Meetings will be smaller and more focused in order to cultivate relationships, promote trust and work towards actionable outputs to advance regional multistakeholder cyber capacity building cooperation. The first dialogue took place in late Spring 2022 in the Western Balkans (Skopje, North Macedonia). Subsequent meetings will be held in Southern Africa (Pretoria, South Africa), Southeast Asia (Singapore), Latin America & the Caribbean (Santiago, Chile) and the Middle East & North Africa (Amman, Jordan).

Key Takeaways

Several themes have emerged from the discussions across the regions. These themes reflect challenges that all regions face in the context of cyber capacity building. Understanding and addressing each of these areas can help improve efforts to build capacity and implement the normative framework for cyber stability.

1. There is a need for increased awareness, knowledge and capacity on cyber policy issues at the political and diplomatic levels.

Cybersecurity and stability issues need to be mainstreamed as core policy issues throughout government. More engagement on these issues at senior political levels will enable leaders to have greater situational awareness of the needs and threats, prioritize cybersecurity and related matters, and ensure that adequate resources are allocated.

At the same time, it is necessary to enhance national capacities to participate in international cyber cooperation processes and strengthen the understanding of the international dimensions of cybersecurity issues. National policymakers, law enforcement officials and diplomats often do not have the bandwidth, resources or technical expertise to engage meaningfully on these topics. Greater national level capacities could lead to more widespread implementation of internationally-agreed norms, principles and frameworks.

2. Donors, implementers and recipients should enhance coordination and cooperation in cyber capacity building.

The number of cyber capcity building projects has increased in all regions in the last few years. However, in all regions, it was noted that a lack of coordination among capacity building efforts was a problem. Better coordination on these initiatives among donors, implementing partners and recipient organizations is required to avoid duplication of efforts, achieve useful outcomes aligned with recipient demand and build on capacities already in place.

"Better coordination [...] is required to avoid duplication of efforts, achieve useful outcomes aligned with recipient demand and build on capacities already in place."

3. Digital transformation is a driver of cyber priorities.

Digital transformation is a key enabler of socio-economic development globally, but rapid digitalization without adequate considerations can exacerbate existing inequalities, lead to increased cybersecurity risks and pose geopolitical, security and human rights challenges. Many countries are looking towards ICTs and the so-called Fourth Industrial Revolution to grow their economies, leapfrog their development, and transform their infrastructure. As such, much of the interest in using and securing ICTs grows out of these goals. Linking development conversation with cybersecurity and stability can result in mutually reinforcing outcomes in both areas. Digital transformation can be a useful entry point for discussing the linkages between cybersecurity and sustainable development, which can help foster approaches to inclusive digital transformation that advance cybersecurity, reduce inequality and safeguard human rights.

4. A multistakeholder approach means breaking down silos and connecting across sectors.

The regional discussions also revealed silos at the national level. There is often a lack of transparency, communication and coordination regarding cyber policy issues between different national agencies and stakeholders, both within governments, for example between Ministries of Foreign Affairs and Defense, and with the private sector, the technical community, and civil society. Cyber policy discussions need to engage the full spectrum of stakeholders (government, academia, civil society and industry), connect across sectors and facilitate increased awareness and cooperation among different communities.

At the international level, discussions at the United Nations about cyber crime (third committee) and international security (first committee) are siloed as well. Improving connections across these two processes could strengthen the outcomes of both as well as advance national approaches to cyber challenges related to both cyber crime and national security.

Similarly, intersections between the Sustainable Development Agenda and ICTs, peace and security have not been adequately explored in either the development or peace and security "silo." A more concerted effort to bridge this gap and cross reference the internationally-agreed norms and principles with development benchmarks could contribute to more informed international processes.

5. The role of the private sector is an important topic.

A common refrain in multilateral discussions about stability in cyberspace and cyber crime is that the private sector has an important role to play, however views about what that role looks like and how it relates to government and civil society differ greatly depending on the context. More meaningful conversations with the private sector, including small and medium-sized enterprises, could be useful in furthering implementation of the international framework for cyber stability and supporting inclusive digital transformation.

THE GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING (GC3B): MAKING 2023 THE YEAR OF CYBER RESILIENCE FOR DEVELOPMENT

Written by: CyberPeace Institute; Global Forum on Cyber Expertise (GFCE); World Bank; World Economic Forum.

Although digital transformation and connectivity have boomed in the past decade, digital development programs have not always been accompanied by adequate consideration of digital threats and corresponding investments in cybersecurity and cyber resilience. As such, many countries are now experiencing new risks, greater vulnerabilities, and a rise in malicious activities that are threatening the security of their digital services and critical infrastructure – all while eroding trust in the digital environment and institutions. In order to bridge the gap and move toward cyber resilient development, the inaugural Global Conference on Cyber Capacity Building (GC3B) will bring together decision-makers, practitioners, and experts to catalyze global action on mainstreaming cybersecurity, cyber resilience, and cyber capacity building (CCB) across the international development agenda as well as raising awareness of how cybersecurity and cyber resilience are key enablers of sustainable development, economic growth, and social prosperity.

Co-organized by the CyberPeace Institute, the Global Forum on Cyber Expertise (GFCE), the World Bank, and the World Economic Forum, the Global Conference on Cyber Capacity Building (GC3B) is gearing up to host its inaugural event in 2023.

The theme of the first-annual GC3B is "Cyber Resilience for Development."

The conference emerged from a recognition that cybersecurity, cyber resilience, and cyber capacity building (CCB) are critical enablers of digital transformation and social and economic development. Over the past decade alone, the number of Internet users has more than doubled from around 2.25 billion to over 5 billion people worldwide, largely driven by growth in developing countries – many of which are prioritizing digitalization and connectivity. By embracing and embedding information and communications technologies (ICTs) into their networked environments and infrastructure, countries around the world seek to improve productivity, foster economic growth, enable skills development, and much more.

The Importance of Cyber Resilient Development

While each country's development requirements may be unique, some common technological building blocks include, at minimum, a national digital identifier layer, a digital payments layer, and a data protection layer. Their application to vital services, like the healthcare sector, is critical to the success of countries' digital transformation.

Yet, digital development programs and robust digitalization in developing countries have not always been accompanied by adequate consideration of digital threats and corresponding investments in cybersecurity and cyber resilience. Coupled with the rapid proliferation of new threats and an ever-changing security landscape, many countries are now experiencing new risks, greater vulnerabilities, and a rise in malicious activities that are threatening the security of their digital services and critical infrastructure, all while eroding trust in the digital environment and institutions.

Cybersecurity and cyber resilience must therefore be mainstreamed into all development programs, modern infrastructure projects, and national digital transformation strategies. Not doing so can undo decades of progress related to countries' digital development due to the accumulating risks that are not always fully considered or mitigated, but also because of the debilitating impact that the lack of such resilience has on the ultimate beneficiaries of digital development: the people who use and rely on these systems.

To adequately support and safeguard their digital and economic development, countries must make cyber resilience a key priority. Realizing this goal demands multi-stakeholder engagement and cooperation, clear policy focus, and increased investment in managing cybersecurity risks, building cyber capacity, and ultimately ensuring public trust in digitally enabled systems. Doing so is paramount to realizing the digital transformation objectives of states and other actors across the globe as well as the United Nations' Agenda 2030, particularly since each of the 17 UN Sustainable Development Goals (SDGs) either include digital components or can be augmented and realized via digital technologies ranging from monitoring to implementation.

The field of international cyber capacity building has emerged over the last decade to share knowledge and assistance for strengthening national cyber resilience. This work is being advanced by a multi-stakeholder community, and there is great potential for deeper cooperation, collaboration, and connection between this field and the international development community, to the benefit of both. Realizing this potential and avoiding duplication of efforts, while also maximizing resources, will be a central aim of the conference.

Figure 1. Global Conference on Cyber Capacity Building (GC3B).

Aims, Objectives, and Expected Outcomes

Built upon four pillars – (1) Making International Development Cyber Resilient; (2) Collaborating to Secure the Digital Ecosystem; (3) Cyber Capacity Building for the Stability and Security of the Digital Environment, and (4) Operationalizing Solutions for Safeguarding Development from Digital Risks and Threats – the GC3B will bring together decision-makers, practitioners, and experts to catalyze global action on mainstreaming cybersecurity, cyber resilience, and cyber capacity building across the international development agenda as well as raise awareness of how cybersecurity and cyber resilience are key enablers of digital, social, and economic development and critical to achieving the SDGs.

The GC3B 2023 is anticipated to:

- Develop a demand-driven and international Global Cyber Capacity Building Agenda for cyber resilient development;
- Enhance CCB efforts by accelerating current multi-stakeholder cooperation and public-private partnerships;
- Mobilize global action, promote coordination mechanisms for CCB at the global and regional levels, and encourage funding of CCB;
- Advance good practices and tools for the protection of critical infrastructure; and
- Showcase examples from developing countries, particularly across the Global South, that have effectively incorporated cybersecurity and resilience into their development strategies and infrastructure projects and successfully coordinated external CCB funding and activities.

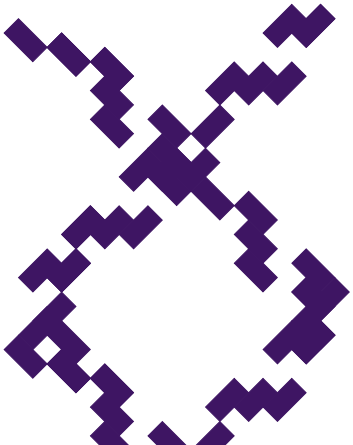
Elevating Global, Multi-stakeholder Perspectives

To showcase the urgent need for this conference, the GFCE and the Permanent Mission of Germany to the United Nations (UN) successfully co-hosted a side event luncheon on 27 July 2022 during the UN Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG). This side event highlighted the genesis and purpose of the GC3B, focusing on elevating middle- and low-income country and donor perspectives to emphasize why CCB should be seen as a fundamental element of digital development.

The event featured many speakers from across the development and governmental sectors. Constance Malomo, representing the Botswana Ministry of Communications, Knowledge and Technology, was the first speaker to take the floor, reflecting on why CCB is critical to Botswana's digital development. She emphasized that the Government of Botswana is prioritizing CCB so that their citizens understand that ICTs are not something to be feared but to be understood.

Kerry-Ann Barrett, the Organization of American States' (OAS) CyberSecurity Program Manager, highlighted the role of cyber resilience in development efforts across Latin America and the Caribbean. Specifically, she noted how it is not enough to merely transform governments and manifest online services. On the contrary, she underscored, it is also fundamental that governments ensure they are cyber resilient and have sufficient cyber capacity – including but not limited to human expertise and resources – to respond when attacks occur. Crucial to realizing this is coordination, which she affirmed is difficult to achieve both globally as well as regionally within Latin America and the Caribbean given the varied starting points and resources of different countries. Thus, managing to avoid duplication, collaborate, and share efforts is critical.

Joanna LaHaie from the United States Department of State reiterated the U.S. Government's support for CCB as it pertains to development and creating a more secure cyberspace. Specifically, LaHaie stressed the importance of ensuring that, while everyone should be able to benefit from technology, we must also recognize the need to defend from and respond to the threats those technologies foster.



Isaac Morales from the Ministry of Foreign Affairs of Mexico focused on the relationship between cybersecurity and resilience regarding Mexico's sustainable development efforts – and how they are intrinsically linked. Drawing from their experience, he echoed Barrett's remarks by emphasizing the high value and importance of building capacity internationally and regionally, while also including CCB and cyber resilience within the innovation agenda of countries at the national level.

Tupou'tuah Baravilala, representing the Ministry of Communications of Fiji, underscored why cybersecurity and digital development go hand-in-hand among small island developing states (SIDS), such as in Fiji, where they are also contending with other challenges and threats to their resilience and development, notably climate change and natural disasters. She also reiterated how the main goal of building cyber capacities is to close the digital divide and ensure a level playing field among all countries as much as possible.

Lastly, Laura Burr, representing the Department of Foreign Affairs and Trade of Australia, highlighted her government's commitment to and interest in making the conference a success, especially as it relates to involving more women around the world in cyber-related discourse, empowering them to be cyber resilient, and expand their cyber capabilities.

Figure 2. The GC3B side event at the UN OEWG, in Conference Room 8, UN Headquarters, 27 July 2022.

Bridging Communities and Catalyzing Global Action

In recognition of the importance of and building capacity for cyber resilient development, as highlighted by various members of the global multi-stakeholder community, GC3B 2023 will bring together decision-makers and experts to catalyze global action on mainstreaming CCB and cyber resilience across the international development agenda as a key enabler of sustainable development, economic growth, and social prosperity.

For more information or to get involved, please visit GC3B.org, follow us on Twitter, LinkedIn, or Facebook, or email Michael J. Oghia, GC3B Communications Coordinator, at: contact@gc3b.org.

LATIN AMERICAN AND CARIBBEAN YOUTH: CYBERSECURITY FORAY TO DELIVER THE PROFESSIONAL SHORTAGE

Written by: Jesús Salvador García Fuentes, Former Intern of the Cybersecurity Program, Inter-American Committee Against Terrorism of the Organization of the American States (OAS/CICTE)

Due to the growing international demand for cybersecurity professionals, Latin American and Caribbean nations have sought to increase cybersecurity education, training, and capacity-building opportunities by introducing new teaching approaches. Yet, the disparity in the maturity of cybersecurity education initiatives and opportunities in the hemisphere calls for collaboration between national policymakers private and civil sector organizations to foster cybersecurity capacity building among youth.

The growing dependence on digital ecosystems and the Internet has made it critical to develop cyber resilience. As cyber-attacks are inevitable in today's digital ecosystems, any cybersecurity initiative must seek to develop the necessary competencies to anticipate, deter, recover, and adapt from a changing and challenging cybersecurity threat landscape. Hence, a knowledgeable and proficient cybersecurity staff is required to achieve this in any sector.

Recruiting and retaining cybersecurity talent is one of the main challenges globally, particularly in Latin America and the Caribbean, especially given the limited training available to young people. Currently, positions are being filled instead and performed by Information and Communication Technology (ICT) experts. Still, at least 59% of them consider themselves incapable of responding adequately to a cybersecurity incident, according to the World Economic Forum (2022). This deficiency is estimated to cause an average annual loss of $4.87 million for threat containment[1].

It is estimated that there are approximately 4.19 million cybersecurity professionals worldwide. Additionally, the 33% annual demand increase for these professionals forecasted for 2030 results in the opening of an average of 16,300 job opportunities in the sector each year[2]. Nonetheless, the present low rate of cybersecurity graduates leads to an unfilled vacancy rate of 2.72 million, a gap that exceeds 701,000 vacancies in the Latin American and Caribbean region[3].

To cover this demand, increasing the training of young professionals and promoting the entry of more women in the field is required, primarily as females only represent 25% of cybersecurity professionals according to the report "A Resilient Cybersecurity Profession Charts the Path Forward" ([ISC][2], 2021).jects that work with small or medium sized enterprises (SMEs) or directly with vulnerable groups, including women and children, rural communities and the elderly or disabled.

Is the region ready to increase the number of cybersecurity professionals?

According to the "Cybersecurity Report: Risks, Progress and the Way Forward in Latin America and the Caribbean," developed by the OAS and the Inter-American Development Bank (OAS/IDB, 2020), the cybersecurity maturity required to increase the number of professionals in the field is linked to the existence of education, training, and capacity building initiatives. Therefore, the report assesses the Cybersecurity Education Maturity Level based on the following indicators:

CYBERSECURITY EDUCATION MATURITY INDICATORS

Awareness	Professional Development Framework	Training Framework
- Awareness Programs - Executive Awareness	- Provision - Administration	- Provision - Administration

MATURITY LEVEL

L-1	L-2	L-3	L-4	L-5
Initial	Formative	Consolidated	Strategic	Dynamic

Figure 1. Cybersecurity Education Maturity Indicators. Source: OAS/IDB (2020).

Figure 2. Cybersecurity Education Maturity Level. Source: OAS/IDB (2020).

The report states that the region presents an average level of formative maturity (L-2) in each of the indicators of the cybersecurity education dimension. Only six (6) of the thirty-two (32) nations evaluated (Brazil, Chile, Colombia, Dominican Republic, Mexico, and Uruguay) meet a consolidated maturity level (L-3) or are in an advanced transition to this level. These countries offer undergraduate, graduate, and diploma courses specialized in cybersecurity and foster the training/awareness of the general population in different educational stages. In contrast, three (3) nations: Antigua and Barbuda, Dominica, and Grenada, rank at an initial level of maturity (L-1) in cybersecurity education as they face challenges in developing a framework for training opportunities. Although these nations promote some of the fundamental safe practices in Internet usage, there are no opportunities for cybersecurity specialization and have limited ICT educational degrees. These examples, hence, exemplify the gap existing between the educational opportunities in the region.

A notable case study is Brazil, the nation with the highest rate of internet access in the region[4]. According to the "Cybersecurity Capacity Review of the Federative Republic of Brazil" study conducted by the OAS in 2020, Brazil has made

significant progress towards the enhancement of the available cybersecurity curricula. In the country, the Ministry of Education is mandated with the establishment of the the national cybersecurity curriculum, which includes requirements and standards, and commends its implementation to universities.

The implementation of this approach has been possible due to the simultaneous strengthening of regulatory frameworks. Through the "Civil Framework", a declaration of Internet usage rights in Brazil (the only one worldwide), protection in digital environments is established as a fundamental principle. Based on the premise that cybersecurity begins with the actions undertaken by the user, the Brazilian government has sought to empower the population to transcend digital threats through a wide range of cybersecurity degrees and learning opportunities.

Similarly, while 40% of countries maintained the maturity level of the 2016 assessment, the case of Guyana is also particularly noteworthy as it showed a 46.15% improvement by adding additional degrees and specialized certification courses.

Since the OAS/IDB first assessed the region regarding cybersecurity education, there has been an 11.02% increase in maturity levels, with the training framework being the main strengthened area.

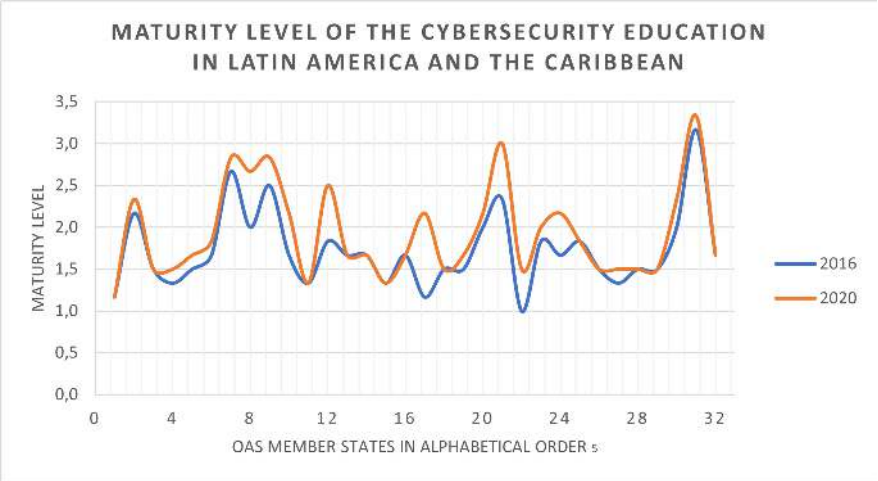


Figure 3. Maturity Level Evolution of the Cybersecurity Education. Source: OAS/IDB (2020).

Gamification Models: An alternative for cybersecurity education

Gamification is a helpful tool to introduce ICT and STEM (Science, Technology, Engineering, and Mathematics) students to cybersecurity practices. Through games and educational modules, it seeks to motivate students to solve problems related to breaches or cyber threats, introducing elements of competition that simultaneously inspire and challenge them.

Cybersecurity education does not have to come necessarily from national plans. It is essential to encourage the integration of educational platforms that allow students to practice their theoretical knowledge in real-life simulations. Institutions that have not yet developed a complete set of initiatives can with their national peers, just as is promoted in Brazil's strategy mentioned above, and appeal to private sector initiatives.

A feasible educational style when internships in specialized companies are scarce is through Capture the Flag (CFT) competitions, one of the most popular methods of gamified learning. CFT competitions involve attack simulations in which those who complete the most difficult tasks or in the shortest time obtain a score that makes them the winner.

For example, the OAS has implemented this practice through the CyberWomen Challenge, a competition organized with Trend Micro. Through this initiative, women of diverse ages and from the Latin America and Caribbean region participate in teams to solve a simulated cybersecurity challenge under controlled scenarios through collaboration, previous knowledge, and team-building exercises. This, in return, also creates further opportunities for women in the region to have a more indirect entry and approach to the cybersecurity industry.

The pathway to youth Cybersecurity Domain

Strengthening cybersecurity education from a technical and legislative approach will enable youth in Latin America and the Caribbean to integrate into the labor market as professionals fully trained to face the growing threats in digital ecosystems. However, there is still a disparity between countries in the region in terms of their educational opportunities, which affects the whole region's capacity to strengthen its cybersecurity capacities. To address this scenario, and as it was described by Pablo Ruiz Tagle-Vial, Dean of the Faculty of Law, and Daniel Alvarez Valenzuela, Professor of the University of Chile in the "Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean Cybersecurity Report: Risks, Progress and the Way Forward in Latin America and the Caribbean" report:

- Countries in the region reaching an initial stage of maturity in cybersecurity education should begin by including specialized cybersecurity content in undergraduate and graduate studies related to ICTs; progressively developing comprehensive cybersecurity curricula.

- Meanwhile, nations in a formative maturity or transition to the consolidated level, besides enhancing and expanding the specialized undergraduate and graduate cybersecurity studies, should promote cross-cutting cybersecurity training, including a gender approach to bridge the pronounced gaps in the sector. Some of the suggested core contents include risk management, technology governance, and cybercrime, areas requiring greater specialization in the cybersecurity sector.

- Finally, countries with a consolidated maturity level should ensure a multidisciplinary approach to prioritize cybersecurity education in ITCs and Social Sciences. In addition, encouraging the development of specialized research in these nations will contribute to progress on some of the current field challenges and the transfer of knowledge to the lower maturity level countries.

Last, but not least, gamification and other techniques should be incorporated in the list of initiatives, as it allows for children and young teenagers to approach cybersecurity from a diverse angle. To implement this, as well as the other initiatives, collaboration between national policymakers private and civil sector organizations must be fostered to build cybersecurity capacities among youth, which will ultimately result in greater capacities for the countries and the region.

"Strengthening cybersecurity education from a technical and legislative approach will enable youth in Latin America and the Caribbean to integrate into the labor market as professionals fully trained to face the growing threats in digital ecosystems."

Notes

1 IBM [2021]. Cost of a Data Breach Report

2 U.S. Bureau of Labor Statistics [2022]. Information Security Analysts

3 (ISC)2 [2021]. A Resilient Cybersecurity Profession Charts the Path Forward

4 According to the report "Internet usage in Brazil" [Statista, 2020], 75.68% of the Brazilian population, equivalent to nearly 160 million habitants, has access to the Internet.

5 OAS Member States in Alphabetical Order (Latin America and the Caribbean Region): Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panamá, Paraguay, Peru, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Saint Lucia, Suriname, Trinidad and Tobago, Uruguay, and Venezuela.

THE NEED FOR CAPACITY BUILDING AND THE CYBERSECURITY SITUATION IN CENTRAL AMERICA[1]

Written by: Abdías Zambrano, Public Policy Coordinator, IPANDETEC Central America.

The Central American region, one of the most unequal, violent and poorest in the world, is facing various challenges in its digitalization efforts, namely the consequences of a poor culture of cybersecurity, from various sectors, including decision makers and public policy makers.

The COVID-19 pandemic has significantly increased cyber-attacks, both on the general population and on public and private institutions.[2] In this sense, Central America is one of the most vulnerable regions with a sustained increase of attacks during the last years as a result of the lack of trained human resources to face the challenges that it implies, small budgets for cybersecurity, the lack of interest from legislators and the lack of knowledge of citizens about these issues.[3,4] Let us analyze the realities of cybersecurity in the region.

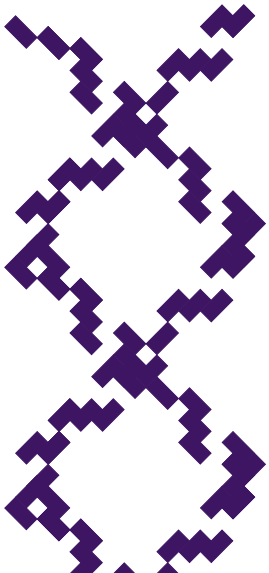


Figure 1. By 2020, only three countries in the region had a cyber attack response team.

Cybersecurity issues in the region

We could mention that one of the first problems is budgetary. In the region, cybersecurity expenditures are not so high, despite heavy investments in technological infrastructure in some countries[5]. This is due to the lack of governmental awareness of cybersecurity.

By 2020, only three countries in the region had a cyber attack response team. Some countries do not even have a catalog that identifies the country's critical infrastructure. Even worse than this, laws do not have the capacity to act efficiently against cybercrime, while at the same time the laws violate various human rights.

This is the case in El Salvador where there is no CSIRT,[6] while recently the Legislative Assembly passed a law that empowers the police to conduct covert online investigations, opening a wide and dangerous door to the persecution of opponents, human rights activists, among other groups that may be at risk.

While Panama, the Dominican Republic and Costa Rica,[7] are signatories to international treaties that oblige them to make changes to their legislation, they maintain a CSIRT that defends them from cyber attacks, and a cybersecurity strategy.

At the same time, the region is in the initial stages of legislating on data protection. Only Panama, Costa Rica and Nicaragua maintain a data protection law, Costa Rica's being very outdated for the needs that digitization demands, while Nicaragua does not maintain a data protection authority that exercises the protection stipulated by law.[8]

These types of particularities, which are seen throughout the region, are unknown to public policy makers, which is another important problem to be addressed. Parliaments do not often include technology-related discussions as a priority because their committees and working teams do not include professionals specialized in areas related to information and communication technologies.

"By 2020, only three countries in the region had a cyber attack response team. Some countries do not even have a catalog that identifies the country's critical infrastructure."

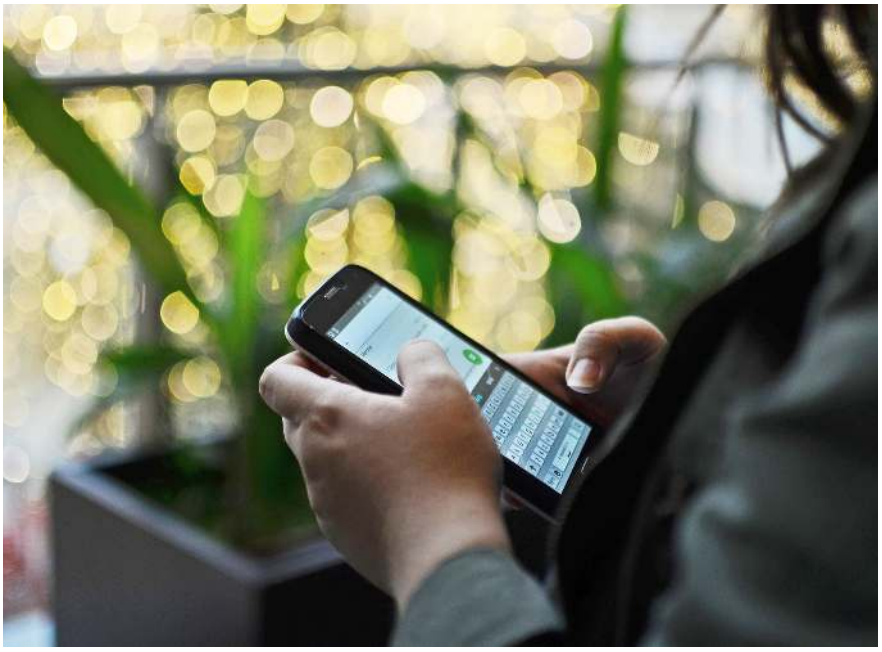


Figure 2. some countries are advancing ambitious bills that seek to create public policies on cybersecurity.

On the academic side, there are not many careers focused on cybersecurity and the vast majority of traditional careers do not include subjects that address this need, both on the technical and public policy side. This leaves the region ill-prepared for the challenges brought about by the COVID-19 pandemic and rapid digitalization in the labor market.[9]

Positive developments

However, not everything is bad in the region, some countries are advancing ambitious bills that seek to create public policies on cybersecurity. This is partly due to their membership of the Budapest Convention on Cybercrime, a document that ensures human rights standards for the benefit of the inhabitants of the signatory member. At the same time, the Council of Europe provides them with frequent training, contacts and materials to address their commitment.

Similarly, Central American states are advised by regional organizations such as the Organization of American States (OAS) or the Central American Integration System (SICA). In this regard, the OAS maintains an Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program, both of which provide support to States that require it when building capacities in their institutions, through training sessions for judges and members of judicial bodies, public policy makers, cyber-attack response teams, defense entities, among others.

From civil society, various organizations are advancing cybersecurity agendas. This is the case of IPANDETEC, where during 2019 and 2020, workshops were held to build capacities in cybersecurity and personal data protection in El Salvador, Honduras and Guatemala.[10] At the same time, the private sector is the one that invests the most in cybersecurity.[11]

The pandemic has provided an unique opportunity for the region to change and improve its security plans, with increased citizen awareness of digitization and the importance of cybersecurity. Let's see if they know how to take advantage of it.

"The pandemic has provided an unique opportunity for the region to change and improve its security plans, with increased citizen awareness of digitization and the importance of cybersecurity."

Notes

1 Central America geographically comprises Guatemala, Belize, Honduras, El Salvador, Nicaragua, Costa Rica and Panama. This article focuses on Spanish-speaking countries belonging to the Central American Integration System, which excludes Belize and includes the concept of the Dominican Republic.

2 https://www.forbes.com.mx/negocios-77-de-las-empresas-ve-mas-riesgos-de-ciberseguridad-en-2022/

3 https://www.laestrella.com.pa/cafe-estrella/tecnologia/210421/panama-presento-767-millones

4 https://www.eleconomista.net/tendencias/El-Salvador-con-58--de-ciberataques-a-empresas-20210503-0008.html

5 https://www.larepublica.net/noticia/mas-de-200-millones-de-intentos-de-ciberataques-afectaron-a-costa-rica-en-2020

6 CSIRT stands for Computer Security Incident Response Team. By definition, a CSIRT is a team of cybersecurity experts whose main task is to provide an organized response to computer security incidents.

7 https://www.ipandetec.org/wp-content/uploads/2020/04/CIBERSEGURIDAD_IP-ANDETEC.pdf

8 https://www.vozdeamerica.com/a/tecnologia-ciencia_reporte-oea-bid-ciberseguridad-america-latina-caribe/6066175.html

9 https://www.bbc.com/mundo/noticias-56247281

10 https://indela.fund/en/ipandetec-3/

11 https://eldinero.com.do/188593/empresas-deben-contemplar-la-inversion-en-ciberseguridad/

STRATEGIES FOR CYBER DIPLOMACY CAPACITY BUILDING

Written by: Dr Patryk Pawlak, Brussels Executive Officer, EU Institute for Security Studies; EU Cyber Diplomacy Initiative – EU Cyber Direct.

Strengthening global capacities to address the challenges in the field of cyber diplomacy has lately attracted attention of the cyber capacity building community. Even though the scope and size of such projects remains underreported, the number of institutions and organizations funding, implementing and receiving support for such projects is growing. But how can we ensure that this burgeoning field of cyber capacity building develops on sound methodological and conceptual foundations? This article discusses three possible strategies: blending, bridging and consolidating.

Capacity building *in* and *for* cyber diplomacy

The place of **capacity building in cyber diplomacy** has evolved over the past decade. The concept of cyber capacity building in the context of international security was first introduced in the report of the UN Group of Governmental Experts (GGE) in 2010 as a mechanism to ensure global ICT security, enhance the security of critical national information infrastructure, and bridge the divide in ICT security. Consequently, capacity building became a vital pillar of cyber diplomacy with concretely defined goals such as strengthening national legal frameworks, creating and strengthening incident response capabilities, training and awareness raising.

However, with the growing geopolitical tensions, the use of cyber capacity building as a mechanism for pursuing political interests – rather than pure developmental goals – has become increasingly apparent. The instrumentalization of cyber capacity building has followed. Capacity building was a cornerstone of the 2017 Russia-led resolution establishing the Open-ended Working Group (OEWG). An absentee in the international cyber capacity building community, Russia was not interested in strengthening the developmental dimension of the discussions in the First Committee but rather sought to broaden the support base for its agenda, in particular among countries in the Global South.

The growing complexity of the debates and policy processes concerning cyberspace as well as multiplication of venues in which these debates occurred – including within the United Nations system - have brought to the forefront the need to close the gap in the **capacities for conducting cyber diplomacy**. Regarding the latter, two streams of capacity building actions became particularly important: one stream aimed at building up the human and institutional capacities

Figure 1.

among the stakeholders to enable their engagement in cyber diplomacy (**capacity to engage**) and the other aimed at supporting the implementation of the commitments regarding the UN framework through adequate national and regional regulatory, institutional and human capacities (**capacity to implement**).

During the OEWG, it became clear that certain countries simply do not have capacities or sufficient resources to meaningfully engage in cyber diplomacy debates. This strengthened the risk that limited participation or even absence of certain countries and regions in these processes will lead to questioning the universality and legitimacy of their outcomes. As a result, the first wave of cyber diplomacy capacity building projects focused on **strengthening capacity to engage** in cyber diplomacy through building knowledge, raising awareness and facilitating participation in the UN meetings. Noteworthy examples of such initiatives include the Women in Cyber Fellowship funded by the governments of Australia, Canada, the United Kingdom and the United States and EU Support Fund created by the EU in 2019 to support participation of countries from the Global South in the OEWG sessions.

At the same time, delivering on the commitments made in the OEWG and GGE processes calls for enhanced efforts to address basic capacity needs (e.g. establishing a CERT in order to promote cooperation among CERTS) and to develop new capacities specific to the field of cyber diplomacy (e.g. strengthening the understanding of international law).

Consequently, the second wave of cyber diplomacy capacity building projects focuses on **capacities to implement** norms or confidence-building measures in order to assist governments in meeting their international commitments. As an example, in March 2022 the Australian Strategic Policy Institute produced a report entitled "The UN norms of responsible state behavior in cyberspace. Guidance on implementation for Member States of ASEAN". The GFCE's Working Group A on Policy and Strategy has also established a Task Force on CBMs, Norms Implementation and Cyber Diplomacy that in 2020 developed an introduction paper on CBMs as they relate to cyberspace and put together a living overview of the existing capacity building initiatives and trainings on the relevant topics (both available at the GFCE website).

Strategies for meaningful cyber diplomacy actions

Many cyber diplomacy capacity building efforts to date have taken form of ad hoc initiatives rather than properly designed actions undertaken as part of a broader engagement between the donors and partner countries. This raises legitimate concerns about the impact of such initiatives on funding in other priority areas closely connected to the Sustainable Development Goals such as closing the digital divide and traditional cybersecurity projects focused on building CERTs, developing strategies, or regulatory adaptation. In approaching cyber diplomacy capacity building, governments can choose among three possible strategies: blending, bridging or compounding.

"Many cyber diplomacy capacity building efforts to date have taken form of ad hoc initiatives rather than properly designed actions undertaken as part of a broader engagement between the donors and partner countries."

The blending strategy focuses on strengthening capacity to engage internationally and meet commitments by including cyber diplomacy objectives as an element in design and implementation of broader cyber capacity building actions. This means embedding cyber diplomacy within other pillars of cyber capacity building (Figure 2) at different levels (e.g. individual and organizational) and across all layers of capacity building (i.e. vision and policies, laws and regulation, institutions and resources, partnerships and cooperation). The biggest advantage of this approach is the focus on sustainability and ownership. For example, norms and principles concerning protection of the critical infrastructure articulated in the UN framework of responsible state behavior can be addressed in the development of national security strategies or incident management pillars. That way, they ideally become part of a larger whole-of-government and whole-of-society effort that ensures buy-in of a larger stakeholder community. In a similar vein, cyber capacity building efforts focused on developing laws and regulations can translate concrete commitments made at the international level into national legislation or regional instruments turning the voluntary commitments into legally enforceable provisions. Finally, initiatives aimed at strengthening individual capacities through trainings can expand their scope to include elements of cyber diplomacy.

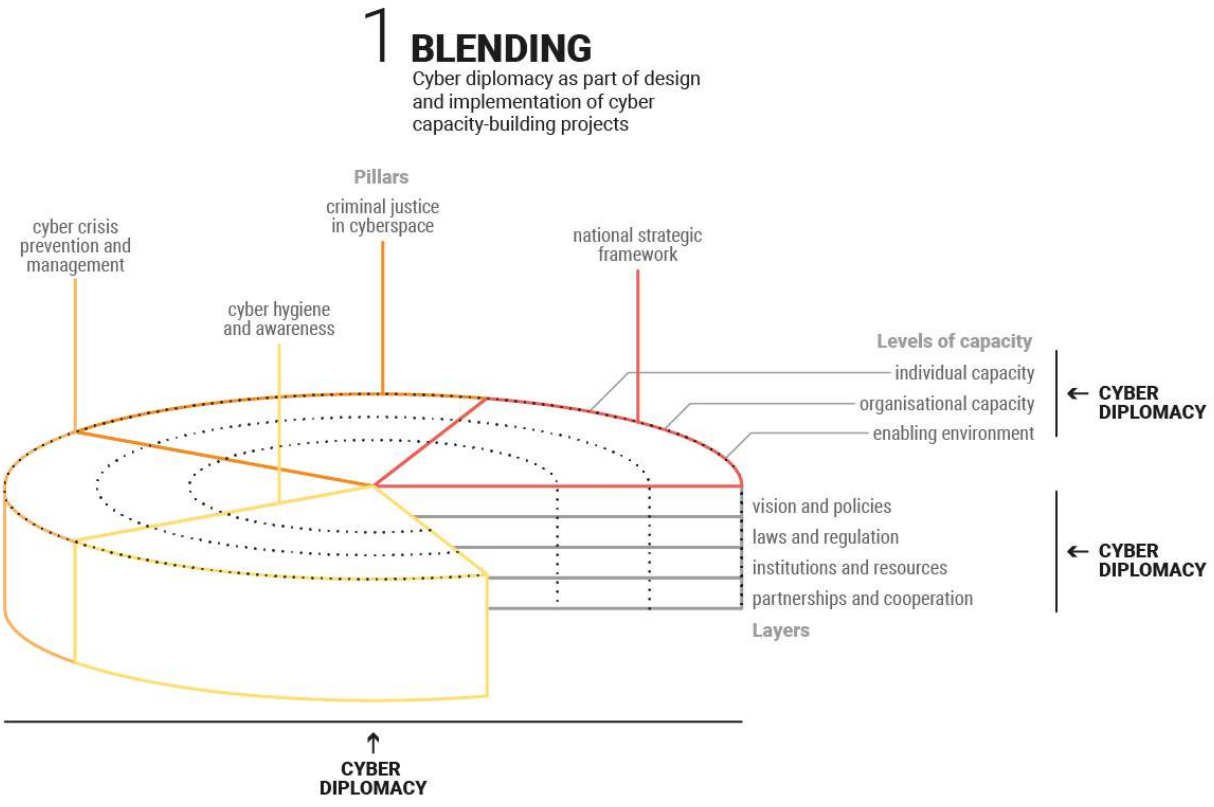


Figure 2. The Blending Strategy.

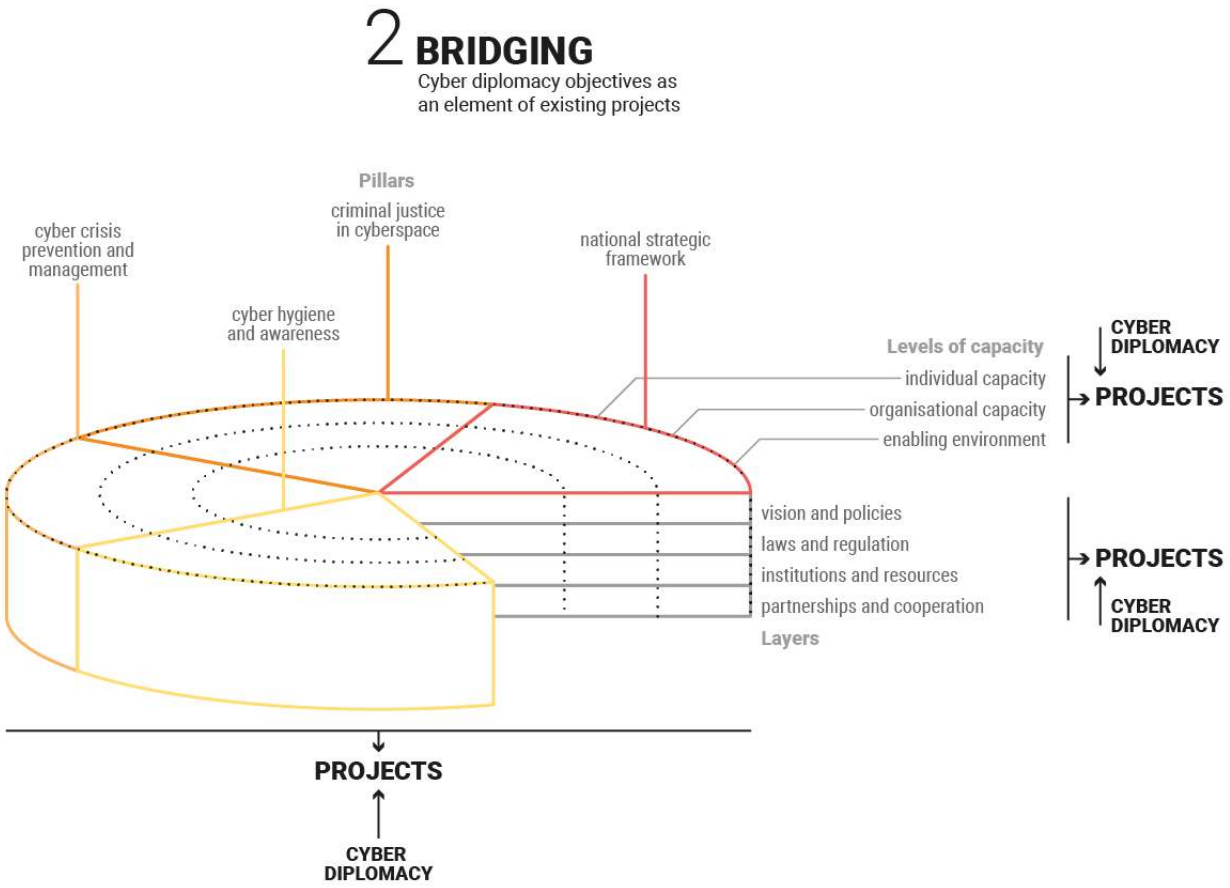


Figure 3. The Bridging Strategy.

The bridging strategy focuses primarily on strengthening capacity to engage internationally and meet commitments by including cyber diplomacy objectives as an element of the existing projects. This means embedding cyber diplomacy within projects with objectives linked to one or more specific pillars of cyber capacity building (i.e. national strategic framework, incident management, criminal justice, and cyber hygiene and awareness). This approach is different from blending in that cyber diplomacy is not included in the design of projects from the beginning but is incorporated at a later stage as an add on. For instance, projects focused on strengthening capacities to fight cybercrime or boost cyber resilience may incorporate certain aspects of cyber diplomacy in their activities with the aim to raise awareness, create a suitable external environment for cyber diplomacy projects, including by strengthening commitment to the application of the existing international law in cyberspace. In practice, this means that EU funded projects such as the GLACY+, Cyber4Dev, CyberSouth, CyberEast, iPROCEEDS2, or OCWAR-C could support cyber diplomacy objectives. While such approach may allow for quick gains and respond to urgent needs, it also has certain disadvantages when it comes to monitoring of the results or other risks linked to the delivery of the core objectives of the projects that are asked to integrate cyber diplomacy on board. This approach requires from donors, implementors and partner countries a clear recognition that such an approach does not guarantee lasting results but also raises questions with regards to transparency and accountability of the outcomes.

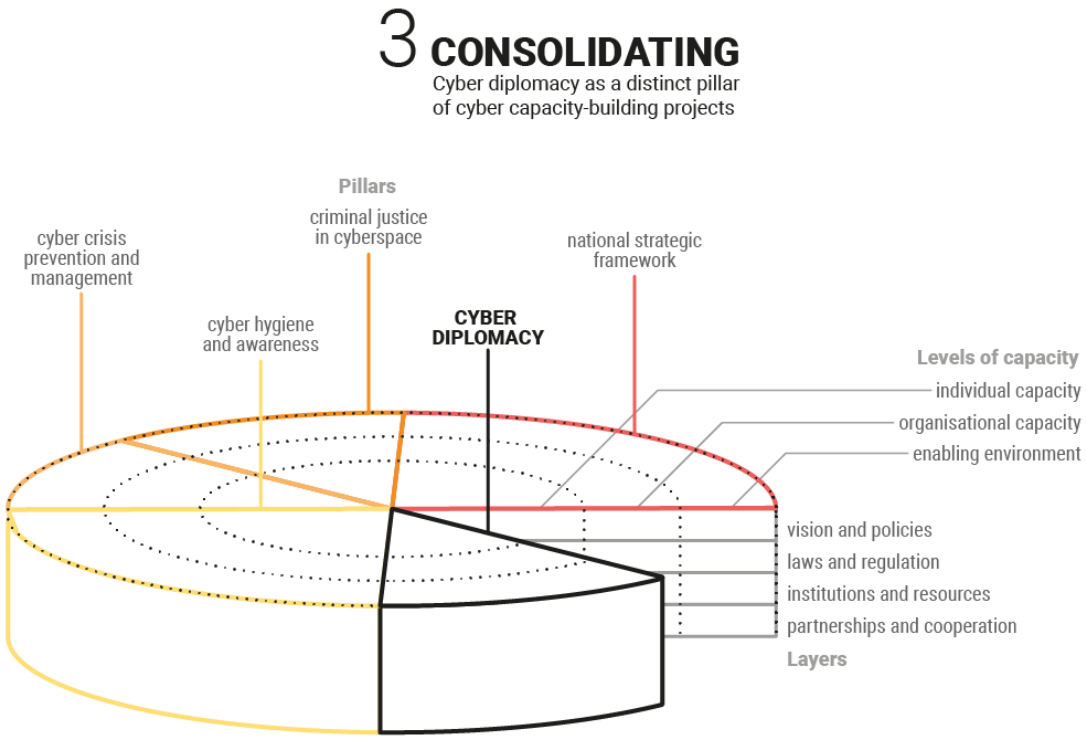


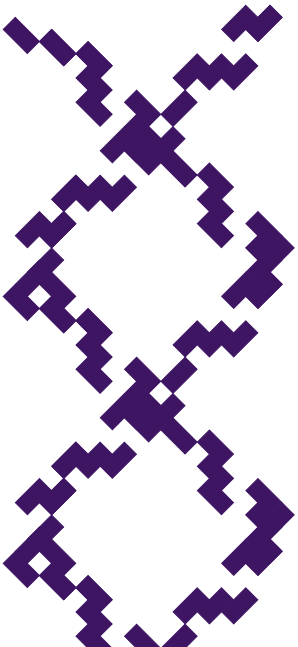
Figure 4. The Consolidating Strategy.

Finally, **the consolidating strategy** approaches cyber diplomacy as a distinct pillar of cyber capacity building (Figure 4) aimed at strengthening governments' capacities to engage and shape international cyber diplomacy policies as well as implement international commitments focused on the application of existing international law in cyberspace or implementation of norms and confidence-building measures. To date, such projects have been funded and coordinated primarily by the ministries of foreign affairs with expertise in cyber diplomacy. However, this also means that in the absence of engagement from the agencies specialized in development, some of the basic principles and methods developed over decades are not necessarily followed.

Cyber diplomacy in international partnerships

With the field of cyber diplomacy capacity building expected to grow in the coming years, it is critical that these projects are methodologically and conceptually sound. The blending and bridging approaches are particularly useful in cases where donors and partners acknowledge the urgency of engagement on cyber diplomacy and could be used as intermediary steps before actions focusing on cyber diplomacy are properly designed. However, to minimize any potential risks in design of such projects and increase the chances of a meaningful impact, cyber diplomacy capacity building through blending, bridging, and consolidating may be the best guarantee to ensure that good practices and principles of development cooperation (i.e. ownership, sustainability, inclusive partnerships, shared responsibility, transparency and accountability) are taken on board from the beginning. Independently on which approach is adopted, it is clear that a closer partnership between development agencies and ministries of foreign affairs is necessary to ensure both coherence between the projects and to minimize the risk of conflicting objectives.

"Cyber diplomacy capacity building through blending, bridging, and consolidating may be the best guarantee to ensure that good practices and principles of development cooperation (i.e. ownership, sustainability, inclusive partnerships, shared responsibility, transparency and accountability) are taken on board from the beginning."



THE DIGITAL ACCESS PROGRAMME – A HOLISTIC APPROACH TO BUILDING AND SUSTAINING CYBER CAPACITY

Written by: Jemima Hodkinson: Head of CSSF Cyber Programme, Cyber Policy Department, at the Foreign, Commonwealth and Development Office (UK).

Cyber threats are a global issue, with impacts that propagate across borders. Rapidly digitizing middle-income countries face a particular challenge to seize the benefits of digital development while mitigating cyber risks. The cyber harms perpetrated by criminals and other threat actors act as a brake on development and prosperity gains. They reduce trust in technology and the internet, particularly among the economically vulnerable. Afraid and unsure, the very people who most need the socio-economic benefit of being online risk missing out. The UK Government's innovative Digital Access Programme (DAP) currently supports five countries to address this challenge through a holistic approach combining digital development, cyber capacity-building and entrepreneurship.

Five countries, sixteen targeted projects

The Programme has three "pillars": Pillar 1 drives sustainable expansion of affordable connectivity, digital literacy, and locally-relevant content and services; Pillar 2 builds cyber security capacity to help ensure safety; and Pillar 3 stimulates local digital economies.

Through Pillar 2, since April 2021, the DAP has been supporting 16 capacity building projects to strengthen resilience to cyber threats affecting governments, businesses and citizens.

In each instance, the ambition is to build a sustainable capability that allows national partner governments to better protect their citizens online or to defend their critical national infrastructure.

Investing in national governments and their agencies allows the benefits to be multiplied at the grass roots level. Almost four-fifths of the programme's budget is therefore being spent directly with the five partner countries' governments.

The remainder supports projects that work with small or medium sized enterprises (SMEs) or directly with vulnerable groups, including women and children, rural communities and the elderly or disabled.

"DAP works with five countries – Brazil, Kenya, Nigeria, South Africa and Indonesia – and is the UK government's largest overseas cyber capacity building project to date."

Catalyzing impact

Clearly, building cyber security capacity takes time. But after a year of full delivery, the programme is already achieving initial results.

In Indonesia, the programme is protecting the availability, security and integrity of the country's telemedicine platforms. These are vitally important in a country where physical access to healthcare professionals can prove challenging.

In South Africa, specialist police officers are being provided with cybercrime and digital forensics training, thereby improving the prospects of successfully prosecuting cybercriminals.

In both Nigeria and South Africa, the programme is boosting the cyber resilience of the countries' SMEs – who contribute enormously to the national economy but who typically display worryingly low levels of cyber readiness. In both we are collaborating heavily with local NGOs, tech hubs and community groups to disseminate free cybersecurity tools, advice and support.

Meanwhile, in Brazil, the programme's toolkit is improving the way that schools teach the fundamental digital skills that children need to keep themselves safe in cyberspace.

Figure 1. UK cybersecurity toolkits for SMEs.

The Programme includes several other projects that aim to improve capabilities within government itself, in areas such as incident response, information security and threat identification.

Behind each project is an extensive monitoring, reporting, evaluation and learning framework. The Programme should ultimately help increase each country's score against the Capacity Maturity Model (CMM), which assesses a country's maturity across five dimensions, policy, culture, education, regulation and technologies.

"Behind each project is an extensive monitoring, reporting, evaluation and learning framework. The Programme should ultimately help increase each country's score against the Capacity Maturity Model (CMM), which assesses a country's maturity across five dimensions, policy, culture, education, regulation and technologies."

Figure 2. UK strengthening the cybercrime defences of Nigerian small businesses owners.

So as digital access continues to grow in these countries, resilience to cyber threats grows too, ensuring millions of new users can enjoy the benefits of a free, open, peaceful and secure cyberspace.

For further information, please see the 3 minute video describing this programme by following this link https://vimeo.com/user39994917/review/672807412/7470a710d0.

Note: In November, the UK will host a hybrid conference in London to discuss lessons from the past 2 years of programme delivery. Senior government cyber policy leads and other stakeholders from the five countries will be invited.

DEVELOPING AFRICAN STUDENTS' STRATEGIC THINKING ON CYBERSECURITY

Written by: Enrico Calandro, Project Leader, Cyber4Dev; Richard Harris, Principal Cybersecurity Policy Engineer, MITRE Corporation.

Building cybersecurity skills in Africa is a complex task which needs to be addressed at multiple levels. Besides building technical knowledge on how to tackle cyber-risks and threats from an information and network security perspective cyber security requires strategic and policy thinking on how to respond to reduce the risks and impacts of cyber-attacks against critical infrastructures that could undermine the political, economic, and financial stability of a territory if not addressed in a timely and coordinated way at a highest national policy level. Cognizant that very little has been done in Southern Africa to build strategic thinking on cybersecurity for the next generation of cyber policy leaders, the Cybersecurity Capacity Centre for Southern Africa (C3SA) has partnered with the Atlantic Council's Cyber Statecraft Initiative by adapting the Atlantic Council's "Cyber 9/12 Strategy Challenge" model to establish a South African Cyber Policy competition to help meet their mutual goals of developing the multidisciplinary cyber security skillsets needed in national workforces. The success of this competition, which can pave the way for future such competitions across the African continent, was made possible through the strong network of the Global Forum on Cyber Expertise (GFCE) and the commitment of the Atlantic Council and C3SA to build cyber security policy capacity across the globe.

The first edition of the competition in the African continent was held virtually on the 12-13 October 2021 and hosted at the University of Cape Town. Twelve teams of graduate and undergraduate students from Southern African Universities grappled with a challenging and far reaching simulated cyber-attack scenario while competing in the first ever cyber policy and strategy competition in Africa.

A second competition, involving students from the South African Development Community countries is scheduled for September 28-29, 2022.

Figure 1. Team South Africa.

What are Cyber Policy Competitions and Why are They Important?

In 2012, the Atlantic Council's Cyber Statecraft Initiative noted an increasing number of "capture the flag" competitions and similar cybersecurity hackathons for students in computer science and information technology. While these types of events represent an effort to build the cyber talent pipeline, they often exclude the social, political, and legal context of cyber crises. Furthermore, these events often have higher barriers to entry for students from a wide range of academic disciplines who might otherwise be interested in cybersecurity amid a global cyber talent shortage. In response, the Atlantic Council established the Cyber 9/12 Strategy Challenge—a cyber simulation—to teach students about the complexity of cyber crisis and conflict. Through this simulation, with the guidance of a mentor and feedback from coaches to develop the talent pipeline of technically literate policy professionals, students address issues such as national security, law, and business, thereby closing the cyber skills gap as well as gaps between technology and policy communities.

Ten years on, the Cyber 9/12 competition model has proven effective not only at training students who might not have considered a career in cybersecurity but also training students from technical disciplines on policy analysis and strategic communication. Ever since, this competition model has spread and there are now competitions across the United States, as well as in Europe, South Africa, and Australia. The program has connected with thousands of students over the years, setting them up for careers in government, industry, academia and much more.

"The Cyber 9/12 competition model has proven effective not only at training students who might not have considered a career in cybersecurity but also training students from technical disciplines on policy analysis and strategic communication."

What are Cyber Policy Competitions and Why are They Important?

In early 2021, C3SA was invited to have a team participate in the Washington, DC 2021 Cyber 9/12 Strategy Challenge which took place in March 2021. This was made possible by members of the GFCE Working Groups and Research Committee who shared their experiences in cyber capacity building and developed a vision for identifying effective and feasible ways to address the need for cyber security policy skills in Africa.

Intrigued by the opportunity of being mentored by international cybersecurity experts based in Washington, DC on how to develop a policy response to a major cyber-attack, C3SA set up a team, consisting of two PhD students specializing in cybersecurity, a master's student and a web developer from the University of Cape Town. This team participated in a virtual competition under the guidance of a Postdoc and senior researcher at C3SA. That was the first time a team from Africa participated in the Cyber 9/12 Competition series, which have been successfully run by the Atlantic Council since 2012.

During the March 2021 competition the C3SA team played the role of experienced and senior policy advisers by acting as a cybersecurity task force. The team prepared, developed, and briefed their policy solutions of a cyber scenario to a panel of judges who are experts in the field of cybersecurity, and who have played the roles of senior officials on the US National Security Council (NSC). The function of the NSC was "to advise and assist the President and to coordinate matters of national security among government agencies.".

The C3SA team and other 36 teams from the US, as well as Australia and Chile, were presented with a fictional scenario of a major cyber incident affecting the supply chain of various ports across the globe. This competition had three rounds of increasingly complicated and escalating events which the teams analyzed, developed policy options to address, and made recommended policy actions to senior government officials. After the first round, the C3SA team prepared a ten-minute oral presentation outlining their assessments and policy recommendations.

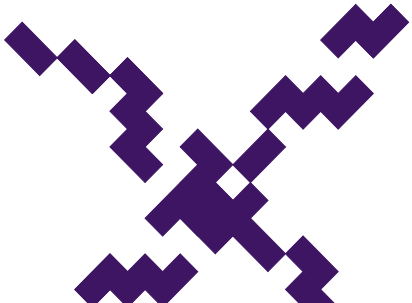
Piloting the South African Cyber Policy Competition

After the Washington, DC competition, joining forces with the Atlantic Council Cyber Statecraft Initiative, the C3SA team and a member of the Advisory Board of the GFCE began to plan for a competition in Southern Africa. As part of this planning, the C3SA team was invited to observe another Cyber 9/12 Competition conducted in Geneva. The experience gained during this competition was invaluable for planning the Southern African competition.

The Cyber 9/12 Strategy Challenge for South Africa was designed as a pilot program, modelled off the traditional Cyber 9/12 Competition format, but adapted to include two rounds held over the course of two afternoons on local time. In addition, during the first day of the competition, a lecturer from the Department of Information Systems at the University of Cape Town provided an overview on cybersecurity challenges from a Southern African perspective; and the second day of the competition began with a panel discussion during which senior cybersecurity advisors shared their own personal experience on how to become an expert in the field of cybersecurity policy.

Twelve teams comprised of 32 students in total participated in this virtual cyber security competition. Students prepared and briefed policy and strategy recommendations to senior government officials portrayed by 18 Judges composed of national and international senior and experienced professionals in the field of cybersecurity policy, law, and research. The teams were required to prepare and present possible solutions (in the form of policy briefs) to the cybersecurity incident simulation exercise developed by C3SA in collaboration with the Atlantic Council. After the presentations by the teams the judges engaged in Q&A, graded the policy briefings and presentations, and provided constructive feedback of the students' briefings and proposed policy recommendations.

The first three placed teams received prizes from ISACA South African Chapter, the Golden Sponsor of the First Edition of the South African Cyber 9/12 Strategy Challenge. ISACA, the international professional association focused on IT governance, also sponsors other prizes, including tickets to participate in their annual conference which will take place on 22 - 23 August 2022. The winning teams may also be considered for a scholarship to write an ISACA certificate exam - subject to requirements and evaluation by the AREC; and a free membership to ISACA for the Top Team.



What Lessons can be Learnt?

Having hosted a piloting cyber policy competition came with some challenges which turned out to be some of the main lessons learnt for the hosting team.

First, **holding a competition virtually had both cons and pros**. The virtual format of the competition expanded geographic involvement in the competition allowing both national and international experts to participate as judges to the competition, as well as students from different SADC countries to compete. Some of the challenges included that C3SA team had to become acquainted with the functionalities of Zoom (a virtual competition's core infrastructure), such as using parallel rooms and quickly switching between them. Also, South Africa was affected by loadshedding during the days of the competition, leaving the organizing team and local competitors to rely on the charged batteries of their laptops. Despite all these challenges, strong spirits of comradeship, partnership, adaptably, and resilience made it possible to overcome all these problems and successfully run the event.

Second, **the competition provided a platform for next-generation African talent to engage and exchange ideas on cybersecurity policy solutions**, developed in response to a cybersecurity incident simulation exercise. In addition to training students in the critical art and science of developing national cyber security policies and strategies in the face of cyber security challenges, the competition increased the awareness of academics and current policy makers who served as judges on how to creatively think about tackling cybersecurity from a strategic point of view.

Third, the South African Cyber Policy Competition **demonstrates the power of global cyber capacity building networks, especially the GFCE, in setting the conditions for extending capacity building opportunities** such as the Atlantic Council's 9/12 competition, to address cyber workforce development needs in Africa. While the story of building cyber security strategy and policy capacities through training and educating African students has just begun, the strong partnerships built between C3SA, the Atlantic Council, and the major sponsors of the Southern African competition, provide a solid foundation for the development of future strategy competitions across the African Continent.

Lastly, **the competition is a great networking opportunity for both competitors and judges**. Competitors had the opportunity to join the Cyber 9/12 Strategy Challenge LinkedIn group where the Atlantic Council's Cyber Statecraft Initiative provides updates on upcoming competitions, events, and job opportunities for Cyber 9/12 alumni. Judges had some opportunities to exchange views and opinions during the briefing sessions. Nevertheless, a hybrid approach which gives the opportunity to both attend in person and remotely will certainly improve the opportunities of meaningful networking.

"The South African Cyber Policy Competition demonstrates the power of global cyber capacity building networks, especially the GFCE, in setting the conditions for extending capacity building opportunities."

What's Next?

Building on the success of the Southern African Cyber 9/12 Strategy Challenge, C3SA will host an in-person competition on September 28-29th this year. Based on the feedback received, this year the Challenge will expand participation and provide students with pre-training, offered by Cyber4Dev, and tools to develop effective policy briefs. The in-person event is expected to improve the opportunities of feedback and networking between the judges (experts in the field) and the students. Finally, considering that many universities from different African countries expressed an interest to participate, C3SA is developing plans to possibly further extend the opportunity to compete to universities in other African regions, as well as encouraging other regional and academic institutions in Africa to sponsor their own competitions.

AFRICA CYBER CAPACITY BUILDING COORDINATION COMMITTEE

Written by: Moctar Yedaly, Africa Programme Director, GFCE; Velimir Radicevic, Senior Advisor, GFCE.

Made up of nearly thirty institutions from the African Regional Economic Communities, the private sector and civil society, and chaired/co-chaired by the African Union Development Agency and New Partnership for Africa's Development (AUDA-NEPAD) and the African Union Commission, the Cybersecurity Capacity Building Coordination Committee seeks to provide oversight and feedback on key CCB projects, while also ensuring a great coordination and effective use of resources across the continent. In March 2022, the Committee met to discuss its most ambitious deliverables to date, aiming to agree on a CCB Agenda for Africa and the work plan for the establishment of a GFCE Africa Hub, both to be presented at the Global Cyber Capacity Building Conference (GC3B) in 2023.

The African Union (AU) and the GFCE are continuing to pursue greater coordination of efforts of African Union members states aimed at increasing their overall cyber resilience, preparedness, and capacities.

Under the auspices of the AU-GFCE Cyber Capacity Building Project, funded by the Bill and Melinda Gates Foundation, two capacity building tracks are observed – one with national policy and technical representatives in the Africa Cyber Experts (ACE) community, and the second through a gathering of regional economic communities (RECs), the private-sector and civil society institutions in the CCB Coordination Committee.

Figure 1. CCB Coordination Committee, meeting in margins of the ACE Kick-Off meeting in Accra, Ghana.

Since the first meeting of the CCB Coordination Committee in September 2021, the need to coordinating cyber capacity building efforts in Africa has only increased, as is the need to create a multi-stakeholder response to evolving challenges targeting Africa's economy and increasingly digital societies.

Accordingly, during the March 2022 meeting in Accra, Ghana, Mr. Moctar Yedaly, the Director for Africa Program at the GFCE, suggested that the Terms of Reference and working modalities of the Committee must evolve to reflect all current and future projects of its membership.

Mr. Yedaly stressed the importance of the Committee's evolving mission:

> "There is a need not only to coordinate CCB programs in the continent but also coordinating among donors and technical institutions."

Figure 2. CCB Coordination Committee, meeting in margins of the ACE Kick-Off meeting in Accra, Ghana.

Moreover, in recognition of the capacities, experience and networks already possessed by the Committee members, the meeting petitioned the present RECs and Specialized Institution to help promote the Committee's work, proposed the creation of work plans, and the establishment of a working group or task force that can proactively address CCB needs identified through the AU-GFCE project, or by the members themselves.

The Committee counts as its members almost thirty institutions across Africa, with an emphasis on geographic representation, but also inclusivity and an active promotion of gender equality.

The meeting itself was attended by AUDA-NEPAD, AfricaCERT, Registry Africa, AFRINIC, IGAD, AFRIPOL, EAC, SMART AFRICA, WATRA, AUCSEG, ECOWAS, UNECA, ARTAC and NAWC.

Established through the AU-GFCE project, managed by Dr. Martin Koyabe, the Committee benefits from its connections to existing GFCE tools, including the Clearing House mechanism, where the Forum staff help match African members and partners with concrete CCB needs to implementers and donors that have the necessary expertise and resources. At the Global Conference on Cyber Capacity Building (G3CB) in 2023, two new developments will rely heavily on inputs by the CCB Coordination Committee and benefit its work further:

- The establishment of the GFCE Africa hub, with the mission to enhance coordination of efforts and demand-driven support for AU member state stakeholders, with an eventual presence in all five regions. The hub is also to develop and deliver capacity-building locally and serve as the liaison between the GFCE and the international community; and
- The adoption of Africa CCB Agenda, a multi-year strategic document that will identify principal needs, seek to mobilize resources, support facilitation of activities aimed at developing cyber capacities and reduce the risk of duplication or non-strategic investments.

Figure 3. CCB Coordination Committee, meeting in margins of the ACE Kick-Off meeting in Accra, Ghana.

Speaking on the importance of having a permanent, regionally-representative, but locally owned resource and support center in Africa, Mr. Yedaly said:

> "The GFCE Africa Hub will undoubtably enhance cooperation among partners of Africa."

The meeting ended with the present CCB Coordination Committee members agreeing to give feedback to the draft Agenda, which will be drafted by a four-person team, led by Mr. Yedaly, and circulated to Committee members in early April, as well as to the proposed GFCE Africa Hub, while sharing information on opportunities for collaboration with the AU-GFCE project and addressing CCB challenges and needs identified by the project through a Working Group or Task Force. The Committee will convene again in 2022 in the margins of the ACE Community Sustainment Meeting in Brazzaville, the Republic of the Congo, on 27 - 29 September.

CYBER STORIES FROM THE PACIFIC: CAPACITY BUILDING IN A REGION MARRED BY CHALLENGING TERRAIN

Written by: Cherie Lagakali, Senior Adviser, GFCE Pacific Hub; Bart Hogeveen, Head of Cyber Capacity Building, Australian Strategic Policy Institute; and Saia Vaipuna, inaugural Director, GFCE Pacific Hub.

The real test of successful capacity building is when people, systems and institutions withstand crises and incidents. As the GFCE Pacific Hub has started operations, it is valuable to now reflect on some cyber incidents that affected the Pacific in the past year. These insights should inform the role of the GFCE in supporting the Pacific cyber community in preventing, responding to, and recovering from a wide variety of security incidents that affect the use of the secure and reliable internet by people and businesses.

The Pacific is no easy terrain. The Pacific is characterised by its remoteness from mainland Australia and New Zealand, and Southeast Asia with many small island economies scattered across an area the size of half the Asian continent. Yet, the region is bustling with innovative entrepreneurs and people are embracing the digital future at a rate much faster than some Pacific island governments can regulate or understand.

The past year, however, has also marked the vulnerability of the Pacific's digital and cybersecurity environment. In October 2021, the government of PNG was affected by a ransomware incident; and in January 2022 a volcanic eruption caused a weeks-long communications blackout in Tonga. After being on the market for a while, Australia's Telstra took over the operations of Digicel Pacific in July. Digicel is the leading mobile telecommunications and network services provider in the region. The islands of Kiribati and Tokelau saw the landing of their first submarine fibre-optic internet cable.

With the GFCE's Pacific hub for regional cyber capacity building ready to start its operations, it is useful to see what these events and subsequent responses teach us about the value-add the Hub is expected to bring.

Together with Australia and New Zealand, Papua New Guinea is one of three Pacific members of the GFCE. Where the PNG government has embraced this partnership with the global multistakeholder community to seek assistance with its indigenous digital transformation drive, other Pacific nations are traversing on their journey of digital transformation and connectivity through bi- and mini- lateral partnerships with donors.

Having joined the GFCE in 2021, the PNG Department of Information and Communication received technical assistance from the GFCE community for the development of the national cybersecurity policy. The policy is part of a broader effort to develop and strengthen PNG's digital government. A Government Digital Transformation Bill has been tabled which will formalise an updated cybersecurity infrastructure and a whole-of-government approach to coordinating the use of ICT services across all public bodies. It also includes standards and regulations for government websites, social media, and general online government services.

With the Bill, the government also introduces a centralised e-government platform where citizens can access a single website to access all necessary government services online, such as obtaining a driving licence, filing tax returns, registering a business, enlisting for school and applying for public service jobs. The draft Digital Government Plan 2023-27 is currently open for public comments.

In spite of its best efforts, the government's central financial management system fell victim to ransomware in October 2021. In response, officials lamented the lack of central coordination even when plenty of cyber incident response capabilities were available. Since 2018, the Australian government has been aiding with the establishment of a national CERT, a Cybersecurity Operations Centre and a National Cybersecurity Centre that is providing shared ICT services.

> "In the Pacific, cyber issues are strongly connected to the broader development agenda and in particular to strengthening public service delivery."

In the global cyber debate, people often concentrate on issues involving the confidentiality, integrity and availability of networks and data, and national (cyber) security strategies. In the Pacific, however, cyber issues are strongly connected to the broader development agenda and in particular to strengthening public service delivery. In fact, cybersecurity and investments in ICTs are increasingly embedded in programs of international development assistance. This was a point successfully raised by the Pacific delegates from Fiji, Vanuatu and Tonga during the recent meeting of the UN open-ended working group on ICT security.

In the Pacific, ICT security also plays a role in efforts to adapt to climatic change. During a cyber capacity building event on national e-government plans in 2019, organised by GFCE partners Australian Strategic Policy Institute and e-Governance Academy, the Tongan delegation drew their colleagues' attention to the cybersecurity need of being able to move the national data centre to higher ground in situations of floods and cyclones. At the time, it was located in a transportable sea container.

The criticality of dealing with the impact of climate change for the future wellbeing of Pacific nations is infusing the regional cybersecurity and digital agenda. At the Glasgow summit of the UN climate change convention, Tuvalu's Minister for Justice, Communication & Foreign Affairs Hon. Simon Kofe made international headlines when he delivered his speech standing knee-deep in seawater.

Figure 1. Tuvalu's Minister for Justice, Communication & Foreign Affairs in his video address to the Glasgow Summit of the UN climate change convention, November 2021 (image source: Reuters on Twitter).

Through the Future Now project, the Tuvalu government is exploring means "to preserve and digitise historical documents; records of cultural practices; and other important texts, images, or multimedia." Tuvalu would be the first country to utilise the opportunities of connectivity and digital tools in an effort to mitigate the consequences of climate change and strengthen national resilience.

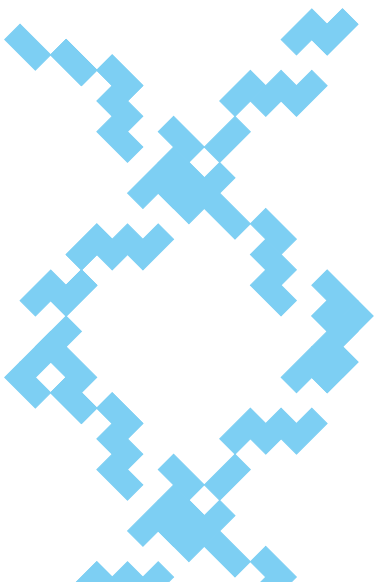
"Tuvalu would be the first country to utilise the opportunities of connectivity and digital tools in an effort to mitigate the consequences of climate change and strengthen national resilience."

Tuvalu is also an example of how small island nations can capitalise on their national treasures. As the owner of the .tv domain, the government has been able to secure a steady and sizable revenue from leasing the domain to an international registry. A new multi-year contract was sealed with GoDaddy this year, expected to amount to more than 7% of the country's annual GDP.

At the start of this year, the region was shaken up by a natural disaster. After the many cyclones that affected Pacific nations in 2021, bringing down telecommunications, the Hunga Tonga–Hunga Ha'apai volcano erupted on 22 January. With the epicentre at 65 kms from the coast of Tonga's main island, the subsequent landslide or turbidity current severed and displaced Tonga's domestic and international fibre-optic submarine cables.

The instant internet blackout forced government and public service utilities to revert back to the use of radio with no power and no phone services available. People and businesses weren't able to access bank accounts or contact family across the islands and overseas.

While international assistance mobilised quickly - the island was covered with volcanic ashes and potable water contaminated - the humanitarian deliveries unfortunately also brought Covid to the Island. It forced the authorities to impose stay-at-home orders which then created a surge in demand for online access to health advice and education.[1]



As the authorities were anticipating a months-long blackout, the regional telecommunications and cyber community rallied together. Regional telco Digicel managed to activate a satellite link with help from fellow operators Telstra and Spark and satellite operators SES and NovelSat. Prompted by a Tweet from a New Zealand Member of Parliament, Elon Musk decided to send 50 ground station terminals for his Starlink Low-Orbit Satellite network to Fiji and Tonga and offer Tongans free use as long as the submarine cable was under repair.

And thanks to operational partnerships with regional internet registry APNIC and through the Pacific Cybersecurity Operators Network (PacSON), CERT Tonga was able to seek technical assistance and receive basic hardware deliveries.

Across the Pacific, there are still a few countries that are only serviced by satellite broadband connectivity (for instance, Nauru and Tuvalu). Many more nations rely only on a single fibre-optic cable (Kiribati, Palau, New Caledonia, Marshall Islands, Solomon Islands, Tokelau, Tonga, Vanuatu and French Polynesia). By contrast, New Zealand has 5 international cable connections, Australia 12 and Singapore 23.

A single connection in remote and volcanic terrain is an evident security risk and hence international partners continue to invest in strengthening the region's cable infrastructure. The US, Japan and Australia in cooperation with the World Bank and Asian Development Bank have committed to a cable connecting Nauru, Federated States of Micronesia and Kiribati and a second redundancy cable for Palau.

The GFCE Pacific Hub is not a crisis response instrument, but it is worth considering what a regional hub for cyber capacity building would be able to provide and tangibly offer affected countries and communities. It is during times of duress that partnerships are tested and credibility validated.

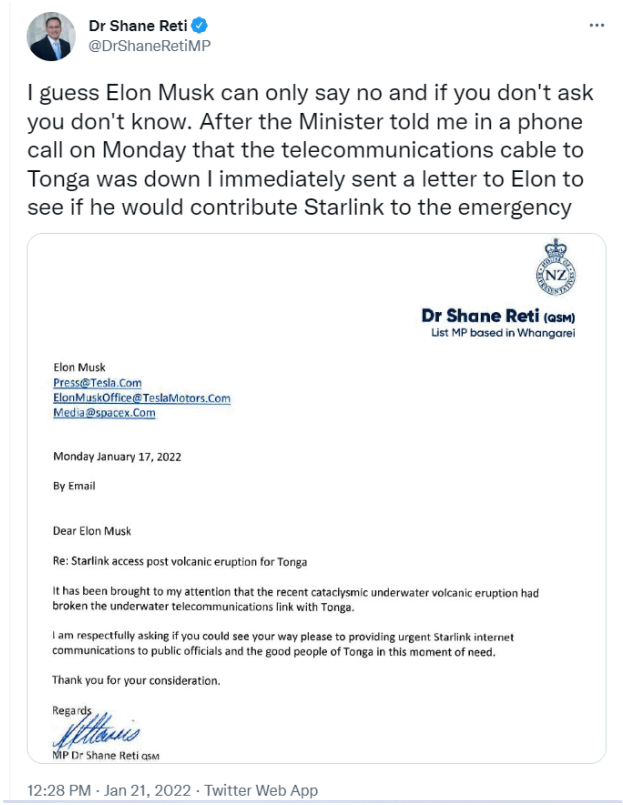


Figure 2. Tweet by Dr Shane Reti, New Zealand MP, asking Elon Musk to provide Startlink internet communications to Tonga. Source: @DrShaneReti, on Twitter.

Here are some thoughts on what this could mean for the Pacific hub's operations. First of all, the GFCE Pacific team should be in a position to connect people, help coordinate assistance and - in extremis - streamline offers of international support and seek to fill any capacity shortfalls. Access to the GFCE's global network of members and partners is of course a key asset.

A key deliverable of the Pacific Hub is to build a facts-based understanding of the regional cyber and capacity building environment without falling in the trap of re-questioning and re-surveying local stakeholders. In remaining authentic to its mantra of 'for the Pacific, by the Pacific and in the Pacific', the Hub will have to rely on the team's deep local knowledge, connections and culture of work. When needed, the future Hub should be in a position to assist affected countries in triaging issues, identifying risks and mobilising resources.

Finally, one of the most important values the regional hub should bring to the Pacific cyber community is a platform for networking, trusted connections and the creation of informal communities of practice, in-country and across the region. Making sure local cyber communities have the skills, confidence and experience to manage their affairs is what cyber resilience in the Pacific will mean, and that includes operational partnerships with peers in places like New Zealand, Australia and Southeast Asia.

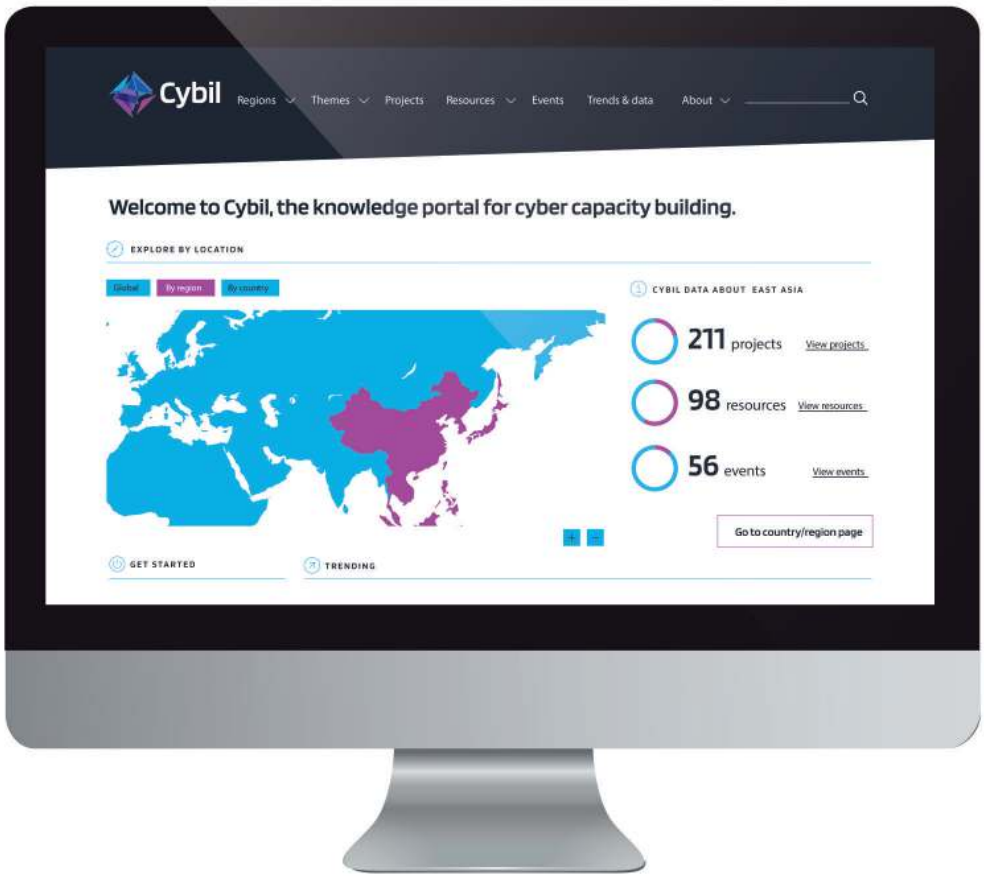
In that context, CERT Tonga and New Zealand recently announced a Cybersecurity Workforce Development Program to help build practical skills and understanding of cybersecurity issues among experienced and aspiring practitioners.

Now that the GFCE Pacific Hub's operations have kicked off, it's important to consider the role of the GFCE and cyber capacity building generally in preventing, responding to, and recovering from a wide variety of security incidents that affect the use of the secure and reliable internet by people and businesses.

Irrespective of the GFCE Pacific Hub's future activities, it shall be focused on delivering practical advice, expertise and assistance, deeply embedded in local cyber communities of practices, and grounded in evidence and facts on the ground.

Cybil 2.0 is here.

The global knowledge hub on cyber capacity building



More interactivity

Discover projects and resources through maps and filters

New resources

Tools, publications and now recordings of webinars

Events calendar

A calendar of past and upcoming cyber capacity building events

www.cybilportal.org

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

Volume 11, September 2022
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 12 submission deadline:
November 2022