Volume 5, September 2018

Global Cyber Expertise Magazine

Online Privacy and Personal Data Protection
Challenges for Africa
-page 4-

European Cybercrime Training and Education Group (ECTEG)
to serve rule of law.
-page 26-

Cyber capacity-building in the Indo-Pacific
A region marked by diversity
-page 16-

USING PUBLIC–PRIVATE PARTNERSHIP TO BUILD CYBERSECURITY CAPACITY

in Latin America and the Caribbean
-page 13-

AFRICAN UNION

GFCE Global Forum on Cyber Expertise

OAS More rights for more people

Volume 5, September 2018

Global Cyber Expertise Magazine

Editorial

Regions

Africa

America’s

Asia & Pacific

Europe

Global developments

Editorial

It is a pleasure welcoming you on behalf of the Editorial Board to this Fifth issue of Global Cyber Expertise Magazine! A joint initiative of the Global Forum on Cyber Expertise (GFCE), the African Union Commission (AUC), the European Union (EU) and, the Organization of American States (OAS).

This fifth edition presents successful experiences and initiatives from the Americas, Africa and Europe on matters related to Cyber expertise.

From the Americas, two initiatives have caught our attention. The first one is a shining example of public private partnership between the Organization of American States and Florida International University to support the development of national cybersecurity workforce. The experience is being emulated by all countries of the region to cultivate cyber talent.

The second initiative is related to the organization of Summer Bootcamps to build capacities of States in monitoring and reacting to cyber-attacks as well as enhancing cooperation and exchange of information among Computer Security Incidents Response Teams (CSIRTs) in the region.

As for Africa, the African Union Commission (AUC) recently shared an overview of the continent's guidelines on Personal Data and Privacy Protection which was prepared in collaboration with Internet Society (ISOC). The AUC also organized two workshops aiming at providing African Experts and Diplomats with the appropriate knowledge to prepare and adopt National Cybersecurity Strategies and Cyber legislations as well as the requirements for setting up and managing National CERTs/CIRTS.

The article about Europe provide an overview of the European Cybercrime Training and Education Group (ECTEG) capacity building programs on computer crime investigations. The programs target mainly enhancing the capacities and effectiveness of law enforcement authorities of the Euro zone for better serving the rule of law.

From the Asia and Pacific region, the Editorial Board selected an article with an analysis of the 2017 Cyber Maturity report wherein huge disparities on Cybersecurity readiness existed among the countries in the region.

Regarding international cooperation efforts to combat cybercrime, the Europol's European Cybercrime Center (EC3) introduced the 6th edition of the Europol-Interpol Cybercrime Conference to be held in this year Singapore which aims at expanding opportunities for cross-border partnerships in fighting cybercrime.

The Editorial Board could not miss the opportunity to mention the adoption of the Delhi Communiqué following which the GFCE community agreed on five priorities and actions to strengthen global cyber capacities and enhance multistakeholder cyber dialogues.

We hope you will enjoy the fifth edition of the Global Cyber Expertise Magazine and we look forward to receiving your feedback and comments.

On behalf of the Editorial Board,

Moctar Yedaly
Head of Information Society, African Union Commission

Online Privacy and Personal Data Protection: Challenges for Africa

In today's digital world, personal data have become the fuel that drives much of our online activities. Every day huge amounts of data are collected, stored and transmitted across the globe. More and more economic and social activities are shifting into the connected digital space, and the volume of trans-border data flows -, particularly of personal data - is increasing every year, making data protection regulations a salient issue in digital policy. For Africa, ensuring appropriate protection for the personal data of African people is the new challenge that faces many countries as the continent embraces its digital future.

Written by: Souhila Amazouz, Senior ICT Policy Officer, African Union Commission

The right to privacy in the digital age

The daily news on the way personal data is being handled and used by industry and governments, as well as reports about mass surveillance and data breaches, have combined to raise new concerns regarding information security and privacy.

While privacy is usually defined as the right of citizens to control their own personal information and decide about disclosing it or not, this right is considered a basic human right in the Universal Declaration on Human Rights as well as in the International Covenant on Civil and Political Rights. In many cases, it is also recognized in national constitutions. A legal mechanism is needed, to ensure respect for privacy through data protection. However, the enjoyment and protection of privacy is challenged and threatened by current Internet business models, many of which are based on collecting, processing and selling users' data for advertising.

The issue of online privacy has been at the center of several discussions in the UN General Assembly, which has, notably, adopted resolutions 68/167 (2013) and 69/166 (2014), as well as at the Human Rights Council, which has adopted of resolution 28/16 (2015) — known as the right to privacy in the Digital Age.

Africa's Limited Data Protection Laws

For Africa, privacy protection remains a challenge as most of its citizens' personal data are stored in digital platforms located outside the continent. The majority of African countries tend to fall behind international standards, with outdated laws and/or without specific technical measures to safeguard the protection of their populations' personal data. This makes those countries vulnerable to all kinds of data breaches.

According to the African Union Commission (AUC) report on Cybersecurity and Cybercrime trends in Africa, published in collaboration with Symantec in 2016, the African privacy and data protection landscape is still nascent. Only 17 of the 55 Members of African Union have adopted comprehensive privacy laws, regulating the collection and use of personal information namely: Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia, and Western Sahara.

And only a further subset of African countries — namely Benin, Burkina Faso, Cote D'Ivoire, Gabon, Mali, Morocco, Senegal and Tunisia — are advanced in establishing personal data governance regimes and creating their own Data Protection Authority (DPA) to sustain their citizens' trust in the use of online services.

Malabo Convention & Regional frameworks on Personal Data Protection

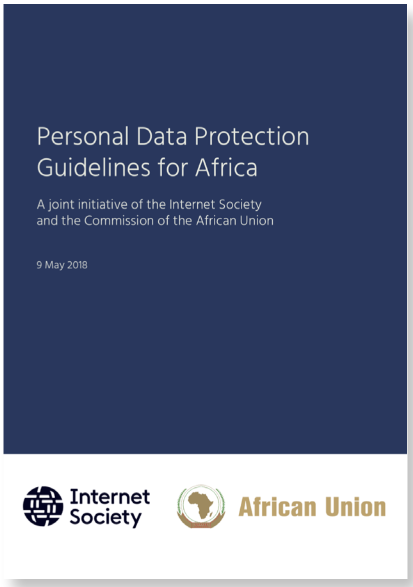
The AU 23rd Assembly of Heads of State and Government, held in Malabo on 26-27 June 2014 adopted "The African Union Convention on Cybersecurity and Personal Data Protection" also known as "The Malabo Convention," with the goals of ensuring effective privacy protection in an evolving technological environment, and establishing a regionally- and continentally-consistent response to criminal activities committed over ICT networks. The Convention aims at achieving a high level of harmonization of legal frameworks in the area of Cyber Security and Personal Data Protection in member States of the African Union.

The Malabo Convention embodies the existing commitments of African Union member States at sub-regional, regional and international levels to build a modern information society that respects the cultural values and beliefs of African nations, guarantees a high level of legal and technological security without hampering innovation, and respects fundamental online rights.

With regard to personal data protection, the objective of the Malabo Convention is to ensure a consistent level of protection for personal data in AU Member States through the creation of a uniform system of data processing at continental level, based on a common set of rules (legal and institutional frameworks) to govern the cross-border transfer of personal data and avoid the risk of divergent regulatory approaches between African countries.

The Malabo Convention is supplemented by regional data regulation frameworks, namely:

- SADC Model Law on Data Protection (2010);
- ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010);
- EAC Framework for Cyber laws (2008).



Personal Data Protection Guidelines for Africa

A joint initiative of the Internet Society and the Commission of the African Union

9 May 2018

Internet Society

African Union

Personal Data Protection Guidelines for Africa

As a new step towards developing national legislative frameworks and helping African countries transpose the provisions of the Malabo Convention into national law, the African Union Commission and Internet Society (ISOC), a global non-profit organization, jointly developed the "Personal Data Protection Guidelines for Africa", which is a detailed set of best practice guidelines on personal data protection.

The Guidelines emphasize the importance of a multi-stakeholder model for building trust in the African cyberspace and ensuring the protection of online privacy for individuals as a key factor in sustaining a productive and beneficial digital economy.

The Guidelines were framed in an African context with contributions from regional and global privacy ex-

Official Launch of the Personal Data Protection Guidelines for Africa at the Africa Internet Summit (AIS), 8 May 2018 Dakar, Senegal, Photo Courtesy: ISOC team

> **“Ensuring trust in online services and enabling cross border data flows among African countries are key factors for developping strong and sustainable digital economy.”**

perts, including industry privacy specialists, academics and civil society groups.

The guidelines also aim at empowering African citizens, as well as establishing legal certainty for all stakeholders through clear and uniform personal data protection rules for the continent.

The Guidelines propose actions at the regional, national and organizational levels, and include recommendations for governments, policy makers, citizens and other stakeholders to address the challenges related to personal data protection processes and systems in Africa.

The Guidelines set out 18 recommendations, grouped under three headings:

Two foundational principles to promote trust, privacy, and responsible use of personal data;

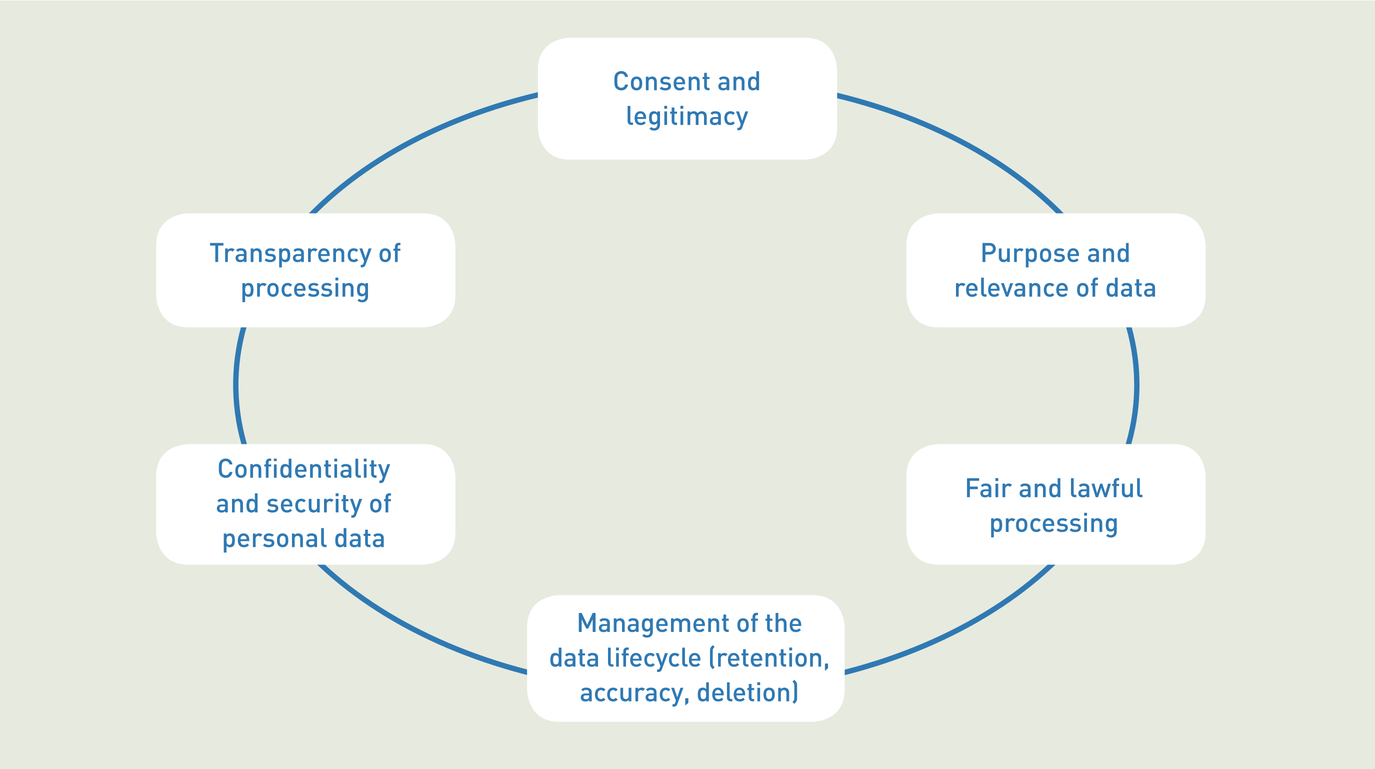
Eight recommendations for action by the following stakeholders:

- Governments and policymakers
- Data Protection Authorities (DPAs)
- Data controllers and data processors

Eight recommendations on the following themes:

- Multi-stakeholder solutions;
- Wellbeing of the digital citizen;
- Enabling and sustaining measures.

Central to the Guidelines are its principles relating to online personal data protection


Consent and legitimacy
Purpose and relevance of data
Fair and lawful processing
Management of the data lifecycle (retention, accuracy, deletion)
Confidentiality and security of personal data
Transparency of processing

Towards safer African Cyberspace

As Africa embraces its digital future, prioritizing sustainable and responsible use of personal data is critical to the development of its information society and its digital economy. The domain of privacy and personal data protection is broad and ever-changing, and the pace of change varies around the world. Africa must both influence and learn from the privacy and data protection strategies of other regions and jurisdictions, and the Guidelines represent a blueprint for doing this, through an evolving, inclusive and structured process of policy development, education, operational guidance, and best practice.

More information is available on:

1. Personal Data Protection Guidelines for Africa: https://isoc.box.com/s/h8pg316el28nmjy22slhqhn97ohy8t0g
2. African Union Convention on Cyber Security and Personal Data Protection: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
3. Cyber Crime and Cyber Security Trends in Africa: https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa

Capacity Building on Cybersecurity continues in Africa

The African Union Workshop on Cyber-Strategy, Cyber-Legislation and Setting up CERTs

Acknowledging the role of Information Communication Technologies (ICTs) and the vital importance of cybersecurity in digitalization, the African Union organs have adopted several decisions aiming at building capacity of their members States in the fields of Cyber Strategies, Cyber legislation and setting up Computer Emergency Response Teams (CERTs). In July 2018, the AU Commission will organize a five-day workshop at the African Union Headquarters to provide African experts with the necessary tools and knowledge to address Cybersecurity issues. Contributors to this capacity building exercise are not only from public and private sectors from outside the continent but also from within the continent to encourage Africa-Africa capacity building.

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

Being now very much aware that ICTs have become indispensable tools for governments, businesses, civil society and individuals, the African Union (AU) member States are striving to accelerate digitalization in the continent. This ambition demands for high connectivity of and within the continent as well as a strategy to protect and secure the needed infrastructure, the increasing amount of electronic transactions and data, which will be generated by digitalization.

This is why in their Declaration on Internet Governance adopted at the AU Summit of January 2018, the AU Heads of State and Governments reaffirmed their *"... commitment to the need for stability, for the safety of citizens and enterprises, confidentiality of online data security, through the AU Convention on Cybersecurity and Personal Data Protection, and taking into account the scalability of Africa's Internet infrastructure..".*

They pledged *"...to work together in the fight against the inappropriate use of Information and Communication Technologies in a bid to reach a consensus, in the medium term, on the best cyber security mechanisms and practices in Africa...".* They also *"...undertake to cooperate at regional and international levels to combat cybercrimes while promoting personal data protection and respecting human rights within appropriate legal frameworks.*

In so doing, the Heads of State

Capacity building workshop on Cybersecurity and Cybercrime policies for African Diplomats held on April 2018 Addis Ababa, Ethiopia, Photo courtesy: African Union Commission.

and Governments intend to preserve the integrity and reliability of the regional Internet Infrastructure as well as local users' trust and reliance on the Internet for secure electronic transactions.

This declaration from the Heads of State and Governments came in support of the 2017 Addis Ababa Declaration of Ministers in charge of Communications and ICT, which was also endorsed by the Executive Council whereby they committed themselves to:

- Collaborate with relevant African and international stakeholders on Internet Governance, Cybersecurity and Cyber Criminality;
- Ensure the follow up of the signing and ratification by Member States of the African Union Convention on Cyber-Security and Personal Data Protection and to dedicate appropriate resources for the implementation of a comprehensive Cybersecurity program including assistance to AU member States to adopt cyber strategies and Cyber legislations and to establish Computer Incident Response Team (CIRT) /CERT;

The Ministers also requested the AU Commission to undertake the necessary measures to adopt cybersecurity as a flagship project of the African Union Agenda 2063;

In 2015 within the framework of the Global Forum on Cyber Expertise (GFCE), the AU Commission in collaboration with the United States Department and Symantec surveyed 32 of the 55 AU member States, geographically and economically diverse cohort of countries to find out that:

- Only 8 of them has a National Strategy on Cybersecurity;
- Only 11 have adopted Cybercrime laws; and
- Only 13 do have National CERT.

It is against this background that the African Union Commission in cooperation with African stakeholders (Member States, RECs and Specialized Agencies) and International partners from Public (USA) and Private Sectors is organizing for AU member States a workshop on Cybersecurity Strategies, Cybersecurity legislation and setting CIRT/CERT. The Workshop will took place in Addis Ababa, Ethiopia at the AU Headquarters from 23-27 July 2018 and aims at providing AU member States with the appropriate knowledge to prepare and adopt National Cybersecurity and National Cyber legislations as well as requirements for the setting of a Computer Emergency Incident/ Response Team (CERT/CIRT).

At least three experts (a Policy Maker, a Legislator, and a Technical person) from each African country are sponsored by the AU Commission to participate in the workshop. Among the contributors we can cite MITRE, a U.S. federally funded research and development center, representatives from AU member States and RECs that will share their experiences. The workshop ran for five days: two days dedicated for Cyber Strategy, two days for Cyber Legislation and one day for the setting of CERTs.

CSIRTAmericas.org Strengthening Incident Response Capabilities in the Americas

Officially launched in October 2016, the CSIRTAmericas.org (i.e. a virtual platform for government-led CSIRTs of OAS member states) has contributed towards greater information-sharing between CSIRTs in the Americas region, a better understanding of cyber incidents and trends in the region, as well as a stronger sense of community. This interaction between member states through the CSIRTAmericas.org has contributed to the strengthening of capacities of national CSIRTs of Latin America and the Caribbean and has improved information sharing in the region as a whole.

Written by: Diego Subero, Cybersecurity Specialist, Cybersecurity Program, and Organization of American States (OAS)

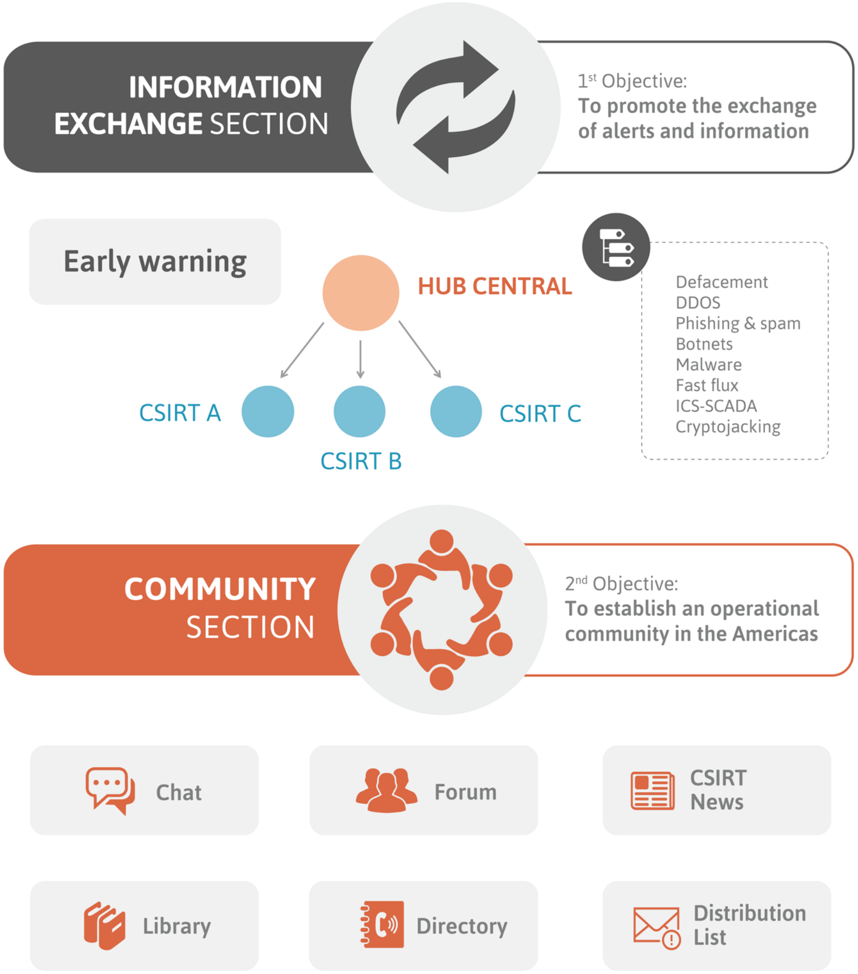
Setting the Stage: the Latin American Context

CSIRTAmericas.org was established in 2016 with two main objectives:

- To promote the exchange of alerts and information – **Information exchange section** and currently provides basic information and communication services, such as newsfeeds, a digital library, a chat, a directory of members (including specializations) and a forum discussion platform, for 18 CSIRTs now participating in the platform.
- To establish an operational community in the Americas – **Community Section**

Information Exchange

Officials connected to the platform have access to monthly sub-regional reports on cyber incidents and trends. This platform also offers specialized services in an Information exchange section, which include early warning systems and country reports on cyber incidents to 12 CSIRTs (i.e. Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, Mexico, Panama, Suriname, and Trinidad and Tobago). By receiving actionable information in real-time (24x7) and trends of cyber-attacks, national, militar and governmental CSIRTs in Latin America and the Caribbean, can better understand their threat landscape and develop an adequate preventive strategy. The ability for member states to be able to interact with each other through the CSIRTAmericas.org has also contributed to a greater cooperation between national CSIRTs of Latin America and the Caribbean.



Specialised Services

An alert system of distributed denial of service (DDoS) attacks has recently been added in the information exchange section of the platform, which allows member states almost real-time information about DDoS attacks in the country. This DDoS alert system provides members of the CSIRTAmericas.org with early warnings, as well as actionable information on various types of attacks (defacement, cryptojacking, botnets, etc), which allows governments to focus their efforts on securing networks in critical areas. The implementation of the DDoS alert system has already proven to be successful among member states. For example, one of the member states uses this information to generate daily mappings of the state of DDoS attacks in the country. With this information, the national CSIRT has been able to identify the threat context that belong to their governmental agencies and to conduct a technical analysis to identify the exact origin of the problem.

Another example of specific services can be seen during May and June 2017 when the CSIRTs in Latin America reported multiple incidents with #Wannacry and #Petya in their constituencies. In this context, CSIRTSAmericas platform was able to: (1) send notification to CSIRTs members of CSIRTAmericas.org about the attacks in Europe; (2) assist in the identification of malicious IP addresses that were the focus of WannaCry distribution in Latin American countries (which was forwarded to the CSIRTs of the countries); and (3) serve as a regional hub for the exchange of indicators of compromise (IoC), technical tools and bulletins about ransomware.

Community Section: Capacity Building

Under the auspices of CSIRTAmericas.org many capacity building activities in the region have been implemented. For example, during the "International Symposium on Cybersecurity and Response Teams" which was co-hosted by the OAS and the Forum for Incident Response and Security Teams (FIRST) in 2016, the platform was launched and members from CSIRTs from many countries in the region, particularly from South America, were able to participate. That same year, within the framework of the "Caribbean Workshop for Parliamentarians and Policymakers on Cybersecurity," representatives of the national CSIRTs from the Caribbean, such as Guyana, Jamaica, and Trinidad and Tobago were invited to attend in order to raise awareness about the importance of CSIRTs and the benefits of the hemispheric platform.

The OAS/CICTE have also organi-

CSIRTAmericas.org

Virtual platform for government-led CSIRTs of OAS member states

zed for the last three years, in partnership with the Spanish National Cybersecurity Institute (INCIBE), a Summer Bootcamp, which takes place annually in Leon, Spain. A special call for applications was created for members of the CSIRTAmericas.org. As a consequence, members of CSIRTAmericas were selected to participate in these Summer Bootcamps, where they are given either basic or advanced training in various incident response techniques, based on their level of knowledge.

In 2016, 2017 and again in 2018, the OAS/CICTE has also worked together with INCIBE for the staging of International CyberEx. This activity usually attracts over 150 participants and involves over 50 teams globally. As it relates to regional participation, in 2016 18 OAS member states, from Argentina, Bahamas, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago, Uruguay, and Venezuela participated. During the exercise, participants are exposed to cyber challenges and capture the flag exercises. These cyber exercises have allowed participants to strengthen their capacities to respond to cyber incidents, as well as to increase and improve collaboration and cooperation against such incidents. Participants were able to work in the monitoring of possible cyber-attacks, intrusion attempts and to work on their reaction capabilities in situations analogous to those that happen in the real world.

Way forward

Building capacity through the provision of information and training will not be sufficient in the long run. It is the intent of the OAS/CICTE to build a pool of incident response professionals at the national level who are able to receive and share information to better improve the cyber resilience of the Americas.

In this regard, in order to improve the exchange of information between CSIRTs in the region, continued training about threat information sharing platforms, covering topics such as basic concepts in incident response, architecture models, virtual machines installation, and common taxonomy used, have been undertaken and will continue. Another vision is the establishment of a communication protocol for the region that will include:

- **Universal taxonomy** to facilitate the exchange of information and notification of incidents among the member countries, contributing to the development of statistics on the trends of cyber incidents in the region (source CIRCL);
- **Information levels** such as categorization of the information used to take measures that support the management of cyber incidents (source ENISA);
- **Communication channels** that include the actionable information described above show how information/data will be shared according to their level by the CSIRTAmericas.org communication channels (source CSIRTAmericas.org); and
- **Dissemination levels** that adopt Traffic Light Protocol (TLP) in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience (source US-CERT).

> **"The ability for member states to be able to interact with each other through the CSIRTAmericas.org has also contributed to a greater cooperation between national CSIRTs of LAC."**

While there are different levels of maturity of CSIRTs implementation across the Americas, there is an overall effort being made to strengthen capacities. There are various common challenges, such as the sustainability of CSIRTs, the need for qualified human resources and retaining of such human resources. Despite the challenges, it is the hope of OAS/CICTE to solidify efforts currently being undertaken by the CSIRT Americas Platform to further strengthen the communication and capabilities across the Americas.

Using P3s to Build Cybersecurity Capacity in Latin America and the Caribbean

In Latin America and the Caribbean, cyber threats are rapidly outpacing the region's ability to mitigate the anticipated growth in cyber-attacks. At the same time, the region is experiencing a shortage of trained information security professionals available to answer the call and there are existing limitations in cybersecurity training and education. To that end, public private partnerships (P3s), similar to the one developed by Florida International University and the Organization of American States, can help improve the region's capacity to deal with cyber threats in the 21st century.

Written by: Brian Fonseca, Director of the Jack D. Gordon Institute for Public Policy and Research Professor at FIU's Steven J. Green School of International and Public Affairs and Randy Pestana, Assistant Director of Research at the Jack D. Gordon Institute for Public Policy and Co-Chair of Cybersecurity@FIU.

Cyber threats facing the world are growing at an alarming rate and will continue to grow well into the 21st century. In Latin America and the Caribbean, the rapid expansion of Internet penetration and interconnected devices, combined with the proliferation of cybersecurity tools and methods is rapidly outpacing the region's ability to mitigate the anticipated growth in cyber-attacks—everything from cyber-crime to cyber-terrorism. At the same time and like most regions, Latin America and the Caribbean are experiencing a shortage of trained information security professionals available to answer the call. Limitations in cybersecurity training and education remain a critical barrier to developing the region's capacity to meet the 21st century cyber threats.

Public and private sectors, through public private partnerships (P3s) should find ways to provide training and educational opportunities to support cybersecurity workforce development and reduce the skills gap. In Latin America and the Caribbean, efforts to build cybersecurity capacity should consider a whole-of-nation approach—that is government, academia, multilateral organizations, think tanks, and industry. To the end, academic institutions could serve as a connector, bringing government, industry and other stakeholders together in an effort to design and deliver a mix of short, mid, and long-term educational programming that supports moving

> "Limitations in cybersecurity training and education remain a critical barrier to developing the region's capacity to meet the 21st century cyber threats."

The first Group of participants in the Executive Certificate in Cybersecurity Leadership and Strategy programme to cultivate cyber talents in Latin America and the Caribbean.

professionals more swiftly into the workforce. However, in many academic institutions cyber-programming remains siloed and disconnected from both government and industry skills requirements.

Executive Certificate in Cybersecurity Leadership and Strategygg

In 2016, Florida International University (FIU)—through the Steven J. Green School of International and Public Affairs and College of Business—joined forces with the Organization of American States (OAS) and its Secretariat of the Inter-American Committee against Terrorism (CICTE) to support cybersecurity capacity building in Latin America and the Caribbean. That year, FIU and the OAS launched a joint Executive Certificate in Cybersecurity Leadership and Strategy to cultivate cyber talent in both the public and private sectors.

FIU and the OAS leverage critical P3s to develop curricula, deliver programming and subsidize the overall costs of the program to ensure affordability. Past iterations have included partnerships with New America, a US-based think tank and GFCE Partner organization, and key private sector partners such as Microsoft, Verizon, United Data Technologies, Trend Micro and Abacode. P3s are critical to ensuring program curriculum alignment with industry needs, and they help subsidize the costs of the program by sending experts to help deliver course content that meets academic standards. Additionally, diverse public private partnerships ensure that participants graduating from the program are exposed to a wide range of content and perspectives. The Executive Certificate in Cybersecurity Leadership and Strategy includes courses on the following:

- **Assessing the Evolving Cyber Threat Landscape —** cultivates an understanding of the current and emerging cyber threats facing the public and private sectors and examines the various types of state and non-state actors perpetuating cyber threats. It also assesses the challenges and opportunities in combatting current and emerging cyber threats.
- **Organizational Approaches to Cybersecurity —** examines the interconnectedness of policy, operations and technology as well as the risk considerations required to ensure the most effective structures, authorities, and processes for public and private organizations. It also explores the impact of policy on the private sector and how public and private sectors can work together to mitigate cyber threats.

- **Developing Strategies to Combat Cyber Threats —** provides insight into various types of strategic responses and helps establish the fundamental building blocks for a sustainable cybersecurity framework at a national level. It also provides an understanding of both offensive and defensive strategies and the cost-benefit analysis of investing in either.
- **Considerations for Effective Implementation —** promotes an understanding of the opportunities and challenges in implementing policies and strategies in both the public and private sectors and examine the keys to successful implementation of strategies. It also assesses ways to measure effective implementation to safeguard security by decreasing vulnerabilities.
- **Scenario-based Simulation —** programming includes industry-led simulations designed to bring the above curriculum together in scenario-based learning in order to stimulate critical thinking. Simulations range from responding to cyber threats to managing crisis after data breach, and bring public and private interests and solutions together.

Executive Certificate in Cybersecurity Leadership and Strategy programme to cultivate cyber talents in Latin America and the Caribbean, 2017 session.

Exporting the Model

The FIU-OAS partnership, with the support of P3s, has reached nearly 150 mid-to-senior level professionals from 18 countries in the Western Hemisphere. Previous iterations of the program were held in Miami and Washington, D.C. In 2018, FIU and the OAS began exporting the program to the region in order to make it more accessible to professionals in the area. The first regional offering was established in Argentina. In that vein, the Argentine government committed logistical support to make the program affordable, with private sector partners supporting in the delivery of the program. Programs are currently being developed for Chile and Colombia.

Using this model, FIU and its partners are expanding cyber curriculum to meet specific technical and policy-related areas, such as digital forensics, Internet of things, protecting critical infrastructure, and cybersecurity and healthcare, among others. Building networks of diverse public and private stakeholders to drive curricula development and deliver programming that adheres to rigorous academic standards is an effective means of developing the region's cybersecurity capacity.

> **"FIU and the OAS leverage critical P3s to develop curricula, deliver programming and subsidize the overall costs of the program to ensure affordability."**

Cyber capacity-building in the Indo-Pacific: a region marked by diversity

The Indo-Pacific is a region marked by great diversity. It hosts some of the world's most advanced cyber nations and industries, but at the same time some of the world's most underdeveloped ones too. This also translates into diverse approaches to cyber security. Whereas some states are preoccupied with countering cyber-enabled transnational crime and terrorism, others are concerned about state-based malicious influence, while some still need high-bandwidth internet connections. These observations can be drawn from the Cyber Maturity in the Asia-Pacific report that ASPI's International Cyber Policy Centre has been publishing annually since 2013.[1] This report has grown into a benchmark for governments, civil society and academia in the region.

Written by: Bart Hogeveen, Director of Cyber Capacity Building, ASPI's International Cyber Policy Centre

Three thrusts of capacity-building

While each capacity-building effort is unique, three broad streams of work can be identified in the Indo-Pacific region:

1. Regional capacity-building, mainly through the prism of cooperation within the framework of the Association of Southeast Asian Nations (ASEAN);
2. Country-tailored programmes focusing on ICT for development issues; and
3. Country-tailored programmes focusing on strategic policy and security issues.

Regional capacity-building

Regionally, ASEAN is the main conduit for economic growth, peace and stability in Asia, which includes non-members like Australia as 'second tier' Dialogue Partners and 'third tier' ASEAN Regional Forum (ARF) members like China, Russia, Japan and the European Union.

At their last Summit in April 2018, the ASEAN leaders again reiterated their "commitment to promoting international stability for cyberspace based on existing international law, cooperative capacity building, practical confidence building measu-

“We should not lose sight of the fact that digital technologies are also profound enablers of sustainable developments and inclusive economic growth.”

res, voluntary, and non-binding norms of responsible behaviour (…)”.[2]

Substantive progress in ASEAN or ARF has however stalled, partly due to limited knowledge and understanding of the matter across the majority of the region’s administrations. The Singaporean initiative for the ASEAN Ministerial Conference on Cybersecurity is a valuable step, but more remains to be done. Stronger education of regional policy communities seems to be an opportunity, judging from the international engagement priorities by states like Singapore, Japan and Australia.

Enabling economic and social development

Many states in the Pacific and key South-east Asian states still stand on the verge of their digital journey with landline and submarine connections being laid at this moment.[3] The bulk of the region’s communities sit at a crossroads between capturing ‘the digital dividend’ or being on the wrong side of ‘the digital divide’.[4]

When opening Australia’s pop-up Embassy in Tallinn in April 2018, Australia’s Foreign Minister Julie Bishop stated that “while we must be vigilant to risk, we should not lose sight of the fact that digital technologies are also profound enablers of sustainable development and inclusive economic growth.”[5] A great deal of cyber assistance in the region therefore targets local governments with the aim of enabling them to capitalize on digital technologies.

Strategic policy and security issues

One of the greatest achievements in cyber security across the region has been the establishment of CERT capabilities, police cybercrime units and, in some instances, military cyber capabilities. Matching these executive capabilities with solid strategic policies, legislative oversight, and protection of political, social and privacy rights is the very next capacity challenge.

This challenge will largely shape the future of cyberspace in the Indo-Pacific. While principles of an open, free, stable and secure internet are heard, there is a requirement to convince political leaders and their advisers that an open and free Internet is not at odds with national sovereignty, domestic security and fighting transnational organized crime.

ASPI’s work

ASPI’s current cyber capacity-building sits within these three endeavours: a bilateral cooperation with Indonesia (in cooperation with the Netherlands’ Clingendael Academy), an engagement with the Pacific Islands (in cooperation with Estonia’s E-Governance Academy) and initiatives at the regional level.

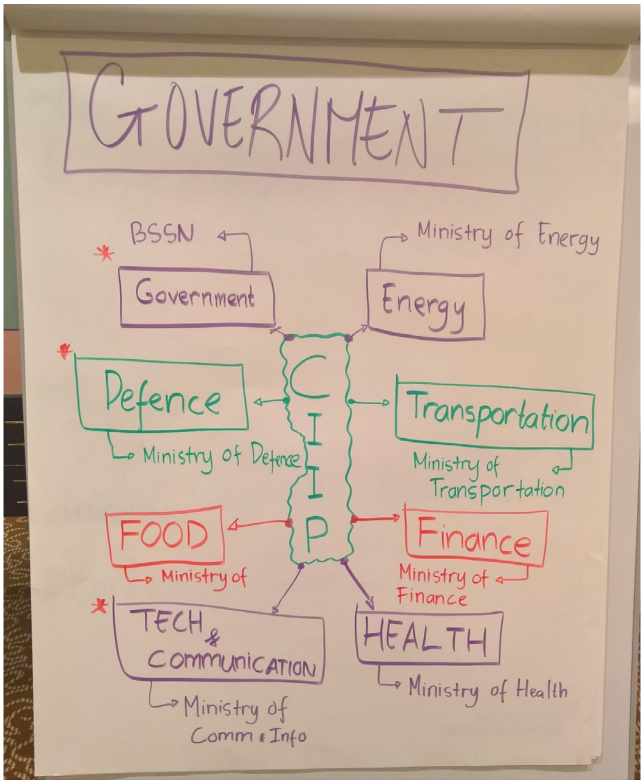
CYBERCAP Indonesia

Jointly with Indonesia, ASPI is implementing a two-year long engagement focusing on strategy and policy development and crisis response management through a series of iterative workshops. Supported by Australia’s Cyber Cooperation Programme, we have partnered with the Cyberdesk at the Indonesian Coordinating Ministry for Political, Legal and Security Affairs and the National Cyber and Crypto Agency (Bandan Siber dan Sandi Negara, BSSN).[6]

E-Governance in the Pacific

Minister Bishop recently announced her support for a project developed by ASPI and Estonia’s E-governance Academy to support e-governance capabilities in the Paci-

> “Stronger education of regional policy communities seems to be an opportunity, judging from the international engagement priorities by states like Singapore, Japan and Australia”



Mapping stakeholders in Indonesia; debriefing results, CYBERCAP workshop, January 2018 (Photo: ASPI_ICPC)

fic. The project will carefully assess the island countries’ absorption capacity to initiate, manage and sustain e-governance systems. Over a two-year period, regional activities will be organized in combination with country-specific follow-up missions.

Practical futures for cyber confidence building in the ASEAN region

In the lead-up to the Special ASEAN-Australia Summit in March 2018, ASPI coalesced fellow think tanks from across ASEAN to work collectively on practical recommendations to advance cyber confidence building in the region. These Sydney Recommendations shape the agenda for a collective effort to get a set of confidence-building measures actioned.

An agenda for Australia

ASPI’s work is not only overseas, there is also a strong domestic agenda. With Australia ranking 7th in the ITU’s Global Cybersecurity Index (2017) but 18th in the World Economic Forum’s Network Readiness Index (2016), there still remains a lot to be done at home. Shortfalls still lie in general cyber security awareness, a strategic understanding of Australia’s role in global cyber stability, consumer and business compliance with internet safety standards and crisis management readiness of federal and state governments, critical infrastructure providers and ASX 200[7] listed companies.

Lessons learned

The GFCE’s global good practices, meeting opportunities and developing knowledge network of experts and practitioners are quite instrumental to ASPI’s domestic and regional capacity-building work. ASPI is obviously not the only actor. Australia alone has multiple organisations working on regional capacity building efforts, including government agen-

Country		Weighted score
1	United States of America	90.8
2	Australia	88.0
2	Japan	88.0
4	Singapore	87.7
5	South Korea	86.8
6	New Zealand	82.0
7	Malaysia	73.2
8	China	70.2
9	Taiwan	56.9
10	India	55.8
11	Brunei	54.7
12	Indonesia	54.3
13	Thailand	54.0
14	Vietnam	53.6
15	Philippines	49.9
16	Cambodia	36.2
17	Vanuatu	35.2
18	Bangladesh	33.1
19	Laos	30.3
19	Pakistan	30.3
21	Myanmar	29.9
22	Fiji	28.5
23	Papua New Guinea	23.6
24	North Korea	17.3
25	Solomon Islands	13.8

2017 results, Cyber Maturity in the Asia Pacific report 2017 (Table: ASPI_ICPC)

cies, industry bodies, telecommunications providers, industry and technical organisations. A platform for coordination in this part of the world may prove valuable to this common effort.

Finally, our engagements greatly benefit from the fact that these take place within a framework of strategic and long-term cooperation between the donor and recipient states, in our case for instance the Indonesia Australia Cyber Dialogue.[8] This allows for a long-term engagement as well as sufficient flexibility in programming to account for shifting priorities.

More information:

[1] The 2017 edition can be found here: https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017

[2] https://aseanaustralia.pmc.gov.au/Declaration

[3] https://www.zdnet.com/article/turnbull-confirms-solomon-islands-subsea-cable/

[4] See: Pacific Regional ICT Strategic Action Plan, 2015-2020 (https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/June-Pacific-Ministerial-Meeting/Pacific_Regional_ICT_Strategic_Action_Plan_Draft_v2.docx)
[5] Global Cyber

[5] https://foreignminister.gov.au/releases/Pages/2018/jb_mr_180423a.aspx

[6] Bart Hogeveen, Is Indonesia catching up in cyberspace?, The Strategist, 14 February 2018, https://www.aspistrategist.org.au/indonesia-catching-cyberspace/

[7] Australia's benchmark stock market index which lists the top 200 traded companies.

[8] Australia-Indonesia Cyber Dialogue, http://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australia-indonesia-cyber-policy-dialogue.aspx

Singapore: a cyber-gateway to Southeast Asia

An interview with David Koh, Commissioner of Cybersecurity for Singapore and Chief Executive of the Cyber Security Agency of Singapore

David Koh receiving the inaugural Billington Cybersecurity International Leadership Award at the 3rd Annual Billington International Cybersecurity Summit in March 2018, in recognition of Singapore's contributions to international and regional cybersecurity cooperation. Credit: Cyber Security Agency of Singapore

David Koh has played an essential role and made significant contributions to enhance cybersecurity in Singapore, by providing strategic direction and leadership of the Cyber Security Agency of Singapore, the successful launch of Singapore's Cybersecurity Strategy and Singapore's comprehensive cybersecurity legislation.

Q: The Cyber Security Agency of Singapore was established on 1 April 2015. Could you elaborate on the origin of the agency?

Prior to the formation of the Cyber Security Agency of Singapore (CSA), there were different government agencies that were responsible for different aspects of cybersecurity. For instance, cybersecurity industry development was undertaken by the former Infocomm Development Authority of Singapore (IDA), while cyber incident response and crisis management was covered by a unit under the Ministry of Home Affairs.

The decision was taken to bring

these efforts under a single authority as the cybersecurity landscape became increasingly complex – driven by the proliferation of threat actors and the evolution of innovative techniques to bypass cyber defences. As such, CSA was established in 2015 to have centralised oversight of the state of cybersecurity preparedness at the national level, and to better engage with the private sector. CSA oversees cybersecurity strategy and policy for Singapore, where cybersecurity is viewed as a key enabler for the digitalisation of our nation.

Q: Singapore ranked first with the greatest commitment to cybersecurity on the ITU Global Cybersecurity Index 2017. Why is cybersecurity a high priority for Singapore and how can Singapore maintain its leader's role in the region while ensuring a safe and resilient cyberspace?

The more digitalised and connected the lifeblood of our economy, the more important it becomes to secure our systems in cyberspace. As a gateway to Southeast Asia and the larger Asia-Pacific region, Singapore is a major banking, telecommunications, aviation and maritime hub. A significant proportion of the world's financial transactions, telecoms, air traffic, and freight flows through our borders. Cyber-attacks that impact such supranational infrastructure could have spill-over effects on systems beyond our shores.

The financial cost of cyber-attacks can be high, but indirect costs, such as the loss of trust, can be even higher. This is especially relevant for Singapore, whose brand name is often associated with trustworthiness and efficiency. Cybersecurity is thus essential, even existential, to Singapore's continued prosperity.

Singapore plays a leading role in the region by first getting our own house in order. Besides setting up a central national agency for cybersecurity and launching a national cybersecurity strategy, we have also worked to pass a comprehensive Cybersecurity Act earlier this year. The Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore,

Regionally, Singapore has been active in moving the conversation on cybersecurity forward. Under Singapore's Chairmanship of ASEAN this year, ASEAN Leaders issued a first-ever ASEAN Leaders' Statement on Cybersecurity Cooperation. This document highlights the need to foster closer regional cybersecurity coordination across the various ASEAN sectorals. It also tasks relevant Ministers from all ASEAN countries to make progress on identifying a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting and implementing.

The broader Singapore International Cyber Week brings together leaders from government, industry, NGOs and academia from around the world to exchange ideas and forge partnerships to further cybersecurity cooperation. Last year's SICW attracted over 7,000 participants from close to 50 countries. This year's SICW will be held on 18-20 September 2018.

> **"The financial cost of cyber-attacks can be high, but indirect costs, such as the loss of trust, can be even higher."**

Q: The theme of the Singapore International Cyber Week 2018 is 'Forging a Trusted and Open Cyberspace'. In your opinion, what elements are needed in forging a trusted and open cyberspace? And how can countries in your region or globally learn from the practices during the SICW?

There are two parts to the SICW theme – trust and openness. First, Singapore recognises that cyberspace can be an enabler of a vibrant digital economy and improved living standards. But we also recognise the need for some basic rules of the road to guide responsible State behaviour in cyberspace. This is why Singapore has consistently been supportive of efforts by the international community to develop **a clear set of practical norms** to help cultivate a degree of predictability and assurance to State

> “I would be delighted to see outcomes achieved through a single region like ASEAN be multiplied and made more effective through inter-regional dialogue and cooperation on cybersecurity issues.”

behaviour in the use of cyberspace.

Secondly, we recognise that norms need to be complemented with **effective implementation of confidence building measures** so that we build a strong culture of trust that will encourage adherence to norms, reduce the risk of misperception and conflict, and foster closer regional cooperation.

Thirdly, we need **robust and targeted capacity building** across the region so that every country is better able to ensure its domestic cybersecurity and contribute to regional cybersecurity, including the means to meet its obligations under those norms. When countries are better organised and have sound strategies and legislation, general confidence of States in being connected to and open with one another increases. These three elements – well-defined, practical voluntary norms, robust confidence building measures and coordinated capacity building – work to reinforce one another in a virtuous cycle. At the end of the day, without capacity building, policy decisions will exist only on paper.

This leads me to the second part – openness. There is no effective way to do any of the above without **being inclusive and open to engagement with other relevant stakeholders.** Governments are not the only players. If industry, academia and NGOs are left out of the conversation, the efforts will be lop-sided and ill-informed. Just as we did with the development of our domestic cybersecurity legislation, there needs to be active consultations and involvement of all relevant stakeholders to ensure that diverse views are taken into consideration so that our collective effort to enhance cybersecurity are well-rounded and no blind spot is neglected.

Q: Singapore aims to be an example for the region in cyber capacity building. What are your aspirations for Singapore and the ASEAN region for the next decade?

A decade is a long time, especially in a rapidly evolving field such as cyber. Over the past two years, there has already been exponential progress in the ASEAN region, as a few of the countries move to establish dedicated national cybersecurity agencies, develop legislation and launch national cybersecurity strategies. At the moment, we are very much focused on developing and implementing a rigorous programme to complement existing ASEAN efforts in building up cybersecurity capacity for ASEAN Member States across both the technical and policy aspects, under the auspices of Singapore’s SGD 10 million ASEAN Cyber Capacity Programme (ACCP).

I look forward to working with our fellow ASEAN Member States and ASEAN Dialogue Partners to identify ways to move ahead on the clear agenda set by ASEAN Leaders through their Leaders’ Statement, including practical recommendations for better coordination of regional discussions and initiatives, as well as a concrete list of practical norms that the region can adopt to guide responsible behaviour in cyberspace.

Further ahead, I would be delighted to see outcomes achieved through a single region like ASEAN be multiplied and made more effective through inter-regional dialogue and cooperation on cybersecurity issues. Dialogues between regional groupings would allow regions to compare notes, exchange best practices and even consider joint capacity building programmes where appropriate. More importantly, such dialogues would allow us to build consensus around issues such as cyber norms, confidence building measures and the applicability of international law to cyberspace – in support of global discussions such as those at the United Nations.

European Cybercrime Training and Education Group (ECTEG): To serve rule of law

Computer crime law enforcement training needs to be improved by integrating an educational approach and a more forensic analysis to address specific issues raised by electronic evidence and the evolution of technology.

Written by: Yves Vandermeer, ECTEG chair person

IT forensics challenging rule of law

When dealing with computer forensics and electronic evidences, so-called accurate technical reporting often leads to some opacity due to complex concepts and lack of vulgarisation. If several sources may be identified to explain why a feeling of obfuscation is perceived by the unspecialised judicial actors, the result is sometimes a clear denial of rule of law fundamentals: right for fair trial by equality of arms guarantee and well-reasoned judgements.

Clarity and associated vulgarisation of findings and proposed interpretation are indispensable to allow individuals and magistrates to understand the nature of the presented evidence, relationship with the investigated or judged criminal offense and to challenge it in a healthy debate.

Opacity identified factors

Over 15 years as computer forensics specialised police officer, and involvement in international projects on computer forensics investigations and trainings, lead me to consider at least the following factors:

- Technical reports are often lacking explanation on how traces may be linked with case facts. Without any technical knowledge, the accused, lawyer, complainant, prosecutor, judge, members of the jury aren't able to fully understand and decide about traces relevance.
- Inexistent or insufficient cross-checks of findings result in tool-based evidence despite the risk of software weaknesses and limitations.
- Specialised forensics practitioners are reticent to produce an interpretation of traces. Interpretation, however, is often needed to understand how different traces correlate and contribute to rebuilding the modus operandi, creating an unwished gap between reality and judiciary reality.
- Judicial actors are reluctant to dig into new technology traces,

> **“ECTEG is an International Non-Profit Association with members representing LEA, Academia and EU bodies supported by an advisory board with representatives from Europol-EC and CEPOL.”**

often being observable without ad-hoc software tools and computer science knowledge.

Looking forward to a soundly based approach

The raise of new technologies during the last twenty years forced law enforcement, forensic institutes and the judiciary system in general to build experience-based knowledge. Tools then developed by the industry quickly became self-assessed. Evolution of technology, like introduction of new file systems features, encryption and computer networks technologies pushed the practitioners to focus on workload efficiency, resting on software tools' supposed accuracy and industry investments in research and development. The computer forensics eco-system then being mostly based on the *“one-eyed are kings in the kingdom of blinds”* paradigm.

Fortunately, something grew in this eco-system, fed by rightful aspiration of pioneers from all sides, challenging established software centric approaches and demanding for an improved understanding and reassessment of the whole process.

In the past few years, with support from EU Commission, law enforcement and universities started to build a more professional approach, intended to better serve the rule of law and encounter basic criteria of evidence admissibility: authenticity, completeness, reliability, believability, proportionality. Rethinking the former “tool-based training” to “educate to handle a forensic analysis” approach wasn't easy and initially faced doubts expressed from people afraid to move to process changes.

Since 2001 ECTEG creates and maintains several course packages, made available free of charge to Law Enforcement Agencies involved in the organisation of a course. **ECTEG is an International Non-Profit Association with members representing LEA, Academia and EU bodies, supported by an advisory board with representatives from Europol-EC and CEPOL.** Activities aim to address the needs for new and up-to-date training packages within the frame of a governance model.

This unique collaboration, where experts work together to address LEA needs on computer forensics and cybercrime topics, contributed to the new approach, more in an education process instead of a sequence of tools centric trainings.

When tools were the topic, trained practitioners followed a linear analysis path incompatible with complex and ever evolving technologies including anti-forensics features. Education improves practitioners' knowledge on “how the things are working”, their capability to; cross-check evidence by using several tools, thwart criminals by deploying counter measures, describe findings relevant in the crime case context and finally their capability to formulate possible interpretations with all transparency. Well-educated practitioners give better advice about expensive tools acquisition which could be mixed with open source tools, when possible. When challenged in front of court, they contribute to a fact and evidence-based debate with clear and understandable technical statements.

Software tools, however, are still an essential part of technical courses but considered as a means to acquire practical knowledge.

Recently ECTEG delivered new course packages on Malware Analysis, Live Data computer forensics and Forensic scripting using Python. With quality and synergies as keywords for all activities, ECTEG members started new courses development to address needs from the first responders profile to experts from LEA involved in cyberattacks investigations.

European Cybercrime Training and Education Group, an International Non-Profit Association with members representing Law Enforcement Agencies, Academia and EU bodies.

> **“With clear objectives supported by affordable standards and course materials, law enforcement will be able to fulfil their tasks in a way expected from all judicial actors: serving the rule of law.”**

Education part of a coherent capacity building effort

Currently not one computer forensic tool is certified and even though some countries put efforts in accreditation of trained practitioners, expertise isn’t validated by an ad-hoc certification process. If some certification frameworks exist, they are tightly linked to commercial tools or training activities instead of profile skills and competences as elaborated in the *Training Competency Framework* created in 2015 by Europol, CEPOL, Eurojust, EJTN and ECTEG, recently validated by the EUCTF.

Certifications

The TOT project, run by Universidad Autónoma de Madrid (Spain), delivered in spring 2017 a set of processes on how to develop profiles based cybercrime certifications. Based on the provided processes, ECTEG started to develop certification packages for several profiles. This project called *Global Cybercrime Certification* will deliver certification packages, piloted and validated by Europol, CEPOL, EJTN and universities involved as first accredited certification bodies.

Experts and trainers

Such challenges cannot be addressed without highly qualified human resources. Experts and trainers should; captivate and motivate course attendees, transfer their knowledge to younger ones and contribute to courses and standards development. This requires law enforcement experts with a high level of in-depth knowledge and years of investigation experience.

Nowadays, all organisations organising IT crime trainings on international or national level are struggling with a lack of expert trainers. National police management realise that working together saves resources. But they face a no-nonsense issue: the best experts are predominantly needed to support investigation cases.

Scalable efforts from national police units involving experts into international cooperation projects, combined with a coherent strategy and support from the EU commission would address this issue efficiently.

Conclusion

With clear aims supported by affordable standards and course materials, law enforcement will be able to fulfil their tasks in a way expected from all judicial actors: serving the rule of law.

Europol-INTERPOL Cybercrime Conference: A joint cooperation that gets better with age

The borderless nature of cybercrime and especially the ease with which criminal activity can take place at any time, in any location, makes it a crime that requires more international coordination and cooperation than any other. As a response, in January 2013 Europol set up the European Cybercrime Centre (EC3) as the focal point in the EU's fight against cybercrime, to work closely together with INTERPOL member countries through its Global Complex for Innovation (IGCI) in Singapore. The goal is to strengthen the support available to law enforcement authorities worldwide, and to ensure a stronger and more pro-active policing of cyberspace. As a tangible result of this valuable partnership, the 6th edition of the Europol-INTERPOL Cybercrime Conference takes places during the Singapore International Cyber Week 2018 (SICW). In just a few years, this event has become a leading name within the global community of cybercrime fighters.

Written by: María Sánchez – Prevention & Communication Officer, Europol's European Cybercrime Centre (EC3)

It was early 2013 when the former Europol and INTERPOL top managers (Rob Wainwright and Ronald K. Noble) reviewed the cooperation between their two agencies and discussed the crime threats they were at that time combating. High on the agenda was cybercrime, with the two chiefs reviewing progress in Europol's EC3 (up and running for a few months then) and INTERPOL's Global Complex for Innovation (which would open its new doors the year after). Both chiefs committed to work in a complementary manner in the response to the growing threat of cybercrime, whose nature, impact and scale posed and keeps posing a considerable challenge to law enforcement.

To ensure the most efficient and dynamic cooperation between cybercrime teams across the world, Europol and INTERPOL agreed to bring worldwide experts together once a year at a joint Cybercrime Conference, initiating a new and innovative concept to be hosted in alternate years in The Hague and Singapore. Under the theme *'How can we cooperate better?'*, the first edition, organised in September 2013 at Europol headquarters, was attended by over 250 professionals from 42 countries

EUROPOL-INTERPOL Cybercrime Conference

representing more than 80 different organisations. These figures rose to a record participation of 420 attendees to the latest event in 2017, which shows the consolidation and importance of the conference in the global cyber agenda.

A practical event with results-oriented nature

The primary goal of each new edition is to look at ways in which all involved sectors can work closer together to maximise cooperation within and outside of their respective areas of expertise. Specific commitments are taken every year in this regard, with an open invitation for partners to join. Europol and INTERPOL agreed on specific steps in the fight against ransomware in their 2017 joint closing statement. These include the following. The first step is a coordinated law enforcement approach to address Dark Web threats. Then, they wish to identify approaches to tackle the threat of cybercrime in a more pro-active and efficient manner. They also aim to continue to focus on coordinated prevention and awareness initiatives to increase baseline cybersecurity. Finally, the two agencies want to nurture the skills and expertise needed to ensure a safer cyberspace.

A multitude of relevant topics has been thoroughly selected to compile every year's agenda. These could range from Internet of Things security and resilience, to solutions for attribution, ransomware, bullet-proof hosting, the criminal abuse of encryption and anonymization, DNS abuse and to the financial aspects of cybercrime. During the Global Con-

> **“Cybercrime remains a real and innovative threat. It evolves over the years and so does the cooperation between Europol and INTERPOL to look at ways of combating the criminals together. The joint Cybercrime Conference is a yearly milestone to share best practices, operational successes and build up relationships.”**
>
> Steven Wilson, head of Europol’s EC3

EUROPOL-INTERPOL Cybercrime Conference

ference on Cyber Security 2015, held in The Hague, several new initiatives were launched. As a consequence, two of them of particular interest for policing were presented at the Europol-INTERPOL Cybercrime Conference 2015: the Global Forum on Cyber Expertise (GFCE) and the discussions on improving international cooperation in cybercrime. This marked the beginning of a fruitful cooperation on cyber capacity building matters, which has been continued both inside and outside the margins of the conference.

6th edition on the making

Both agencies are fully engaging in the conference, happening in Singapore from 18 to 20 September 2018. The conference will focus on the following main areas:

- Cyber Criminals and their Networks;
- Strategies to counter cybercrime;
- Global response to critical cyber threats;
- Policing Cybercrime – the role of intelligence.

Always under renovation, this year our joint conference comes with the added value of taking place during the Singapore International Cyber Week, providing extra opportunities to discuss, network, strategise and form cross-border partnerships in the cybersecurity space.

We welcome all participants from law enforcement, private sector, academia, government and NGO representatives. In preventing, disrupting and combating cybercrime, together we have a challenging task ahead of us, so let’s get to work and remain actively united for a safer cyber space.

GFCE: Towards Global Cyber Capacity Building Implementation

The Global Forum on Cyber Expertise (GFCE) was launched in 2015, during which time it was anticipated that the GFCE would develop into a global, informal and coordinating platform for Cyber Capacity Building. Nowadays the GFCE functions as an ecosystem that enables efficient international cooperation in building cyber capacities.

Written by: Manon van Tienhoven, Advisor, GFCE Secretariat

Endorsing the Delhi Communiqué

During the 2017 Global Conference on Cyberspace the GFCE community endorsed the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building. The Delhi Communiqué prioritizes five themes in cyber capacity building and calls for action to jointly strengthen global cyber capacities. This endorsement is essential in coordinating global efforts and to encourage the multistakeholder dialogue on the implementation of cyber capacity building.

The first step towards concrete action is in the form of GFCE Working Groups based on the five prioritized themes:

- Working Group A: Cyber Security Policy and Strategy;
- Working Group B: Cyber Incident Management and Critical Infrastructure Protection;
- Working Group C: Cybercrime;
- Working Group D: Cyber Security Culture and Skills;
- Working Group E: Cyber Security Standards.

Multistakeholder dialogue on CCB implementation

The Working Groups will bring together the GFCE global community to encourage and enhance the multistakeholder dialogue on cyber capacity building. This will also strengthen international cooperation by developing a common focus, enabling efficient use of available resources and avoiding duplication of efforts. In line with the Delhi Communique, the mandate of the Working Groups is to effectively respond to the needs and expertise available on the specific themes to encourage and enhance the multistakeholder dialogue on the implementation of cyber capacity building activities (as demonstrated in Figure 1).

Broadening the CCB knowledge community

Since the launch of the GFCE in 2015, the focus has been on expanding the member network (countries, international organizations and priva-

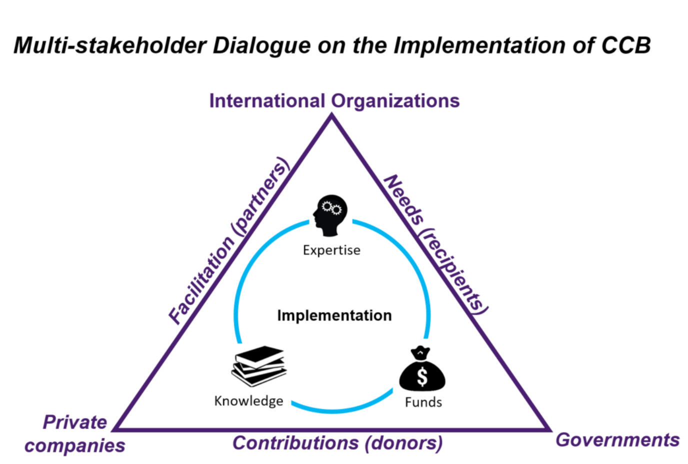


Figure 1: Multistakeholder dialogue on CCB implementation

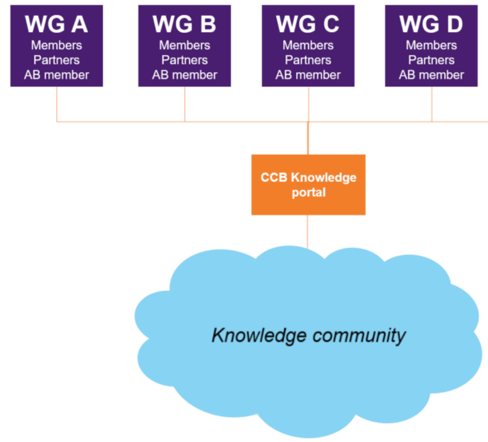


Figure 2: GFCE Working Group process and the link with the knowledge community

te companies). The members have the resources and the ambitions on cyber capacity building. Through the GFCE network, access is provided to the available tools and expertise necessary for the implementation of cyber capacity building. Since the practical knowledge tools and expertise in this field are often not available and fragmented globally, a strong knowledge network is essential for the contribution of the practical knowledge tools and implementation expertise to the GFCE network. The GFCE is developing a CCB knowledge community (f.e. academia, think tanks and implementing organizations) which has practical knowledge tools and implementation expertise on various themes of cyber capacity building. Some of these knowledge organizations will participate as formal GFCE partners within the Working Groups. As a result, a neutral and open knowledge portal will be developed that will elevate the GFCE community and the CCB knowledge community to the next level. The CCB knowledge portal is the linking pin between the knowledge community and the GFCE community (as demonstrated in Figure 2). The portal will be open to all knowledge organizations who can provide and contribute relevant content on CCB implementation, these stakeholders will form the broader CCB knowledge community.

Sharing outcomes globally

The Working Groups will encompass existing and planned efforts of the GFCE community in building the global cyber capacities along the line of the five prioritized themes with the focus on 2018 and 2019. The first step is to provide an overview of the global state of the needs and ongoing projects and to involve the relevant and necessary stakeholders. This will be a stepping stone towards connecting the needs with existing and potential new activities of the GFCE community. Since the GFCE community has different needs and expertise, each Working Group will focus on different outcomes depending on the respective theme. Possible outcomes of the groups can be:

- Joining existing activities / sharing results, etc.
- Identifying new activities (filling in the gaps);
- Joining efforts where there is a mutual interest;
- Awareness raising activities;
- Adoption / development of implementation tools/instruments.

During the 2018 GFCE Annual Meeting in Singapore, the Working Groups will provide a first progress report that is presented by the Chair of each group wherein they will present the community's ambitions on CCB implementation. Therefore, this Annual Meeting reflects the positioning of the GFCE as the facilitating and coordinating platform on knowledge and expertise sharing for the implementation of cyber capacity building.

GFCE Triple-I: Improve Justified Trust in the Internet, together

Triple-I (the Internet Infrastructure Initiative) is a GFCE initiative with the objective to enhance trust in Internet and email through open Internet security standards and by sharing good practices on a global level. The GFCE Triple-I aims to organize capacity building workshops in different regions with the support of the GFCE community, as well as from members of the global "technical community". The objective is to facilitate awareness raising and capacity building in the region, and thus setting local priorities and stimulate local actions.

Written by: Maarten Botterman, GFCE Triple-I Facilitator

On Monday 7 May 2018, during the Africa Internet Summit 2018, AfricaCERT and AfriNIC hosted the GFCE Triple-I Internet Infrastructure Security Day. Together with over fifty participants, from various stakeholders groups, different ways for a more trusted use of Internet and email in the African region were explored. Participants in this workshop were regional Internet stakeholder groups, including the government, business and technical community who all contributed in finding solutions to strengthen an open end-to-end Internet. This is the first of a series of workshops that will be organized globally for the upcoming year.

Improving justified trust in the Internet

The workshop was organized in a U-shape setting to allow open discussions and stimulate involvement from all participants.

Nii Quaynor opened the workshop with a clear call for getting involved – and support each other in steering change. Nii played an important role in the introduction and development of the Internet throughout Africa and is therefore recognized as an *Internet Hall of Fame inductee*. He encouraged the participants to work together on development and implementation of cyber capacity activities to improve trust in the Internet in the African continent.

The workshop started with Alain Aina (WACREN) and Olaf Kolkman (ISOC) debating the use and importance of Open Internet Standards such as DNSSEC, TLS, DANE, DMARC, DKIM, SPF and IPv6, followed by strong participation from the floor. A key take-away from the meeting was the importance of implementing a state-of-the-art Open Internet Standard, al-

Olaf Kolkman and Alain Aina talking about Open Internet Standards during Triple-I workshop in Dakar, Photo courtesy: Maarten Botterman

> **“During the first GFCE Triple-I workshop, participants explored the current state of global resources and expressed their interest to support local activities and implement good practices.”**

ready available today. The majority of the participants seem to settle for the status quo rather than setting up new and improved systems and services. This has led to vulnerabilities that are avoidable – and solving these requires action by all.

Inspiration from Good Practice

In line with sharing good practices, experiences on how to mitigate Internet and email vulnerabilities were discussed. Ms. Octavia de Weerdt from NBIP.NL shared the good practices by discussing the NBIP on-demand DDoS security for small Internet providers, medium-sized and larger businesses, and VoIP providers that helps to put up a powerful joint resistance against DDoS attacks.

Marcus Adomey (AfricaCERT) stressed on the importance of Incident and called for a coordinated approach.

Michuki Mwangi from ISOC talked about Mutually Agreed Norms of Routing Security (MANRS) and the need for a culture of collective responsibility whereby best practices on routing security are shared among the stakeholders.

Kevin G. Chege from ISOC discussed the growing impact of the Internet of Things on the Internet, recommending the adoption of the OTA IoT Trust Framework as a guideline for safer IoT implementation. Jesse Sowell explained the work of the Transnational Anti-Abuse Working Group Development (M3AAWG) in terms of good practice experiences in detecting and fighting abuse on the Internet.

Finally, Yurie Ito explained that Cyber green provides recommendations to improve cyber health by informing Computer Security Incident Response Teams (CSIRT) on the most important risks and helps them to adapt the right security measures.

Participants to the Triple-I workshop gathering around the core action ideas in the "market place", Photo Courtesy: Maarten Botterman

Market place for actions to improve trust

Subsequently, participants explored three possible actions that culminated from the morning discussions and provided plausible solutions to the main question raised: *"What to do together to improve justified trust in using the Internet and email in the region"*.

As such, participants deliberated on: (1) stakeholders' actions for stimulating the uptake of MANRS (proposed by Michuki Mwangi); (2) activities on enhancing sustainability of IoT (proposed by Kevin Chege); and (3) support to setting up an African chapter of M3AAWG (proposed by Jesse Sowell). In order to take action on the latter, participants agreed to keep the dialogue going, and focus on identifying specific regional issues and setting up an exchange of threat warnings with the main M3AAWG center.

"A key take-away from the meeting was the importance of implementing a state-of-the-art Open Internet Standards, already available today."

Conclusions

The good practices presented on IoT security, MANRS, M3AAWG, CyberGreen, CERT activities and the NIBP approach to fight DDoS attacks were relatively new concepts for the majority of participants. During this first GFCE Triple-I workshop, participants explored the current state of global resources and expressed their interests to support local activities and implement good practices.

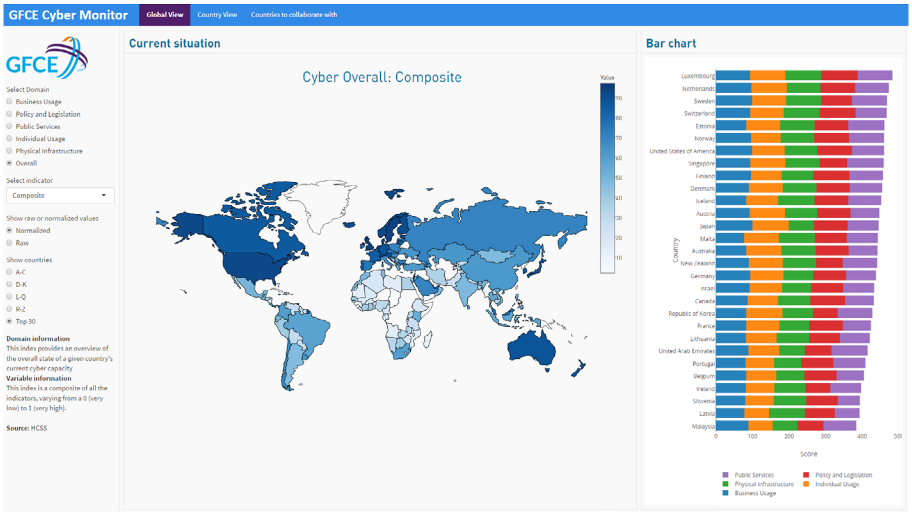
More information:

This was the first of a series of Triple I Workshops that will be organised in different regions globally. The various contributors to this workshop – co-organisers, presenters and participants are highly appreciated and valued. The results and outcomes will be shared on the Triple-I event website in due time. Similar workshops will be held this year and are currently being developed. For the full report and more information on Triple-I, please visit www.thegfce.com. Organisations that are interested, can contact the GFCE Triple-I facilitator Maarten Botterman at: maarten@gnksconsult.com.

GFCE Cyber Monitor

In joint effort with the Hague Centre for Strategic Studies, the GFCE has provided an overview of the overall state of a given country's current cyber capacity. The GFCE Cyber Monitor considers the following variables; Business Usage; Policy and Legislation; Public Services; Individual Usage; Physical Infrastructure. Data was gathered using open sources.

The GFCE Cyber Monitor is available on the GFCE website: www.thegfce.com



GFCE Cyber Monitor | Global View | Country View | Countries to collaborate with

Select Domain
○ Business Usage
○ Policy and Legislation
○ Public Services
○ Individual Usage
○ Physical Infrastructure
● Overall

Select indicator
Composite ▾

Show raw or normalized values
● Normalized
○ Raw

Show countries
○ A-C
○ D-K
○ L-Q
○ R-Z
● Top 30

Domain information
This index provides an overview of the overall state of a given country's current cyber capacity
Variable information
This index is a composite of all the indicators, varying from a 0 (very low) to 1 (very high).

Source: HCSS

CYBERSECURITY CAPACITY PORTAL

A Global Resource for Cybersecurity Capacity Building

The publically-available online platform of the Global Cyber Security Capacity Centre is designed to be a central point of reference to those responsible for cybersecurity capacity building across the world. It provides up-to-date curated content on new developments and good practices in capacity building. It also includes — in partnership with the GFCE — an inventory of current international and regional capacity-building programmes and projects around the world that may be leveraged to expedite the impact and efficiency of cybersecurity capacity building.

Visit: www.sbs.ox.ac.uk/cybersecurity-capacity

Global Cyber Security Capacity Centre

SAID BUSINESS SCHOOL | OXFORD MARTIN SCHOOL | UNIVERSITY OF OXFORD

For more information: cybercapacity@oxfordmartin.ox.ac.uk | www.oxfordmartin.ox.ac.uk/cybersecurity

Volume 5, September 2018
Global Cyber Expertise Magazine

Colophon

Editorial board
Manon van Tienhoven (GFCE)
Belisario Contreras (OAS)
Panagiota-Nayia Barmpaliou (EU)
Souhila Amazouz (AU)

Guest editors
Sophia Nesri
Moctar Yedaly
Diego Subero
Brian Fonseca
Randy Pestana
Bart Hogeveen
David Koh
María Sánchez
Yves Vandermeer
Maarten Botterman

Artwork & design
Ivonne Vivanco (OAS)

Chief editor (rotating)
Souhila Amazouz (AUC)

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

The opinions expressed in this publication are solely those of the authors and do not necessarily reflect the views of the AU, EU, GFCE or OAS or the countries they comprise of.

Global Cyber Expertise Magazine

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

Deadline submissions issue 6:
March 1st, 2019