Volume 6, October 2019

Global Cyber Expertise Magazine

What's in a project name? Cyber4Dev
A project by the EU
-page 4-

The current process of OAS confidence-building measures in cyberspace
-page 17-

GFCE: Strengthening the cyber capacity building ecosystem
Prioritizing implementation
-page 34-

CYBERSECURITY A FLAGSHIP PROJECT OF THE AFRICAN UNION AGENDA 2063

Africa's digital transformation
-page 24-

AFRICAN UNION

GFCE
Global Forum on Cyber Expertise

OAS More rights for more people

Volume 6, October 2019

Global Cyber Expertise Magazine

Editorial

Regions

Europe

4 What's in a project name? - Cyber Resilience for Development (Cyber4Dev)

8 Cyber Security – a joint responsibility calls for extensive cooperation

Asia & Pacific

11 Combatting Cybercrime: Enhancing Collaboration to Build Capacity in the Asia Pacific Region

13 Indian Initiative of Capacity Building for Senior Government Officials

America

17 The current process of OAS confidence-building measures in cyberspace

21 The OAS and CISCO launch "Cybersecurity Innovation Councils"

Africa

24 Cybersecurity a Flagship project of the African Union Agenda 2063

27 An interview with Dr. Amani Abou-Zeid on cybersecurity and the AUC's priorities

Global developments

30 UN Office for Disarmament Affairs and Singapore Cyber Security Agency launch online training course "Cyberdiplomacy"

34 GFCE: Strengthening the cyber capacity building ecosystem

Editorial

On behalf of the Editorial Board, welcome to the sixth edition of the Global Cyber Expertise Magazine! We are proud to present this edition at the Global Forum on Cyber Expertise Annual Meeting 2019 in Addis Ababa.

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

In this edition, we see practical cyber capacity building (CCB) activities carried out in all regions especially with a focus on international cooperation. This reflects an improvement in the coordination of CCB resources, knowledge-sharing and expertise around the world. Our cover story on Africa discusses the African Union Commission's role in ensuring member states are equipped to face cybersecurity challenges posed by the digital transformation of the region. An interview with Dr. Amani Abou-Zeid, African Union Commissioner for Infrastructure and Energy, similarly gives insight to the priorities of the AUC and promoting cybersecurity.

From Europe, Norway shares their lessons learnt in drafting and implementing a cybersecurity strategy after publishing their fourth strategy this year (hint: it involves international cooperation and building on best practices). International cooperation is highlighted again in an article on European Union's Cyber Resilience for Development (Cyber4Dev) project which promotes a multi-layered approach to security and provides assistance to partners in developing countries.

From Asia & Pacific, we have an article on cybercrime capacity building and training with the formation of an Asia-Pacific "hub", a collaboration between the Korea Supreme Prosecutors' Office (KSPO), World Bank and the GFCE. Also, read more about India's new training program, the "Cyber Surakshit Bharat", for senior government officials to address and mitigate cybersecurity challenges and create awareness.

From the Americas, a key takeaway from both articles is that cybersecurity challenges requires collaboration, public and private. In one article, the Organization of American States (OAS) and CISCO describe the launch of their Cybersecurity Innovation Council and how this will enhance cybersecurity in the Americas. In a second article, the OAS delves into their confidence-building measures in cyberspace and the importance of cyber diplomacy.

From Global developments, the UNODA shares their new online training course on cyber diplomacy that was developed in partnership with Singapore's Cyber Security Agency. In another article, the GFCE Secretariat reflects on the GFCE's progress since its launch in 2015 and how we may continue to accelerate forward.

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

On behalf of the Editorial Board,

David van Duren
Head of the Global Forum on Cyber Expertise Secretariat

What's in a project name? - Cyber Resilience for Development (Cyber4Dev)

The increased reliance on digital solutions for greater progress in economic and social development has brought new risks. Recognising that building effective capacity in cybersecurity requires strong international cooperation, the European Union launched the Cyber Resilience for Development (Cyber4Dev) project to promote a multi-layered approach to security and provide assistance to partners in developing countries. Through cooperation and coordination, significant challenges faced when building cyber capacity can be overcome and we may move towards greater cyber resilience together.

Written by: Maurice Campbell, Project Leader of Cyber4Dev

Why cyber capacity building matters

The challenges facing ministers in developing and middle income countries are many faceted, complex, and cross-cutting. Strategic approaches to national development planning are increasingly reliant on digital solutions both to ensure the effective and efficient delivery of public services, and to mitigate the drag created by the slow implementation and often spiralling cost of physical infrastructure improvements.

But becoming more active in, and reliant on, virtual space brings new risks. These new concerns are amplified by the often central and critical position of the services concerned, and by the open nature of access to the internet itself.

So we can see that the connection between a national commitment to creating a safe and secure cyberspace and crafting a climate for wider progress in economic and social development is a pretty obvious one.

Tackling cybersecurity threats is something which has to happen at multiple levels, and across the globe. The European Union has recognised that strong international cooperation is an essential element of building effective capacity in cybersecurity. The Cyber Resilience for Development (Cyber4Dev) project funded under the Instrument Contributing to Stability and Peace, implemented by the EU's International Development and Cooperation Directorate (DG DEVCO), is but one part of the EU's response.

It is clear to researchers, policy-

Figure 1. Cyber4Dev Project Leader Maurice Campbell and Project Manager Belinda Conlan attending the EU Cyber Forum in Brussels in April 2019.

"Tackling cybersecurity threats is something which has to happen at multiple levels, and across the globe."

makers and practitioners that we can no longer hope to protect ourselves by building an effective barrier which keeps all threats out. So we will from time to time suffer successful attacks on our systems. Effective capacity building in cyber resilience promotes a multi-layered approach to security, doing all we can to keep malware at bay, whilst at the same time helping governments and entities to develop the ability to bounce back from successful attacks on their systems.

Building cyber capacity with Cyber4Dev

Cyber4Dev, which seeks to draw upon a wide range of European and wider experience in order to spread best practices, has three main components:

1. Providing high quality expertise to support the development and implementation of national cyber security strategies and implementation plans.
2. Providing support to developing computer emergency response teams (CERTs) at the national level and
3. Facilitating national participation in regional and global fora focused on cybersecurity.

Under component one, the project has benefitted from engagement by ministers and representatives of critical national information infrastructure providers. The project has been designed to pay full attention to EU guidelines on the adoption of a rights based approach, and seeks to also involve civil society in activities. Particular attention is also given to opportunities that support cybersecurity education initiatives, including developing materials to support cyber hygiene awareness-raising activities in schools and universities.

"Just as the global security of aviation relies on effective controls at all airports, a more secure and resilient cyber space in one place, creates a safer global cyber space too."

Figure 2. The Cyber4Dev Logo

Under component two, a number of training courses have been held for staff working in national CERTS, each of which has been through a Security Incident Management (SIM3) maturity model assessment, the output of which has informed development plans. A number of cyber resilience exercises, both technical and table-top, have been supported and more are planned. Such exercises create very valuable opportunities for important learning, demonstrating to participants, on occasion including ministers, the risks faced and the importance of pre-planned responses, tailored to the local environment.

Under component three, the project has been able to facilitate and fund the engagement of government officials from our core countries in regional and global discourse on developing trends in cyber-security, at events organised by bodies such as AfricaCERT, The One Conference, FIRST, Meridian, the GFCE and the UK's NCSC.

Overcoming challenges through EU cooperation

Cyber capacity building is not an easy environment to work in, both because of the scarce combination of technical and international development skills required, and because of the fast pace of change in the field.

Significant challenges faced include those arising from capacity building absorption capability, and in the related areas of stakeholder engagement. Often technical and policy teams are under-resourced, and technical teams find themselves under pressure to deliver in areas which are not core to their mission, an example being computer forensic analysis in support of criminal proceedings which can divert already stretched resources. Effective stakeholder engagement also requires sustained contact, and disillusionment within especially private sector stakeholder communi-

ties can result from perceived slowness of governmental response.

Another issue can be a perceived lack of candour in the private sectors, especially in banking and finance, which arises from a risk of disclosure affecting the standing of institutions which rely very heavily on trust in building their relationships with clients.

We have benefited greatly from the counterpart working model we use to overcome such challenges. The delivery of the project is being managed by NI-CO (Northern Ireland Cooperation Overseas) in partnership with the Estonian Information System Authority (RIA), the United Kingdom's Foreign and Commonwealth Office (FCO) and the Kingdom of the Netherlands Ministry of Foreign Affairs. This allows us to access to a wide range of EU expertise and to draw upon, and learn from, significant experience.

At both the national and regional levels we have been well supported by the EU's EEAS Delegations as well as by diplomatic representations of our delivery partners. Such help was critical in establishing the right contacts from the very beginning, and in helping to ensure that host governments understood the nature and benefits of the project at the highest level. The effectiveness of this work was demonstrated at launch events attended in each case by cabinet level ministers.

Following an inception phase during which sensitization and assessment missions were conducted in three countries, Sri Lanka, Mauritius and Botswana, the project deployed coordination and technical experts to each of those countries, and is now also about to commence delivery in Rwanda. Recognising the global nature of the challenges faced, scoping missions are planned shortly in South East Asia, and South America.

We have also benefited from the excellent support of DEVCO to ensure full coordination between this project and others, including especially our sister project GLACY+, also EU funded but delivered by a highly experienced Council of Europe team, who complement our focus on cyber security with strong and effective support on tackling cyber-crime.

Towards global cyber resilience

So a minister at his desk in any of our partner countries now knows that prioritising the development of cyber resilience is not only good practice technically, but an essential underpinning of progress in many areas of wider national economic and social development plans. His staff have strong expertise to hand to assist in creating and reviewing national cyber security strategies, and the implementation plans that activate them. World leading technical assistance is provided in the development of effective Computer Incident Response Teams, and high quality training is available for staff. The new skills learnt are exercised and tested, and learning captured facilitated.

In this inter-connected world, such a focus on enhanced cyber security benefits not only the states directly assisted, but neighbouring and distant states as well. But it is also at the level of all individual citizens that we seek to have a real impact, bringing a stability that encourages investment, spreading knowledge of not only risk but also of opportunity, engaged not only with people in capital cities, but also bringing knowledge to adults and children, girls and boys, women and men alike, in all communities.

Just as the global security of aviation relies on effective controls at all airports, a more secure and resilient cyber space in one place, creates a safer global cyber space too.

"Prioritising the development of cyber resilience is not only good practice technically, but an essential underpinning of progress in many areas of wider national economic and social development plans."

Cyber Security – a joint responsibility calls for extensive cooperation

Building on Experience - the importance of an open process

Earlier this year Norway released its fourth National Cyber Security Strategy. An important part of preparing the strategy was building on experiences with previous strategies and looking internationally to build on best practices. To succeed in meeting the challenges that arise from moving towards a fully digitalized society, and at the same time take full advantage of the benefits, it was essential to align all stakeholders to pull them in the same direction. Cyber security is a joint responsibility and concerns everyone. This should be reflected in both creating and implementing a national strategy.

Written by: Robin Bakke, Specialist Director Cyber Security, Norwegian Ministry of Justice and Public Security

Strategy drafting as an open and inclusive process

The strategy drafting process was perceived to be as important as the Cyber Security Strategy itself. By having an open and inclusive strategy process, Norway sought to create ownership of the strategy for a large group of stakeholders. An ambition early on was to truly make it a national strategy for society as a whole, not only for the public sector. An open and inclusive process where everyone could contribute with ideas and input, was considered as one of the main success factors to increase the likelihood for the strategy being perceived as relevant for the different stakeholder groups.

The strategy drafting process was launched with a strategy conference that was opened by the Prime Minister. It was important to get the target group's attention from a very early stage, and to include everyone that was interested in contributing. The event was thus open to everyone who wanted to attend and the involvement of over 300 delegates, written input and high participation in a range of workshops clearly indicated that there is great interest in identifying shared solutions. Subsequent workshops with participation from both the public and private sector were also used to follow up on various target groups and prioritized areas. Drafts

> "There is no use in having a good strategy that nobody knows about."

of the strategy were shared openly in these workshops for further input and discussions in order to include stakeholders throughout the different stages of the strategy process.

Generating attention to the strategy

There is no use in having a good strategy that nobody knows about. Therefore, as an integrated part of the strategy process was to develop a media plan to get attention around the process. The media plan was developed in cooperation between selected ministries and agencies. This was seen as crucial in order to make sure the strategy got attention and was successfully implemented in the wider community.

A separate strategy launch conference was organized to increase attention for the release of the strategy. The Prime Minister of Norway, Minister of Public Security, Minister of Justice and Immigration, Minister of Defence and Minister of Research and Higher Education played a vital part in the conference and presented different parts of the strategy. This showed that the challenges we face are cross-sectorial and a key priority for the whole government. This open event was fully booked within a day, and the conference was livestreamed to gain as much attention as possible, resulting in over 1000 people following the launch of the strategy.

The Strategy

When it came to the strategy itself, it was a goal to communicate in short, easy and precise language to be able to address people with in-depth knowledge and rookies alike. The strategy contains a pull-out poster that sums up the most important aspects of the strategy so that the strategy is visible for the end user in their daily work life. In this way, it increases the likelihood of the strategy being read, remembered and used.

From the publishing of the first strategy in 2003 to now, and as Norway became the first country to release a fourth National Cyber Security Strategy, it has been important for Norway to establish a systematic approach and build on previous experiences to make the best possible strategy. An independent committee focused on identifying and assessing Norway's digital vulnerabilities was formed in 2014 and they delivered a detailed report with around 60 recommendations at the end of 2015. This assessment was followed by Norway's first white paper on Cyber Security in 2017. Together, this paved the way and lay the foundations for the new strategy. Furthermore, for the first time, Norway fully incorporated a civil-military and an international dimension in the strategy, and combined it with an "all-hazards" approach, making it a truly holistic strategy. A corner stone of the strategy is to reinforce public-private, civil- military and international cooperation.

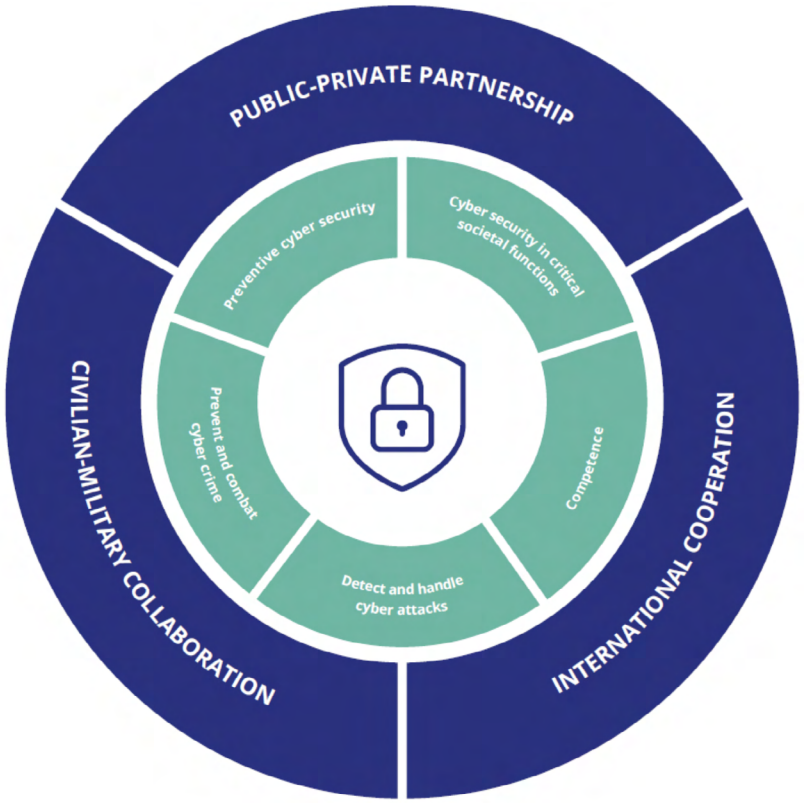
A separate list of measures was released as part of the strategy to support its implementation. It is important to underline that this only contains a selection of measures, and that all ministries are responsible for following up in their own sectors, as well as to establish whether measures initiated in their own sector sufficiently contribute to achieving the goals of the strategy.

A new approach was to not only have large national actions for the government to follow up on, but to also include ten basic points of advice for all companies in Norway to follow. The main purpose of this advice is to raise the cyber security level across

Top 10 takeaways for strategy drafting

1. Don't underestimate the value of the strategy process	6. Developing an action plan is a critical success factor. Making it available for the wider community is also important.
2. Create ownership early on and ensure relevance through engagement of all stakeholders	7. Having the action plan separate from the strategy creates flexibility in regards to updates
3. Cut to the chase – keep the strategy short and to the point	8. Not having a fixed time frame on the strategy creates flexibility to revise when necessary, not because of a fixed date
4. Use common and understandable language that communicates to both management level and technical staff	9. Look beyond the strategy – what will you be doing next and creating stepping stones
5. The strategy should support both digitalization of society and national security needs	10 Learn from others!!

Figure 1. The main elements in the Norwegian National Cyber Security Strategy



"It's only through collaboration and the sharing of experiences that we can all fully reap the benefits of digitalisation and meet common security challenges."

the whole of society. By doing this, the National Cyber Security Strategy contained something for everyone, so that all can play their part in making Norway more secure.

Capacity building at the international level is an integrated part of the strategy. Authorities and academia are encouraged to make professional experts available to participate in expert groups at the international level. The GFCE is an important partner for this and Norway participates in the Working Groups and Task Forces to share experiences with strategy development amongst other things. The long tradition Norway has with developing cyber security strategies, and with a stronger focus on international collaboration in the strategy, is something Norway sees as important to share with the international community. It's only through collaboration and the sharing of experiences that we can all fully reap the benefits of digitalisation and meet common security challenges. In this way, Norway's Cyber Security Strategy could hopefully be seen as also having an international impact.

Combatting Cybercrime: Enhancing Collaboration to Build Capacity in the Asia Pacific Region

The Korea Supreme Prosecutors' Office (KSPO), the World Bank and the GFCE are collaborating in the creation of a "hub" to combat cybercrime in the Asia-Pacific region through awareness raising, capacity building and training of key stakeholders, including policy-makers, legislators, investigators, law enforcement, NGOs, civil society and the private sector.

Written by: David Satola, Lead Counsel, The World Bank

Cooperation needed to combat cybercrime effectively

It has become clear that awareness raising, capacity building and training of key stakeholders, in addition to working with countries on elaborating enabling policies and laws, are necessary tools to effectively combat cybercrime. The Korea Supreme Prosecutors' Office (KSPO), the World Bank and the GFCE are pleased to report on a flagship initiative to address this issue.

The three parties mentioned are collaborating to establish a center for training and capacity building focused on the Asia-Pacific region. The "Hub" will facilitate coordination of delivery of training and capacity building initiatives by various organizations (mostly members of GFCE Working Group on Cybercrime) as well as working as a regional clearinghouse to ensure enhanced coordination on delivery of these activities by Working Group C members.

How the "Hub" was born

The call for enhanced coordination and collaboration was raised at the GFCE Annual Meeting in Singapore in 2018. At the meeting, under the leadership of its chair, Zahid Jamil, the members of the Working Group on Cybercrime agreed on a number of initiatives. Key among these initiatives was to focus on collaboration of its members and coordination of their various initiatives to deliver cybercrime awareness and capacity building.

In the lead up to the Singapore meeting, the GFCE undertook a mapping exercise of the various capacity-building activities of its members. This "mapping" revealed that members' coordination of delivery of their capacity-building, training and awareness-raising initiatives would benefit recipient countries, create synergies and improve efficiencies.

In the spirit of the 2018 Singapore Annual Meeting, two GFCE Members, the KSPO and the World Bank, undertook a feasibility study of various options for establishing a center for training and capacity building focused on the Asia-Pacific region under the auspices of a grant provided by the Korea World Bank Partnership Facility (KWPF).

The feasibility study recommended that delivery would be best coordinated through the active involvement of the organizations and institutions that are already involved in that delivery. To arrive at this conclusion, the feasibility study aimed (i) to maximize efficiencies of delivery and to avoid duplication of effort and (ii) to ease the burden on recipient countries in managing multiple providers. Given the demand for both training and capacity building as well as the demand for enhanced coordination, the GFCE seemed a ready-made platform as it already includes all of the major players – international organizations, bilateral donors, NGOs and private sector actors. The idea of a "hub" for coordinating these activities in the Asia Pacific region was born.

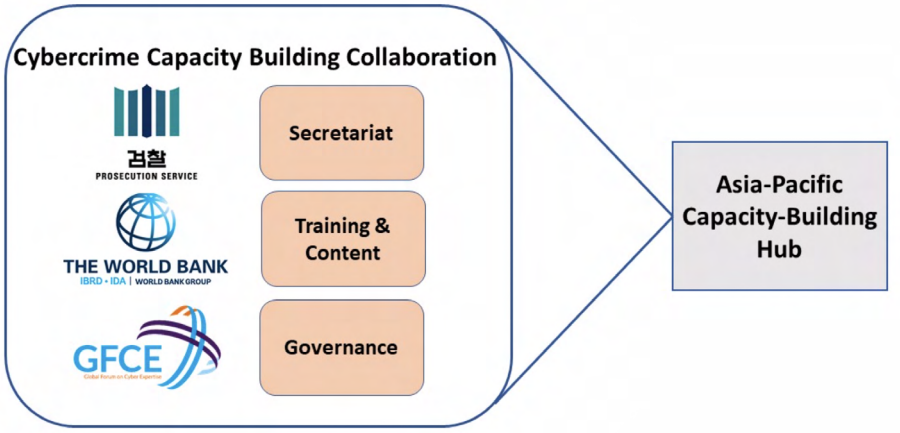


Figure 1. The proposed collaboration between the KSPO, the World Bank, and the GFCE.

The Hub

The ethos of the Hub is to enhance synergies for the benefit of the countries receiving assistance. Organizations already delivering capacity building activities will continue to do so in accordance with their existing mandates. The Hub will thus function as a facility for countries and organizations in the region to better coordinate their activities and take advantage of the activities of other organizations.

In addition, the GFCE has also conducted an in-depth mapping exercise of activities of all of its members. It is expected that the Hub would benefit from and also contribute to such an exercise.

KSPO and the World Bank presented a proposal for the Hub to the members of the GFCE Working Group on Cybercrime at the GFCE's inaugural intersessional Spring Meeting in The Hague in April 2019. The essence of the proposal is shown in the graphic Figure 1.

Under the proposal, the World Bank will coordinate and provide training materials to the Hub in accordance with the KWPF grant. These materials will follow the structure of the Toolkit (available at http://www.combattingcybercrime.org). The Toolkit was also financed by KWPF and included participation of Working Group C members, including the Council of Europe, UNODC, KSPO and the Oxford Cybersecurity Capacity Building Centre. Additionally, KSPO will act as the secretariat and coordinator of the activities of the Hub and the GFCE Working Group on Cybercrime is expected to serve as a platform for to providing peer review and logistical and administrative support for the delivery of capacity building programs. The Working Group on Cybercrime endorsed this proposal at the GFCE's inaugural Spring meeting in the Hague.

It is hoped that once the Hub has "demonstration effect" it could be a model for other regional coordination initiatives.

Indian Initiative of Capacity Building for Senior Government Officials

The cyber threat landscape is changing rapidly. In this quick changing scenario, it is necessary to keep Government officials abreast of latest developments in cyber security. The deep-dive training programme "Cyber Surakshit Bharat" was initiated with the objective to educate & enable Chief Information Security Officers (CISOs) and the broader IT community within Government to address and mitigate the emerging challenges of cyber security and create awareness. The programme aims to train 1200 officials and since its launch, 486 officials have already been trained.

Written by: Dhawal Gupta, Shri Dipak Singh, and Shri Rakesh Maheshwari, Cyber Law & e-Security Division, Ministry of Electronics & Information Technology

Digitalisation of India's Government

India is moving towards a digital economy with an ever-increasing use of internet and interconnectivity technologies. As technology drives governance, traditional work culture is expected to change and hence, keeping abreast with the technology is very important for senior government officials so that they can make informed decisions.

National e-Governance Plan (NeGP) was launched in 2006 as a holistic view of e-Governance initiatives across the country with the vision to "make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realise the basic needs of the common man". In order to promote e-Governance in a holistic manner, various policy initiatives and projects were undertaken to develop core and support infrastructure.

The NeGP was later subsumed under the 'Digital India' campaign in 2015, with the vision to transform India into a digitally empowered society and knowledge economy. This project pulled together many then-existing initiatives which were to be restructured and refocused for implementation in a synchronised manner.

With the growing penetration of the internet and the digitalization of governance, ensuring cyber security

Figure 1. The launch of the Cyber Surakshit Bharat programme by Honourable Minister of State (Electronics & IT) with industry leaders.

is becoming critical. A cyber breach can cause severe financial damage and bring the functioning of government and government organisations to a standstill. It is therefore imperative, that every organisation involved in the use of Information Technology in the discharge of its functions must identify and document its Information Security (IS) requirements.

To strengthen cyber security in government departments, the appointment of a Chief Information Security Officers (CISO) was advised to State governments, government organizations, public sector units (PSU), etc. The CISOs shall be responsible for maintaining and updating the threat landscape of the organisation on a regular basis, including staying up to date on the latest security threat environment and related technology developments and take corrective actions.

The "Cyber Surakshit Bharat" programme

The "Cyber Surakshit Bharat" programme was launched on 19th January 2018 to educate and enable the CISO's and broader IT community within Government to address and mitigate the emerging challenges and create awareness. This includes a series of regional workshops, deep-dive trainings for designated CISOs and the officers responsible for cyber security in their respective government organization.

The deep-dive training of CISOs and other frontline IT government officials is supported by a consortium of industry partners and it is unique example of Public Private Partnership. The industry partners are Microsoft, IBM, Intel, PaloAlto Networks, E&Y, Samsung and Amazon Web Services. The knowledge partners from the government include the National Information Centre (NIC) - an arm of the Ministry of Electronics and Information Technology (MeitY), Computer Emergency Response Team of India (CERT-In), Standardization Testing and Quality Certification (STQC) Directorate - an attached office of MeitY, and Centre for Development of Advanced Computing (C-DAC) an autonomous organization under MeitY. The training is conducted at 6 cities in the country namely New Delhi, Mumbai, Kolkata, Bengaluru, Chennai and Hyderabad.

Cyber Security is a vast domain that ranges across policy, process, legal and regulatory framework, change management and core technology. As such, the target audience for the deep-dive training have different backgrounds as well, some with a highly

"Since the training started in June 2018, 486 officials representing various Central and State Ministries and PSUs have been trained so far through 12 batches of training."

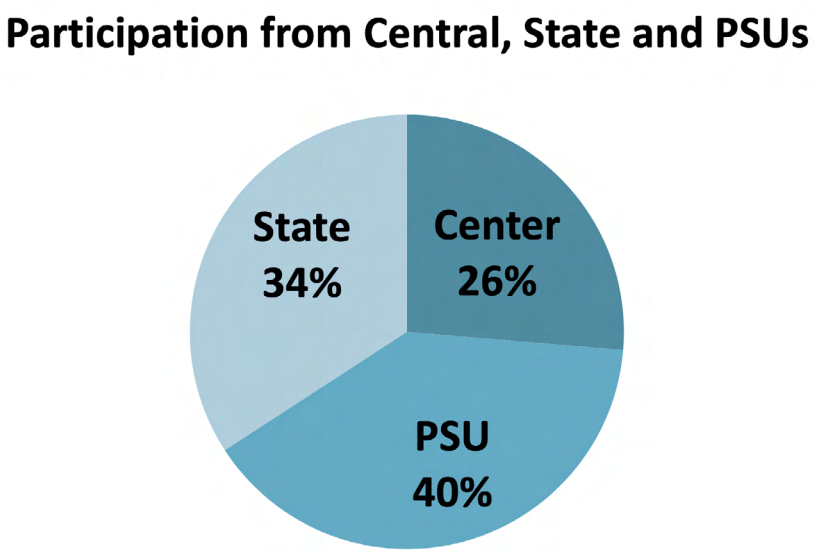


Figure 2. Pie-chart showing the percentages of participation by Central/State Government and Public Sector Unit officials in Cyber Surakshit Bharat programme.

technical background while some with no prior technical experience. The basic CISO deep-dive training is therefore designed for a heterogeneous audience group to accommodate all participants and encourage cross-learning built through intensive class group work and individual assignments.

The programme has a target of training 1200 CISOs and officials responsible to observe cyber security in their respective organizations. Since the training started in June 2018, 486 officials, representing various Central and State Ministries and PSUs have been trained so far through 12 batches of training.

Feedback on the training sessions

By and large, the post-training feedback and validation suggests that the training has been immensely useful for participants in better understanding their roles and responsibilities as a CISO, while enhancing their knowledge about cyber security. It has also broadened their understanding of the technical and legal aspects involved in drafting policies for safeguarding their organizations against cyber threats. The participants also felt that program provided a forum for interaction and enabled learning from peers in similar roles.

As a part of the structured feedback collected, participants also provided suggestions on improvement or enhancement of future programs. One major suggestion is to have further training to address sector specific training needs, for example in the power and finance sector.

The way ahead

This training initiative has created an army of Cyber Security enthusiasts in State and Central government organizations, including critical sectors like IT services, defence & defence production, energy, telecom,

"There is an opportunity to institutionalize and scale up the capacity building drive, which is currently limited to basic training of a targeted set of officers in the Government."

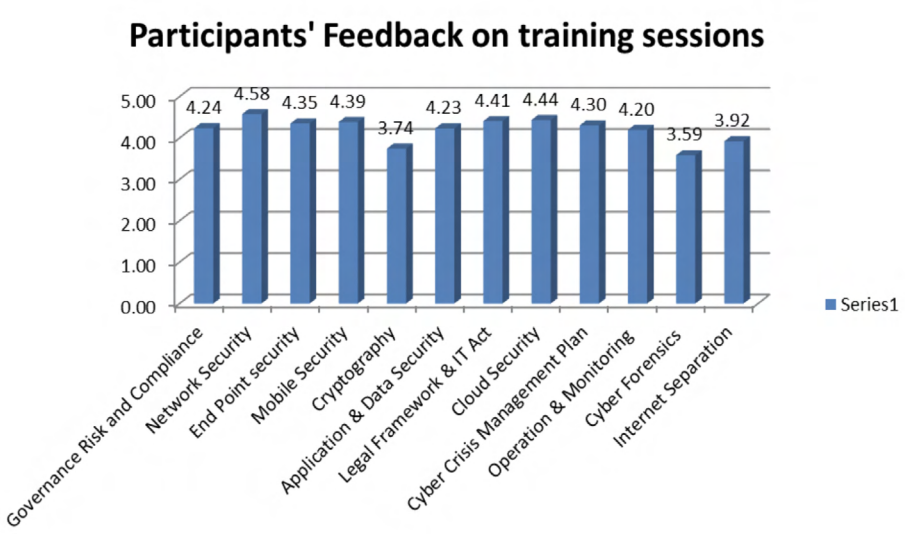


Figure 3. The cumulative qualitative feedback collected based on a scale from 1-5, with 5 being best.

election bodies and public service examinations, finance, public sector banks and insurance companies.

It is important to not only keep this motivation aligned but also build an enabling ecosystem to further ensure transfer of learning and tangible outcomes of the developed capacities within the Government. Furthermore, there is an opportunity to institutionalize and scale up the capacity building drive, which is currently limited to basic training of a targeted set of officers in the Government.

Most of the CISO training participants have also underlined a need for a platform where they can regularly interact with other participants to share their problems and issues, and to consult peers and experts easily. Besides continuing with the basic programme to achieve the initial target training of 1200 CISOs, the way forward is to develop a:

- **Community of CISOs** for ongoing cross-learning and knowledge exchange.
- **Reward and Recognition of CISOs:** This will not only help in encouraging documentation and adoption of better practices, but in the long run, will be critical in institutionalizing CISOs as an important function in government organizations.
- **Impact Assessment of CISOs Training and ongoing Training Need Analysis:** To evaluate changes in the job behaviour that resulted from the programme and its impact on organizational effectiveness.
- **Vertical Deep-Dive training programmes:** There are regular requests and feedback reiterating the need for specific training programmes that dives vertically into each module with a focus on technology and hands-on experience.
- **Assessment and Certification** of basic skills and competency to assume responsibility as a CISO.

The current process of OAS confidence-building measures in cyberspace

Stability and governance of cyberspace has become one of the most relevant issues in the field of international security. Confidence-building measures (CBMs), understood as a diplomatic tool to reduce mistrust, misunderstandings and enhance cooperation have historically contributed to maintaining peace in the Western Hemisphere. In 2017, the Organization of American States (OAS) established a Working Group (WG) on Cooperation and CBMs in Cyberspace that has met annually since then. During the last meeting, held in Santiago de Chile, the WG agreed on four measures that addresses the need to increase engagement among Ministries of Foreign Affairs (MFAs) in the development of cybersecurity and cyberspace policies. MFAs are essential when building cooperation between States, but also for discussion, work and negotiations on international norms.

Written by: Mila Francisco Ferrada, Alternate Representative from Chile to OAS
Pablo Castro Hermosilla, Analyst, Ministry of Foreign Affairs Chile

International law and cyberspace

The debate on the stability and governance of cyberspace has become one of the most relevant issues in the field of international security. Until States and relevant stakeholders reach an agreement on exactly how this new domain will be governed, many countries have been investing in offensive and defensive cybernetic capabilities of a military nature, while others do not refer to international law when using cyberspace. These factors increase the risk of escalation and conflict and will continue to do so as Internet-based platforms and infrastructure continue to grow.

The consequences of such scenarios can be serious. For this reason, the international community has engaged in global and regional processes that seek to determine how international law applies to cyberspace, to the development of norms that regulate the behavior of States in this area and underpinning a renewed agenda of confidence-building measures (CBMs).

Creating a culture of cybersecurity in the Americas

CBMs are a diplomatic tool that aim to deter escalating conflicts by reducing mistrust, misunderstandings and miscalculations. In our Region, CBMs have been an effective tool that have historically contributed to maintaining peace at the inter-state level.

At the Regional level, the current regime of CBMs, which must be notified in accordance with OAS resolutions, is the Consolidated List of Confidence and Security Building Measures approved in 2009 (with subsequent modifications). In this regard, the OAS, through CICTE, has developed an important work in the field of cybersecurity and cyberspace.

In 2004, the OAS established "A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". This strategy encompasses a series of initiatives aimed at strengthening trust in cyberspace, such as the establishment of an Inter-American vigilance and alert network to rapidly disseminate cybersecurity information and respond to crises and incidents, and to develop legal capacities of the OAS member states to protect Internet users and information networks.

Figure 1 and 2. First meeting of the Working Group on Confidence Building Measures in Cyberspace with a round table to facilitate discussions between participants.

Working Group on CBMs

Following the strategy's initiatives, in April 2017, the OAS approved a Working Group on Cooperation and CBMs in Cyberspace. This proposal was presented by Chile, Colombia, Peru, Costa Rica, Canada, Guatemala and Mexico.

The first meeting of this Working Group was held on February 28 and March 1, 2018 in Washington. Two CBMs were agreed upon: the first on the exchange of information on national cybersecurity policies (strategies, white papers, legal frameworks, etc.), and the second on the identification of national contact points at the political level. These measures were included in the 2009 consolidated list in the non-traditional section. The meeting also decided to establish a work plan to develop additional measures. Colombia assumed the presidency of the group in 2018.

Figure 3. Chile assumed the presidency of the Working Group on Confidence Building Measures in Cyberspace during the second meeting.

"MFAs and diplomacy are powerful and important tools when it comes to building not just "cooperation bridges", but also in the discussion, work and negotiations on international norms and CBMs."

The second meeting of the Working Group was held in Santiago, Chile on April 23 and 24, 2019. During the meeting, Chile assumed the presidency for the period of one year, and Member States agreed to the following additional voluntary cyber CBMs to promote and strengthen the engagement of MFAs and diplomacy on cybersecurity, and cyberspace policies in the region:

1. To designate points of contact, in the event that none exist, within the MFAs, with the purpose of facilitating the work on international cooperation and dialogue in cybersecurity and cyberspace.
2. To develop and strengthen capacity-building through activities such as seminars, conferences, workshops, among others, for public and private sector officials in cyber diplomacy.
3. To foster the inclusion of cybersecurity and cyberspace subjects into training courses for diplomats and officials of the MFAs and other government agencies.
4. To foster cooperation and exchange of best practices on cyber diplomacy, cybersecurity and cyberspace through, for example, the establishment of working groups, other dialogue mechanisms, and the signing of agreements among states.

Also, considering the importance of implementing the measures adopted, the Working Group agreed on recommendations to make effective use of the national contact points (CBM 2 from 2018).

The adoption of these four measures responds to the need to increase engagement among MFAs in our region in the development of cybersecurity and cyberspace policies. Perception of these subjects as technical and not necessarily political challenges tend to diminish the importance the MFA plays in their definition. However, MFAs are essential when building cooperation between States. MFAs usually coordinate national policies and decisions on cyberspace and cybersecurity in the international scene.

Strengthening cyber diplomacy and cooperation

MFAs and diplomacy are powerful and important tools when it comes to building not just "cooperation brid-

"It is important to build an open, stable, secure, transparent and governable cyberspace in the region, in accordance with international law and with clear rules of responsible behavior."

Figure 4. Second meeting of the Working Group on Confidence Building Measures in Cyberspace held in Santiago, Chile on April 23 and 24, 2019.

ges", but also in the discussion, work and negotiations on international norms and CBMs. Cyber diplomacy, then, is a crucial dimension for the international discussion of cybersecurity and cyberspace. Considering that the current process of discussion, negotiation and adoption of CBMs within the framework of the OAS is a good example of this, it seems logical that States adopt measures that allow and help to strengthen cyber diplomacy.

Cyber diplomacy is also relevant considering that the Americas presents unique characteristics that could generate a renewed approach to CBMs in cyberspace, which goes beyond the aim of de-escalating possible conventional conflicts alone. Here, the possibility of states using cyberspace to conduct attacks on other states may be remote, given the increasing occurrences of conflicts and inter-state tensions.

Consequently, at the Regional level, the establishment of CBMs in cyberspace should encourage cooperation, joint work, the development of national capacities and cyber diplomacy, amongst others. This region, as demonstrated in the past, has the capacity to agree on principles and practices, between States with a similar vision, which can become standards that others tend to accept. It is important to build an open, stable, secure, transparent and governable cyberspace in the region, in accordance with international law and with clear rules of responsible behavior. A long term challenge will be to establish effective mechanisms for implementation, and in this regard, it will be essential to be able to help countries within the region develop their national cyber capacities.

OAS and CISCO launch the "Cybersecurity Innovation Councils"

Innovation at the service of the cybersecurity

The General Secretariat of the Organization of American States (GS/OAS) through its Cybersecurity Program and CISCO launched the Cybersecurity Innovation Councils (CICs) in Latin America. This initiative aims to drive innovation, raise awareness, and expand best practices in cybersecurity across the region.
The CICs will be comprised of representatives of the GS/OAS and CISCO, and prestigious professionals from the public and private sector, industry associations and academia. The multi-stakeholder design seeks to solve cybersecurity challenges by incorporating varied perspectives with the understanding that no single actor can effectively solve today's cyber challenges. Collaborative innovation is required between these key players for the purpose of developing better approaches and effective solutions for today's cyber issues.

Written by: Co-authored by the Inter-American Committee against Terrorism (CICTE) – OAS and CISCO

The partnership

With over 12 years of experience, GS/OAS Cybersecurity Program has become a regional leader in assisting countries in Latin America and the Caribbean to build technical and policy-level cybersecurity capacity. The initiatives and activities carried out by the Program aim at ensuring an open, secure and resilient cyberspace throughout the Western Hemisphere. To promote cybersecurity in the Western Hemisphere, the GS/OAS recognizes that it is essential that representatives from the private sector be involved in the protection of citizens' rights in cyberspace.

CISCO has been an important partner in promoting education and technology that help improve cybersecurity by contributing to capabilities needed for a safer cyberspace globally. CISCO, as

"Members of the CICs will discuss the best way to promote innovation, raise awareness among citizens and disseminate best practices in cybersecurity."

Figure 1. Michael Timmeny, SVP and Chief Government Strategy Officer, Cisco and Luis Almagro, Secretary General of the OAS.

a global technology and cybersecurity leader, plays a vital role in cybersecurity and continually works with customers, partners, and governments to understand the cybersecurity landscape and prepare for evolving threats. As an example, Cisco blocks globally 20 Billion threats per day through the broadest threat telemetry. Given the focus that many regional governments have on digital transformation both of their government and in their country, CISCO has jointly developed the CIC to collaborate with the OAS and key members of the cybersecurity community.

The agreement

The collaboration agreement was signed in August this year and the Launch Event took place during the Fall at the OAS Headquarters in Washington DC. At that initial meeting, key members of the OAS and Cisco. The CICs will meet three times over the course of two years for workshops that reconvene the Council members to collaborate on innovative solutions.

CIC meeting will be organized as a strategic workshop by CISCO and the GS/OAS. Members of the CICs will discuss the best way to promote innovation, raise awareness among citizens and disseminate best practices in cybersecurity. Design thinking techniques will be used to engage the participants, lead collaboration on key ideas and drive pragmatic conclusions.

The OAS and CISCO will provide cybersecurity content and technical expertise during the Council discussions and workshops. There will also be follow-on presentations and discussions of Council content with re-

levant stakeholders in each country to share the findings of the Council and promote local discussions of cybersecurity.

An additional regional event will be held during 2020 after the first round of CICs have taken place. This event will bring together again the first representatives, OAS and Cisco to share once again the best practices and lessons learned from the first year of activity.

A key output of the CICs and this alliance will be the joint dissemination of content generated by the Council such as white papers, blogs or other publications for use in various channels such as social media, press releases or online presence.

Funding innovative projects

In the spirit of collaboration and innovation, a key final area of the alliance and the councils will be to design new projects that respond to the issues raised regarding national cybersecurity concerns. By definition, the final scope of these innovation projects will be agreed at a future date with the input from the CICs taking into context the specific challenges of each country. Some possible examples include:

a. Youth projects: education-focused campaign or event to raise awareness of cybersecurity threats and good habits among the youth population of the country.
b. SME's: Design a project for collaboration between national Computer Security Incident Response Teams, including technical training and exploration of best practices for incident response process across national entities.
c. Certification or training: GS/OAS Cybersecurity Program and CISCO offer significant training of many types regarding cybersecurity, technical training and ongoing certifications. Cybersecurity, IoT, and core network security are all key components of the certifications offered around the region.
d. Hackathons: creation of cybersecurity focused hackathons which result in hands-on experience followed by guidance and support to cybersecurity technicians from across the region.
e. Simulations: using, for example, "Capture the Flag" or "Red Team Green Team" techniques to offer experience in threat hunting, cybersecurity incident response, cyber defense or other simulations of real attacks and defenses.

Enhancing Cybersecurity in the Americas

In conclusion, the OAS and CISCO will convene national Councils with the overall objective of advancing cybersecurity solutions, best practices and education in an innovative fashion. The Council approach will by design bring together different perspectives from multiple distinguished participants with expertise in the various facets of cybersecurity. The Council and its objective are directly aligned with the OAS' focus on hemispheric security, as well as with CISCO's focus on a broad approach to education and technology for improving cybersecurity for citizens, companies and countries. The contributions of the Councils of each country will ensure that the local context is captured at the same time that the regional approach will enable international sharing to enrich all of the participants and the public discourse around cybersecurity in the Americas.

Cybersecurity a Flagship project of the African Union Agenda 2063

Cybersecurity is a major risk for the digital revolution in Africa. Decision makers and business leaders in Africa always cite the proliferation of cyber incidents as the culprit for the slow adoption of ICTs on the continent. The African Union Commission has been playing a leading role in ensuring its member states are well equipped to face this challenge and to mainstream cyber culture across Africa.

Written by: African Union Commission

Digital transformation for Africa

Africa presents a sea of economic opportunities in virtually every sector, and the continent's youthful population structure is an enormous opportunity in this digital era. For this reason, Africa is making digitally enabled socio-economic development a high priority.

Digital Transformation is a driving force for innovative, inclusive and sustainable growth in Africa. From innovations such as for mobile money platforms to large-scale business process outsourcing developments, digitalization is creating jobs, addressing poverty, reducing inequality, facilitating the delivery of goods and services, and contributing to the achievement of Agenda 2063 and the Sustainable Development Goals.

It is within this context that the African Union (AU) Commission in collaboration with the UN Economic Commission for Africa, Smart Africa, AUDA-NEPAD, Regional Economic Communities, African Development Bank, Africa Telecommunications Union, Africa Capacity Building Foundation, International Telecommunication Union and the World Bank, is currently finalizing the development of a Comprehensive Digital Transformation Strategy for Africa to guide a common, coordinated digitalization agenda. Cybersecurity, privacy and personal data protection is one of the cross-cutting themes of the Strategy.

Cybersecurity needed for digital development

The incidents and threat of cyber breaches, as well as the spread of viruses and malware is pervasive. Given the global threat, a comprehensive and consistent response is required. Only by raising the awareness of the public, educating businesses on

Figure 1. Workshop for AU Member States on cyber strategy, cyber legislation and setting up CERTS organized in July 2018

cybersecurity, collaborating with industry groups and associations, and encouraging cybersecurity firms and services, can the enormous threat be mitigated. Without trust, the digital economy cannot flourish.

It is against this background that the AU Executive Council at its 32nd Ordinary Session held from 25- 26 January 2018, in Addis Ababa, Ethiopia adopted decision EX.CL/Dec.987(XXXII) in which it endorsed the AU Declaration on Internet Governance and development of digital economy and adopted cybersecurity as a flagship project of the African Union Agenda 2063.

Furthermore, the AU 23rd Assembly of Heads of State and Government adopted the AU "Convention on Cybersecurity and Personal Data Protection". This convention also known as the Malabo Convention seeks for a common approach at continental level on the security of the cyberspace and to set up minimum standards and procedures to define a credible digital environment for developing the electronic communications and guarantee the respect of the privacy online.

The convention is now open to all Member States of the AU for signing and ratification in conformity with their respective constitutional procedures and subsequently the convention shall enter into force thirty (30)

"Without trust, the digital economy cannot flourish."

"Online training materials will be made available to ensure the capacity building effort reaches as many African Internet communities and policy makers as possible."

days after the date of the receipt by the Chairperson of the Commission of the AU of the fifteenth (15th) instrument of ratification.

More steps to promote and improve cybersecurity

Since the adoption of the Malabo Convention, the AU Commission has been organizing cybersecurity capacity building workshops, in collaboration with our key partners, Regional Economic Communities (RECs) and Member States, to promote cybersecurity culture and build trust and confidence in the use of ICTs by and for the African citizens, provide guidance on cybersecurity policy and strengthening cyber capacities of Member States on:

- Cybercrime prevention,
- Online Privacy and personal data protection,
- Preparation of Cyber-Strategy and Cyber-Legislation; and
- Setting up incident response mechanisms such as CERTs/ CIRTs

In addition, the AU Commission in cooperation with Internet Society, developed Guidelines on "Security of Internet infrastructure in Africa" and "Personal Data Protection for Africa", and also published a report on cybersecurity and cybercrime trends in Africa in cooperation with Symantec and US State Department.

Sensing the need for sound and consensus-based advice on emerging issues pertaining to cybersecurity, the AU Commission has undertaken steps to create an African Cybersecurity Experts' Group, composed of 10 – 15 members representing the African region, whose sole mission is to advise the AU Commission on cybersecurity matters.

Another important step taken by the AU Commission in close collaboration with the European Commission, is the launching of the "Policy and Regulation Initiative for Digital Africa (PRIDA)". Building capacity of African Internet stakeholder groups in all 55 AU Member States on Internet Governance (IG) and Cybersecurity/ Cyber-resilience matters is one of the critical tracks of PRIDA. It is anticipated that IG training courses will be administered at national, regional and continental levels. Online training materials will be made available to ensure the capacity building effort reaches as many African Internet communities and policy makers as possible.

Finally, for the AU Commission to make significant advances and real impact in this space, promoting robust partnerships with reliable domestic and international allies who enjoy leading-edge capabilities and know-how will be vital.

An interview with Dr. Amani Abou-Zeid on cybersecurity and the AUC's priorities

Dr. Amani Abou-Zeid is the African Union Commissioner in charge of Infrastructure, Energy, ICT and Tourism

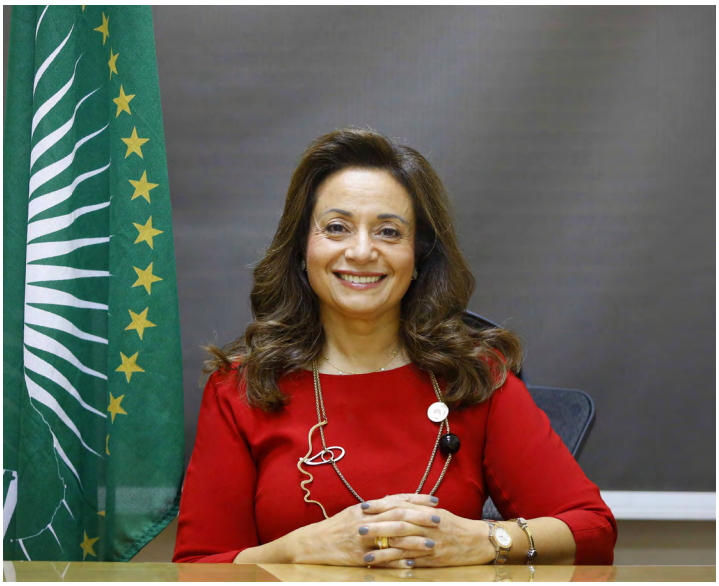


Figure 1. Dr Amani Abou-Zeid

Written by: African Union Commission (AUC)

For more than 30 years, Dr. Abou-Zeid has served in leadership positions in international organizations, such as the African Development Bank, UNDP and USAID, with a focus on infrastructure and energy programs. Over her career, she has amassed a remarkable mix of experience from across Africa, France, UK and Canada and worked across constituencies and with wide array of stakeholders.

Q: Why is digital transformation for Africa urgent now?

Digital Transformation is the greatest opportunity for Africa's development potential. It is well know that for every 10% increase in broadband penetration, GDP can rise by 1.3% and jobs will grow by 3%. Digital transformation contributes to promoting education accessibility and social integration in Africa, reducing unemployment rate, ensuring both public and personal safety and security, and improving government and business efficiency and transparency.

With the right Digital Transfor-

"The increasingly digital and data driven economy also comes with risk and challenges, therefore requiring new rules that would generate trust, protect and secure data across the entire value chain."

mation strategy, Africa will be in a better position to leapfrog into the 21st century and catch up with the rest of the World.

Digital Transformation is now at the top of African Union Agenda as an enabler of socio-economic development. The Chairperson of the AU Commission H.E. Mr. Moussa Faki Mahamat and other African leaders have repeatedly emphasized this including more recently during the 32nd African Union Assembly of Heads of State and Government that took place early February 2019 and in the presence of many of our continental and international partners like Estonia, the United Nation Agencies, the African development Bank, the World Bank, and the European Investment Bank.

It goes without saying that the Digital Transformation is at the top of my department's priorities. We will be working with all our partners around the world to make sure that our African Digital Agenda priorities are timely implemented for the benefit of our people.

Q: What is the strategic imperative of cybersecurity for AUC?

Undoubtedly, the rise of digital technologies offers the prospect to unlock tremendous opportunities and new pathways for economic growth, economic mobility, innovation, job creation and access to quality services by citizens. The accelerating pace of technology, the convergence of multiple technologies, and the emergence of global platforms are changing traditional development models and value chains. With that said, the increasingly digital and data driven economy also comes with risk and challenges, therefore requiring new rules that would generate trust, protect and secure data across the entire value chain.

Being connected to the rest of the world means that Africa is now within the perimeter of cybercrime, making the continent's information systems and digital infrastructures rather vulnerable. Unfortunately, both governments and private sector entities in Africa have increasingly been experiencing cyber-attacks, reflecting and sometimes amplifying the global trends in this area. In essence, there is an urgent necessity to ensure that citizens, governments and businesses are protected.

Q: What are some of the concrete steps that the AUC has taken to promote Cybersecurity?

First: Following the adoption of the Malabo Convention in 2014, the AUC has been organizing capacity building and sensitization workshops on Cybersecurity for our Member States to address:

- Cybercrime issues,
- Online Privacy and personal data protection,
- Drafting of Cyber-Strategy and Cyber-Legislation,
- Setting up of incident response systems such as CERTs/ CIRTs

Second: The AUC published in collaboration with Internet Society, Guidelines on:

- Security of Internet infrastructure in Africa; and
- Personal Data Protection for Africa;
- We also published in 2016, in cooperation with Symantec and US State Department, a report on Cybersecurity and Cybercrime trends in Africa

Third: The AUC has recently established an African Cybersecurity Experts' Group whose sole mission is to advise the AUC on Cybersecurity matters. The first experts' group meeting will take place during this year.

Finally: The AUC has launched in cooperation with the European Union the "Policy and Regulation Initiative for Digital Africa (PRIDA)". Building capacity in all 55 AU Member States on Internet Governance and Cybersecurity/ Cyber-resilience matters is one of the critical tracks of PRIDA project.

Q: Given all that has been accomplished by the AUC so far, what are the missing elements in order to have real impact?

At the continental level, the Executive Council of the African Union endorsed in 2018 "the AU Declaration on Internet Governance and development of the Digital Economy in Africa and adopted Cyber Security as a Flagship project of the African Union Agenda 2063".

However, in order for the African Union Commission to make real progress and ensure that all African countries are well positioned and fully equipped to tackle this serious issue, the AUC must firstly embark on a cybersecurity awareness campaign targeting policy makers, businesses and citizens at national, regional and continental levels. AUC must ensure that sound cyber culture policies are being implemented on the continent.

Secondly, to enable actions and concrete steps in this area, the AUC must foster strong partnerships with countries and international players who possess capabilities and know-how.

Q:With the limited resources available to AUC, what are the key priorities in the short term?

It is critically important to assist the AU Member States with:

First: Development of national cyber-security strategies, in line with international standards and practices as well as supporting the creation of national governance for Cyber-security;

Second: Adopting and Implementation of legal frameworks for online privacy and personal data protection as to allow African citizens to safely and securely use ICT for their socio-economic development (Health, education, governance etc.) as a sine qua none condition for peace and stability;

Third: Enforcing the existing national criminal laws and adapt them to the reality of digital environment to effectively fight against all kind of cybercrime and cyber-attacks. Developing legal and Regulatory frameworks and specific provisions related to cyber legislations,

Fourth: Develop technical capabilities to monitor and defend national networks to protect Institutions against the threats and attacks capable of endangering their survival and efficacy;

Fifth: Establishing and operating Computer Emergency / Incident Response Teams (CERTs/CIRTs),

Finally: Developing continental and regional mechanisms to increase regional and international cooperation on Cybersecurity and build an Africa CERT at the African Union Commission HQ

The AUC must foster strong partnerships with countries and international players who possess capabilities and know-how."

UN Office for Disarmament Affairs and Singapore Cyber Security Agency launch online training course "Cyberdiplomacy"

In partnership with Singapore, the United Nations Office for Disarmament Affairs has developed an online training course on cyber diplomacy to encourage a greater understanding of the use of ICTs and its implications for international security. Through an interactive audio-visual learning experience, the course aims to promote the application of international guidance developed by a series of Groups of Governmental Experts (GGEs) convened since 2004 and to help Member States prepare for the intergovernmental processes taking place from 2019 to 2021. Experts from different sectors contributed to the course, which is also intended as a useful tool for stakeholders in civil society, academia and the private sector.

Written by: UN Office for Disarmament Affairs (UNODA)

Use of ICTs and International Security

Since 2004, the UN General Assembly has established five Groups of Governmental Experts (GGEs) to examine the existing and potential threats from the use of ICTs and possible cooperative measures to address them. Three of these Groups have agreed on substantive reports, with conclusions and recommendations that all UN Member States have welcomed.[1]

Importantly, in 2016, the General Assembly adopted resolution 71/28, calling on Member States to be guided in their use of information and communications technologies by the 2015 report[2] of the Group of Governmental Experts on ICTs in the context of international security.

With three in-depth substantive documents in place and the possibility that this corpus of international guidance on cybersecurity will continue to grow, the UN Office for Disarmament Affairs, in partnership with the Singapore Cyber Security Agency, developed an online training course to

encourage greater understanding of the use of ICTs and its implications for international security, based on the contents of the GGE reports.

Meeting the demand for awareness-raising on the work of previous GGEs

By unpacking the key elements and recommendations formulated by the GGEs, the training course is designed to facilitate their application by UN Member States. The course is also intended to support the capacity of States to engage in cyber diplomacy as UN Member States prepare to collectively consider, over the coming years, the issue of international ICT-security in an Open-ended Working Group, and in parallel, a new Group of Governmental Experts[3]. These processes will be informed by the work of the previous GGEs. This online training course fulfils a need for greater understanding of previous findings and recommendations, and its online format makes it readily accessible to audiences around the world.

The training course is also available to the private sector, non-governmental organizations and academia, which will be engaging with intergovernmental processes on international ICT-security for the first time. In this context, the course provides an opportunity for these actors, many of whom have never engaged with these processes, to enhance their understanding of the issues being considered by States.

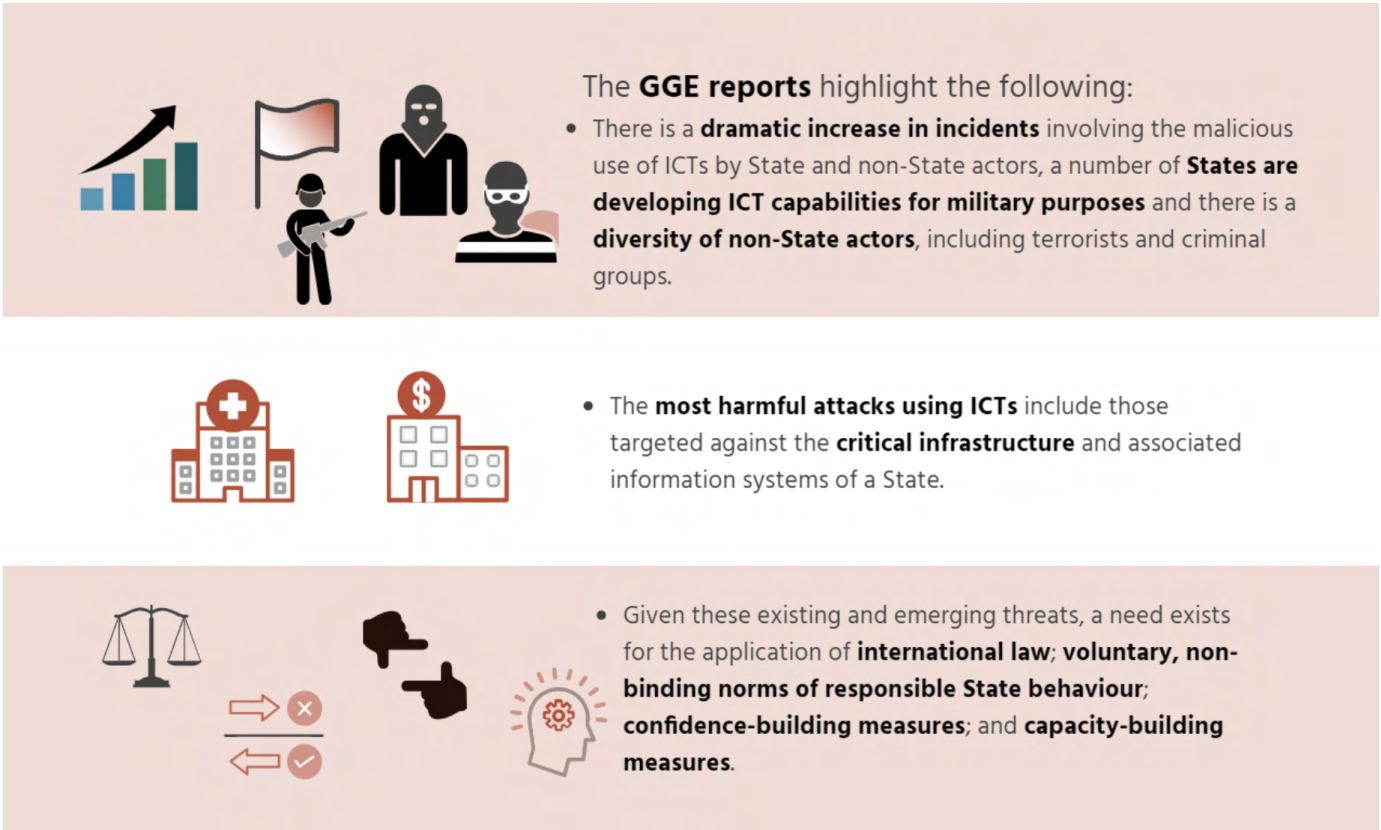


Figure 1. In an "Existing Threats" module, participants are introduced to the range of threats in cyberspace.

Substantive scope of the course

The modules of the training course are based on the five pillars of the GGEs' work:

1. Existing and emerging threats in the ICT environment;
2. How international law applies to the use of ICTs;
3. Norms, rules and principles for the responsible behaviour of States in the use of ICTs;
4. Confidence-building measures to ensure a peaceful ICT environment; and
5. International cooperation and assistance in ICT security and capacity-building.

The course can also be tailored to be used in workshops or other trainings aimed at building the capacity to implement regional or global measures in the field of international ICT-security. These could include, for example, the 11 voluntary, non-binding norms of responsible State behaviour and the confidence-building measures recommended in the 2015 GGE report.

The learning experience

The course incorporates a variety of audio-visual content in a user-friendly manner, meeting the highest standards of accessibility. With its interactive elements, the learning experience encourages participants to progressively deepen their thinking on international ICT-security by applying newly acquired knowledge to solve problems.

The training materials were deeply enriched through the collaboration with a range of experts and organiza-

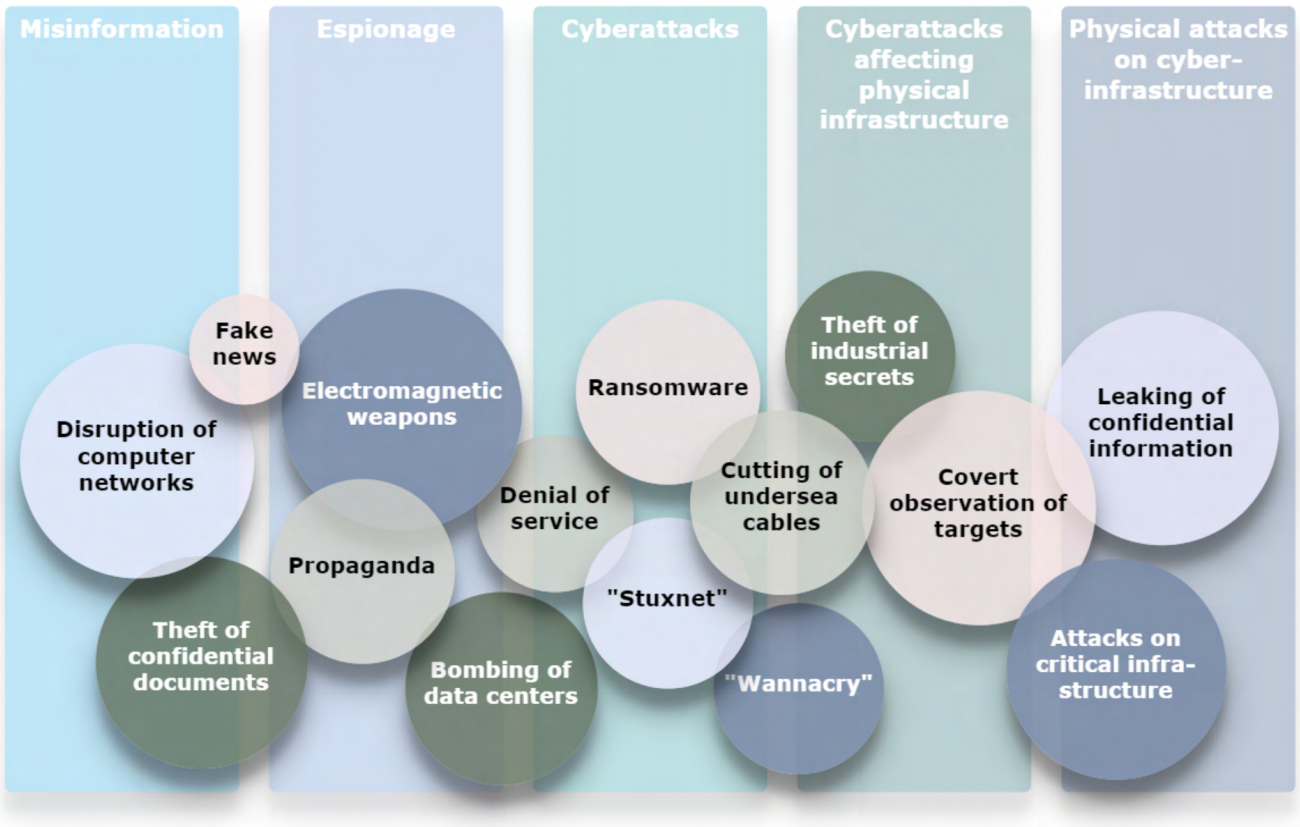


Figure 2. Which type of attacks belongs to which category? This drag-and-drop activity challenges participants to apply their acquired knowledge.

tions from around the world, many of whom took part in a collective review of the course in New York. Throughout the modules, learners can benefit from interviews that offer a wide variety of global perspectives, reflecting views from the regional level alongside those of Governments, the United Nations system, non-governmental organizations, think-tanks and academia.

Supporting States to engage in the OEWG and GGE processes

As the Open-ended Working Group and the new GGE on international ICT-security get underway, States are organizing capacity-building events in New York and in capitals to raise awareness and knowledge of the normative framework developed in this area through the previous GGEs.

The online training course supports these efforts by offering training materials that have been reviewed by experts. This provides States with factual information and a greater understanding of the potential threats related to the use of ICTs, as well as the impact of these threats on international security and ways to mitigate them. UN delegations in New York already benefited from workshops based on the course materials in the lead-up to the first substantive session of the Open-ended Working Group, held from 9 to 13 September 2019.

Anyone interested in the topic of international ICT-security is warmly invited to participate in the online training course, which is available through un.org/disarmament/ict-security.

"This online training course fulfils a need for greater understanding of previous findings and recommendations, and its online format makes it readily accessible to audiences around the world."

More information:

[1] Visit un.org/disarmament/ict-security for more information on the work on developments in the field of information and telecommunications in the context of international security under the auspices of the United Nations, including relevant resolutions, reports and fact sheets.
[2] The 2015 report is available on https://undocs.org/A/70/174
[3] The Open-Ended Working Group was established by the General Assembly in resolution 73/27, available through https://undocs.org/A/RES/73/27. The new Group of Governmental Experts was mandated through resolution 73/266, available on https://undocs.org/A/RES/73/266

GFCE: Strengthening the cyber capacity building ecosystem

Since 2015, the Global Forum on Cyber Expertise (GFCE) has focused its efforts on growing the community and building a strong foundation to facilitate efficient exchange, collaboration and knowledge-sharing. Today, the GFCE functions as a thriving ecosystem that enables international cooperation in cyber capacity building (CCB) and prioritizes the practical implementation of cyber capacities. To continue accelerating forward, the GFCE shifts its attention to strengthening the GFCE ecosystem through the Working Groups, launching the CCB knowledge portal, implementing the clearing house mechanism, and progressing towards internationalization.

Written by: Manon van Tienhoven, Advisor at the GFCE Secretariat

GFCE Working Groups

The GFCE Working Groups were formed to create momentum for the implementation of global ambitions for CCB, based on the five prioritized themes identified in the 2017 Delhi Communique. The five themes are: Cyber Security Policy and Strategy; Cyber Incident Management and Critical Infrastructure Protection; Cybercrime; Cyber Security Culture and Skills; and Cyber Security Standards.

The objective of the five Working Groups was then set during the GFCE Annual Meeting 2018 in Singapore, to encourage multi-stakeholder dialogue on the implementation of CCB. As of mid-2019, around 85% of our Members and Partners are involved in these Working Groups. The Secretariat has prioritized achieving more coherence and transparency between the Working Groups and more structure within Working Groups. Three new cross-cutting groups were formed this year with the aim of introducing new roles and responsibilities to accelerate this process:

To ensure transparency and to enable the open-flow of information, the GFCE Secretariat continues to encourage the GFCE community to utilize the GFCE online workspace (on Microsoft Teams). On this platform, Working Group members can find an archive of notes and important documents pertaining to their respective Working Groups such as work plans, best practice documents, guides, etc. The online workspace also allows

2019	Cross-cutting group	Roles and Responsibilities regarding the Working Groups
New	Clearing House Advisory Group	Clearing house mechanism – advise on specification of the request for support, potential coalition and monitor the process
New	CCB Knowledge Portal Advisory Group	Translation of Working Group results mapping and deliverables translation to CCB Knowledge Portal
New	Private Sector Group	Private sector representation
Existing	GFCE Working Group Chairs	Coordination and activation of Working Group participants
Existing	GFCE Advisory Board	Civil society representation and general advisory role to the GFCE, Working Group Chairs, and Secretariat
Existing	GFCE Secretariat	Overall Working Group and cross-cutting group coordination and secretarial role

Figure 1: GFCE cross-cutting groups

members to work together outside of scheduled conference calls and meetings (for example, they may collaborate on online documents).

Launch of CCB knowledge portal

In line with the GFCE's efforts to enable and support global CCB processes, the CCB knowledge portal will be launched during the Annual Meeting 2019 in Addis Ababa, Ethiopia. The portal aims to be a neutral, globally-owned, one-stop knowledge hub that brings together information on cyber capacity building from available open-sources and input from the GFCE community and CCB knowledge community. Input from the GFCE community was collected by the Secretariat over the summer through our Questionnaire 2019, allowing Members and Partners to share information on their ongoing and completed CCB projects, knowledge products, and events. The portal, which would not be possible without the valuable contributions of the GFCE's extensive network, thus contains a wealth of unique information on products, toolkits, and activities on CCB as well as the GFCE Working Group outcomes. The portal is accessible for everyone on: www.cybilportal.org.

"The portal aims to be a neutral, globally-owned, one-stop knowledge hub that brings together information on cyber capacity building."

"Countries that require assistance may be matched to stakeholders quickly and more efficiently while providing the recipient with a clear visualization of the practical areas that they may receive support."

GFCE CLEARING HOUSE PROCESS IN PRACTICE

Sierra Leone is one of the first countries to make use of the GFCE's Clearing House process. They requested support related to several Working Groups, but chose to begin with Cyber Security Strategy development - under Working Group A. To start the process, the GFCE Secretariat's relationship manager for Sierra Leone brought together all GFCE members with current or planned projects there. This informal group discussed Sierra Leone's requirements with its government and each other. Participants coordinated plans for activities, invited all group members to join workshops and reported back to the group after country visits. The group is now expanding and open to anyone who would like to support Sierra Leone.

When Sierra Leone's Minister of Information and Communication visited London in July he was able to meet with several GFCE participants in the Clearing House group in one trip. He requested a joined-up offer of assistance from the group as his ministry develops and implements a new national cyber strategy. This joined up offer will be developed over the summer, in the margins of capacity building workshops, and finalized through a planning session at the GFCE Annual Meeting.

Implementation of the clearing house mechanism

A core aim of the GFCE is to match countries that require assistance in capacity building with resources and expertise. Through our clearing house mechanism, the GFCE is able to connect countries that require CCB assistance with multi-disciplinary stakeholders that can offer support. During this process, stakeholders working on similar CCB projects in the same region are also brought together to collaborate and coordinate on the requirements for the project.

To facilitate the clearing house mechanism, each Working Group is in the process of creating a menu of support that they can share with the wider GFCE network. With this, countries that require assistance may be matched to stakeholders quickly and more efficiently while providing the recipient with a clear visualization of the practical areas that they may receive support. The clearing house process is one of the most visible outcomes of the Working Group.

Working Group Workshops during the 2019 Annual Meeting

With a continued focus on the outcomes of the Working Groups, each group organized two 2-hour workshops on the Tuesday of the Annual Meeting 2019 in Addis Ababa.

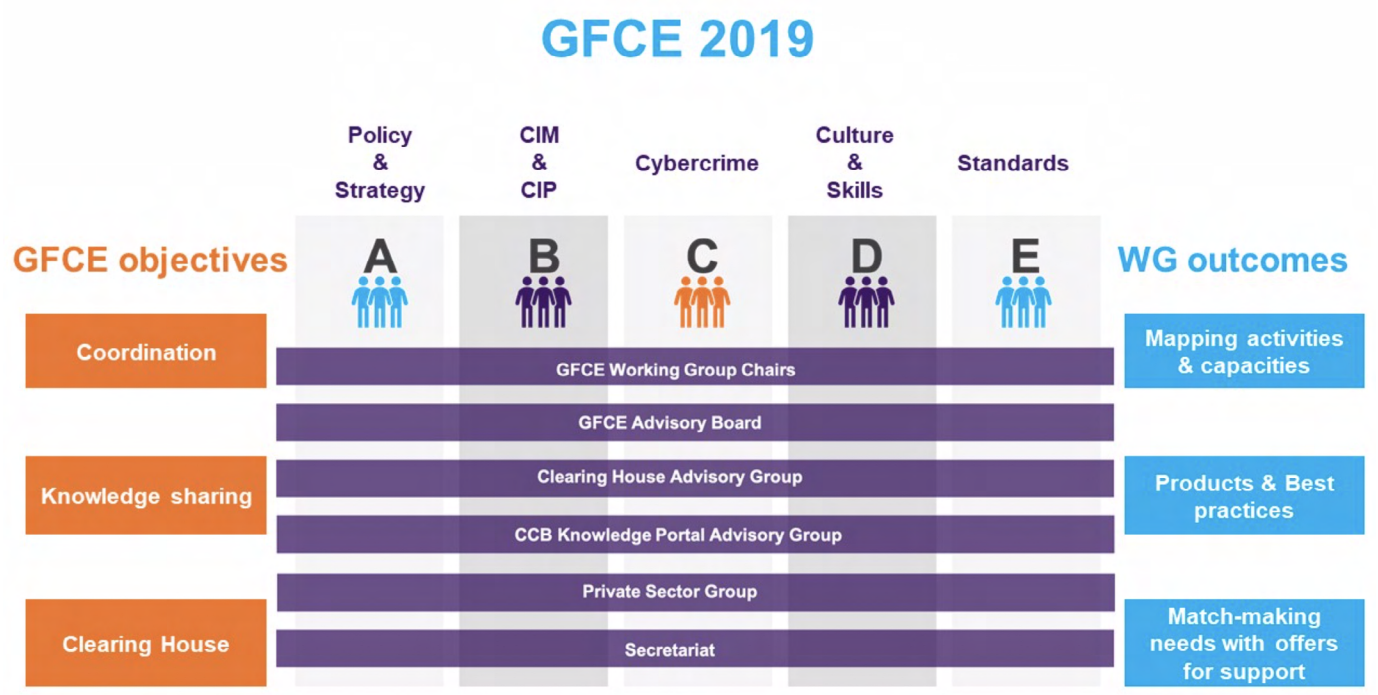


Figure 2. The GFCE ecosystem in 2019.

The workshops were designed with the beneficiary community in mind, to engage regional participants and emphasize more practical implementation of CCB. Prior to the workshops, participants were given a menu of workshops with descriptions so that they could choose to attend the ones that are most relevant or pertinent to them. The workshops covered a range of topics from National Cyber Security Strategy, IoT Security, and Critical Information Infrastructures Protection, to Cyber Security Awareness and Cybercrime. During the action-oriented workshops, participants learnt about real experiences through case studies, best practices, and interacting with experts one-on-one.

Besides these Workshops, Members and Partners also have the opportunity to share their own CCB projects and experiences at the GFCE Base Camp booths over the three days. This provided an excellent networking opportunity for the community as they could walk around the booths, ask questions, seek advice, and network with others.

As we have laid the foundation over the last four and a half years for a strong ecosystem to cooperate on CCB, the GFCE Annual Meeting 2019 is the next milestone to demonstrate its importance through its knowledge-sharing, Working Group deliverables, and the GFCE clearing house mechanism.

Meet Cybil.

The new one-stop-shop for knowledge and expertise on Cyber Capacity Building

Understand

Read recent publications to learn best practices and understand the experiences of others in their cyber capacity building journey.

Coordinate

Learn about cyber capacity building initiatives from around the world and identify relevant actors by region, theme or topic.

Improve

Build up your cyber capacity by using and implementing tools developed by the global community.

SPONSOR

GFCE Global Forum on Cyber Expertise

PORTAL GROUP

ASPI Australian Strategic Policy Institute

DiPLO

FIRST

Global Cyber Security Capacity Centre

NUPI Norwegian Institute of International Affairs

www.cybilportal.org

Got an initiative, report, event to share? Get in touch with us via the portal.

Volume 6, October 2019

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.com,
contact@thegfce.com, #thegfce

Organization of American States, www.oas.org/cyber,
cybersecutiry@oas.org, @OEA_Cyber

Disclaimer

Global Cyber Expertise Magazine

AU • EU • GFCE • OAS

contact@thegfce.com

Deadline submissions issue 7:
January 31th, 2020