

Global Cyber Expertise Magazine

Cyber Aspirations in West-Africa
ECOWAS Cyber
Strategy Workshop
-page 7-

Cyber Challenges in LAC
Bridging the technical
skills gap
-page 11-

Australia's International Cyber Strategy
Global in perspective,
regional in focus
-page 21-

GFCE: PUTTING PRINCIPLES INTO PRACTICE

Moving forward
-page 25-



OAS More rights
for more people

Editorial

Regions

Africa

- 4 Capacity Building is the Key to Fight Against Cybercrime: The Mauritian Perspective
- 7 U.S. Department of State and ECOWAS Partner to Promote Cyber Due Diligence in West Africa

America's

- 11 Addressing the Skills Gap in Digital Security
- 14 Brief history of the extinct National Computer Security Network of Mexican Universities

Asia & Pacific

- 17 UNODC: Countering cybercrime in Southeast Asia and beyond
- 21 Australia's inaugural International Cyber Engagement Strategy: global in perspective, regional in focus

Global developments

- 25 GFCE: Moving forward
- 28 Developing the building blocks for a global Incident Response Capability
- 31 GFCE and Meridian: Combining forces on CIIP

Editorial



Welcome to the fourth edition of the Global Cyber Expertise Magazine! We are proud to present this edition at the Global Conference on CyberSpace 2017 in New Delhi.

The Global Cyber Expertise Magazine is a joint initiative of the African Union, the European Union, the Organization of American States and the Global Forum on Cyber Expertise, this magazine is aimed at providing to cyber policymakers and stakeholders an overview of global cyber policy developments and capacity building projects.

This fourth edition covers again a wide range of topics that touch upon key developments on global cyber capacity building as well as regional updates and initiatives across the cyber spectrum.

Our cover story comes from the Global Forum on Cyber Expertise (GFCE) with a reflection on the process of developing a Global Agenda for Cyber Capacity Building with the aim to give a political impulse to the importance of cyber capacity building during the Global Conference on Cyberspace 2017 in New Delhi. The Global section further covers the efforts of the Forum of Incident Response and Security Teams (FIRST) and the significance of the implementation of Critical Information Infrastructure Protection by both the Meridian and the GFCE.

From Africa we have the Mauritian perspective on the fight against cybercrime in their National Cybercrime Strategy and the promotion of cyber due diligence in the ECOWAS Cyber Strategy Workshop. From the Americas we have an article that demonstrates how Latin America bridges the technical skills gap as well as an article on the extinct National Computer Security Network of Mexican Universities. Our Asia section includes an overview of UNODC's work, capabilities and partnerships on countering cybercrime in Southeast Asia and beyond and a review of how Australia's International Cyber Strategy is complemented by capacity building and creative partnerships.

We welcome your feedback and invite you to share with us information regarding cybersecurity conferences, workshops, training events, policies or case studies that other global entities might find useful. We would be particularly interested to learn about new capacity building initiatives, legislations or strategies in cybersecurity.

We hope you enjoy this issue of the Global Cyber Expertise Magazine and look forward to your continued feedback!

On behalf of the Editorial Board,

A handwritten signature in black ink, appearing to be 'D van Duren', written in a cursive style.

David van Duren

Head of the Global Forum on Cyber Expertise Secretariat

Capacity Building is the Key to Fight Against Cybercrime: The Mauritian Perspective

Currently, governments are working hard on how to effectively counter threats posed by cybercriminals. While cybercrime evolves, new challenges emerge for traditional regulatory and law enforcement agencies. There is a need to go beyond traditional law enforcement and explore means that predict, prevent and disrupt online criminal activities through an effective capacity building framework. This article describes initiatives on cyber capacity building which have been included in the Mauritian National Cybercrime Strategy.

Written by: Kaleem Ahmed Usmani, Head, and Jennita Appanah Appayya, Information Security Consultant, Computer Emergency Response Team of Mauritius (CERT-MU), National Computer Board, Mauritius

Facing an increase in threats in cyberspace, cohesive and comprehensive policies are essential in building an effective cyber defense. The changing phase of cyber-attacks and sophistication of attack methodologies have presented new cyber security challenges. The need for individuals and organisations to keep pace and be prepared to prevent and respond to these security risks and challenges is growing.

Mauritius recognises the serious threats posed by cybercrime and the necessity to trial cybercrimi-

nals. The capabilities of law enforcement agencies need to improve in order to detect, handle and prosecute cybercriminals. Further, the judiciary must advance their understanding in terms of the technicalities and complexities whenever cases are brought before courts. It is therefore imperative to develop a coordinated approach in terms of a National Cybercrime Strategy that would cater to these needs.

The National Cybercrime Strategy of Mauritius provides an insight into what approach the government

takes in their fight against cybercrime. It is constructed to provide a swift response to cybercrime through improved law enforcement capability, effective criminal justice framework and active international engagement. In addition, collaboration between all key players in both public and private sectors to safeguard national cyberspace is underlined. Six high priority areas have been identified that will help in strengthening the national response to cybercrime:



Opening Ceremony: East Africa Regional Conference on Cybercrime and Electronic Evidence, BalACLava, Mauritius

“The capabilities of law enforcement agencies need to improve in order to detect, handle and prosecute cybercriminals.”

Priority Areas:

- 1. The development of an effective legal framework to detect, handle and prosecute cybercrime:** This will facilitate the enforcement of new laws with regard to different types of cybercrimes and its prosecution. It would also provide legal practitioners and judicial officers with the capacity and expertise to deal with digital evidence.
- 2. Building capacity to better address cybercrime:** The capacity and capability of legal professionals and the judiciary need to be enhanced to deal with the technical aspects of cybercrime such as examination of the digital evidence.
- 3. Cyber Intelligence and Cyber Defense:** The value of collecting intelligence about (possible) cyberthreats cannot be underestimated. To tackle cybercrime, it is important to gather and exchange intelligence from the public, businesses and government agencies.
- 4. Public and Private Partnership:** The dynamic participation of the public and private sector is a key component in the fight against cybercrime. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation and recovery operations.
- 5. International collaboration:** Cybercrime is an international problem which requires a coordinated and cooperative international response.
- 6. Advocacy and public awareness:** The public needs to be made aware of possible cyber threats. Education on responsible use of the Internet and the impact of cybercrimes is key.

Capacity Building from the Perspective of Cybercrime Strategy

Capacity building as an approach to cybercrime has a number of advantages. It responds to needs and produces immediate impact, favours multi-stakeholder cooperation and contributes to human development.

—

“The National Cybercrime Strategy stresses the importance of building capacity on different levels of the institutions dealing with cybercrime.”

The National Cybercrime Strategy stresses the importance of building capacity on different levels of the institutions dealing with cybercrime. The proposed recommendations are as follows:

Cybercrime Investigation

The investigation of crimes involving technology requires that new knowledge and skills are acquired by those tasked with the investigation process, usually a law enforcement agency, such as the Mauritius Police Force (MPF). A comprehensive capacity building programme to be developed to enhance the cybercrime investigation expertise within the units dealing with cybercrime under the MPF.

Forensic Examination of Digital Evidence

Forensic examination of digital evidence is a key component in the

investigation and prosecution of cybercrime. This process requires trained staff due to its fragile and easily tampered nature. The strategy proposes specialised training programmes in digital forensic skills for police officers. Furthermore, as part of the Global Action on Cybercrime Extended project (GLACY+), the Government of Mauritius, the International Association of Prosecutors (IAP) and the Council of Europe jointly organized the East Africa Regional Conference on Cybercrime and Electronic Evidence. Here, representatives of 12 countries in the region worked to improve international cooperation against cybercrime in Mauritius from 10-12 July 2017.

Cybercrime Assessment Exercises

Cybercrime Assessment Exercises in the form of cybersecurity drills will be carried out to assess and evaluate the capabilities of law enforcement agencies and the other stakeholders dealing with cybercrime. It is also an effective way to join forces in combatting cybercrime at international and regional levels through information sharing, investigation and capacity building.

Educational Campaigns

As part of the “Cyber Smart Programme”, educational campaigns targeting diverse groups in society will be organised to raise awareness on cybercrime issues and the measures required to protect it.

Promotion and Development of Best Practices on Cybercrime

To encourage businesses to adopt practices aimed at promoting

secure online behaviour throughout the wider community, the distribution and development of low cost tools will be promoted to help businesses to prevent and detect online threats.

Final Note

—

Combating cybercrime is a shared responsibility and requires the attention of a broad range of stakeholders to become successful. The Mauritian National Cybercrime Strategy has placed strong emphasis on capacity building to improve law enforcement capability and enhance the criminal justice framework. The implementation of the above-mentioned capacity building programmes on cybercrime will certainly build a better protection framework.

References:

1. National Cybercrime Strategy 2017-2020 of Mauritius
2. Global Action on Cybercrime Extended (GLACY)+ Project, Council of Europe
<http://www.coe.int/en/web/cybercrime/-/glacy-eastern-african-countries-meet-in-mauritius-to-address-the-growing-threat-of-cybercrime-in-the-region>

U.S. Department of State and ECOWAS Partner to Promote Cyber Due Diligence in West Africa

The growth and diffusion of Internet-based technology globally has created new economic, social and political opportunities in every region of the world. It has also presented new challenges to countries that seek to harness the Internet for economic development while also addressing threats in and through cyberspace. Cyber strategies act as a tool to help nations navigate activities in cyberspace. The Department of State– sponsored ECOWAS Cyber Strategy Workshop was designed to help national leaders do just that –plan strategically for cyber as an enabler for national objectives.

Written by: Johanna Vazzana, Lead Cybersecurity Engineer, The MITRE Corporation

Cooperating Across Borders to Address Challenges in Cyberspace

International cooperation is critical in achieving national objectives. The Economic Community of West African States (ECOWAS) together with the U.S. Department of State (DoS) recognize the importance of regional cooperation to advance mutual interests in cyberspace.

To assist in meeting regional goals ECOWAS, the DoS' Office of the Coordinator for Cyber Issues (S/CCI) and Bureau of International Narcotics and Law Enforcement Affairs (INL) supported MITRE, a U.S. federally funded research and development center, to co-host a cyber strategy workshop for senior leaders from all 15 ECOWAS Member States.

The four-day workshop, held June 12-15 and hosted by the U.S. Embassy in Abuja, sought to streng-

then regional understanding of cyber threats and opportunities; identify areas of mutual interest for regional cooperation; inform development of national cyber strategies and plans; and promote more effective international legal cooperation in the sharing of electronic evidence.

The workshop enjoyed the maximum attendance of 60 participants representing each of the 15 ECOWAS Member States. Subject matter experts from international



ECOWAS Cyber Security Strategy Workshop was held June 12-15, 2017 Abuja , Nigeria

organizations and industry attended as well, including representatives from the Council of Europe, the Commonwealth Telecommunications Organization, the U.K. Foreign and Commonwealth Office, the Dutch Embassy in Abuja, the European Union, the African Union Commission, the ECOWAS Commission, local industry partners, and from the governments of Cape Verde, Cote d’Ivoire, Nigeria, and Senegal.

Promoting Cyber Strategies

S/CCI directed MITRE to create the National Cyber Strategy Fra-

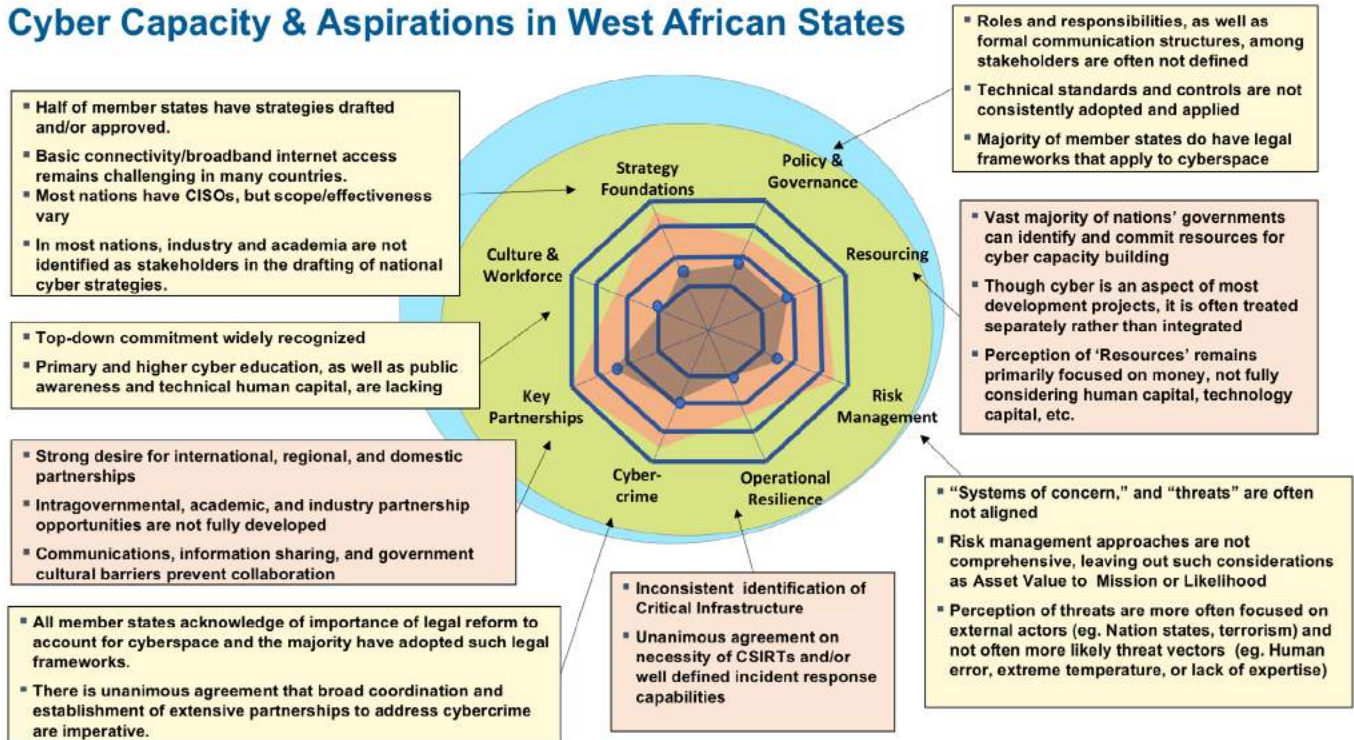
mework to assist in executing this workshop and other State Department missions related to developing and implementing national cyber strategies. This tool framed all activities throughout the week and encouraged Member States to think strategically under a common lexicon and framework. Participants drafted national “strengths and challenges” statements; a preparatory exercise to help determine national readiness to engage in strategic cyber planning; a table top exercise to help illuminate process gaps in responding to a cyber incident; specific national goals for cyberspace and implementable tasks and subtasks; and a sample public service announcement to raise citizens’ aware-

ness of the opportunities and threats in cyberspace.

Collaboration and discussion were rich; participants engaged across national boundaries, asking questions, sharing information and extending offers of assistance. Some of the most significant takeaways included:

- The provision of best practices for national cyber strategy development and implementation that provide a tool to communicate and mandate national goals for cyberspace.
- The exposure provided to assist Member States in harmonizing their legal frameworks in line with ECOWAS Community Acts

Cyber Capacity & Aspirations in West African States



and the Council of Europe Convention on Cybercrime (Budapest Convention).

- The presentation of a clear visual of regional goals and aspirations in cyberspace as compared to current regional capacity, as defined by Member States themselves. This visual clearly represents the region's level of cyber capacity and where efforts should be focused to meet self-identified regional aspirations.

In addition, a prioritization exercise utilized the gathered data and led participants through a process that resulted in a focused list of possible next steps for the region that reflected

Member States' opinions of the most pressing concerns for cyber capacity building. Key issues from the prioritization exercise included: the need for all member states to publish national cyber strategies; the desire to establish national Computer Security Incident Response Teams (CSIRTs) with a regional coordination mechanism among them; and the importance of raising leadership understanding of the criticality of planning for cyber.

What next?

Workshop activities provided participants with individual national next steps and take-home wor-

“This visual clearly represents the region’s level of cyber capacity and where efforts should be focused to meet self-identified regional aspirations.”

Cyber Aspirations for the ECOWAS Region

- **1 – ALL MEMBER STATES PUBLISH NATIONAL CYBER STRATEGIES**
 - 1 – TOUS LES ETATS MEMBERS PUBLIENT DES STRATEGIES CYBERNETIQUES NATIONALES
 - 1 – TODOS OS ESTADOS MEMBROS PUBLICAM ESTRATEGIAS CIBERNETICAS NACIONAIS
- **2 – BROADBAND INTERNET INFRASTRUCTURE**
 - 2 - INFRASTRUCTURE INTERNET À LONG TERME
 - 2 - INFRA-ESTRUTURA DE INTERNET DE BANDA LISTA
- **3 – NATIONAL CSIRTS AND REGIONAL COORDINATION MECHANISM**
- **4 – ADOPTION OF INTERNATIONAL STANDARDS**
 - 4 - ADOPTION DES NORMES INTERNATIONALES
 - 4 - ADOPÇÃO DE NORMAS INTERNACIONAIS
- **5 – INTEGRATION OF CYBER INTO DEVELOPMENT PROJECTS**
 - 5 - INTÉGRATION DE CYBER DANS LES PROJETS DE DÉVELOPPEMENT
 - 5 - INTEGRAÇÃO DE CYBER EM PROJETOS DE DESENVOLVIMENTO
- **6 – RAISE LEADERSHIP UNDERSTANDING OF THE CRITICALITY OF PLANNING FOR CYBER**
 - 6 – SENSIBILISER LE LEADERSHIP A LA CRITICITE DE LA PLANIFICATION DU CYBER
 - 6 – AUMENTAR A COMPREENSAO DE LIDERANCA SOBRE A CRITICIDADE DO PLANEJAMENTO DO CYBER
- **7 – IDENTIFICATION OF CRITICAL INFRASTRUCTURE AND DEVELOPMENT OF A CI PROTECTION PLAN**
- **8 – HARMONIZATION OF LEGAL FRAMEWORKS IN LINE WITH REGIONAL AND INTERNATIONAL CONVENTIONS**
- **9 – REGIONAL EVENTS TO PROMOTE PARTNERSHIPS**
 - 9 - ÉVÈNEMENTS RÉGIONAUX POUR PROMOUVOIR DES PARTENARIATS
 - 9 - EVENTOS REGIONAIS PARA PROMOVER PARCERIAS
- **10 – EDUCATIONAL CURRICULUM AND PUBLIC AWARENESS**
 - 10- CURRICULUM CYBER DE L'ÉCOLE PRIMAIRE ET LA SENSIBILISATION DU PUBLIC
 - 10 - CURRICULUM DE CYBER DE ESCOLA PRIMÁRIA E SENSIBILIZAÇÃO PÚBLICA

“The ECOWAS Cyber Strategy Workshop provided attendees with the tools to view cyber capacity and cybersecurity as enablers to national objectives.”

ksheets for further development. In addition, briefings, activities and discussions were used to draw out regional priorities, leveraging the discoveries made during the workshop and from pre-workshop surveys. The activities culminated with participants discussing and debating potential regional priorities that could help advance cyber strategy and cybersecurity in West Africa.

The results of workshop activities provided a solid foundation for regional strategic cyber planning. Secure information and communication technologies have the potential to strengthen business confidence and enhance good governance throughout the ECOWAS region thus enabling new prospects for economic growth and development. Workshop activities reinforced that na-

tional leadership has an important part to play by establishing thoughtful strategic and legal frameworks that create an enabling environment for these technologies to grow and remain secure. Through regional cooperation and the necessary frameworks, a digital economy can be nurtured that facilitates investment and industry growth. In this economy, cyber capacity and cybersecurity are valuable and necessary. The ECOWAS Cyber Strategy Workshop reinforced this concept and provided attendees with the tools to view cyber capacity and cybersecurity as enablers to national objectives, to think strategically about cyber issues, and to promote more effective international legal cooperation.

Addressing the Skills Gap in Digital Security

With one of the fastest Internet growth rates since the beginning of the century, Latin America and the Caribbean have experienced an increase of over 2% in the number of Internet users between 2000 and 2017. As the technological revolution spreads within the region, new opportunities are created in the labor market, increasing the need for a more skilled labor force. While this growth has brought numerous opportunities for the region, concerns are raised about the current and potential use of the Internet for criminal and terrorist purposes. With the rising threat of cyberattacks, having an understanding of cybersecurity becomes a highly valued skill in the labor market. Latin America has one of the highest shortages of skilled labor in the world, especially in the cybersecurity and information technology (IT) sector. In fact, it is predicted that by 2019, the region will lack more than 400 000 IT professionals. However, there has been an increase in capacity building programs on cybersecurity education, which are being developed to bridge the technical skills gap in Latin America and the Caribbean.

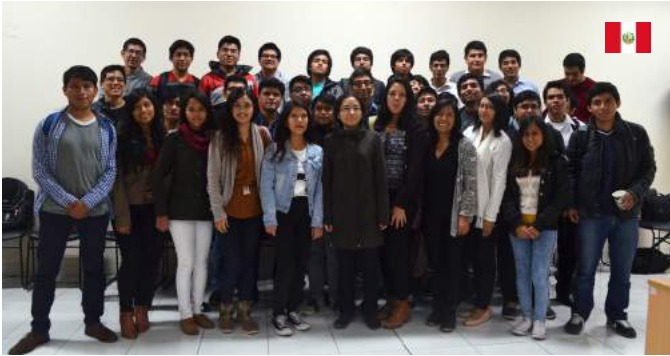
Written by: Gonzalo García-Belenguer, Project Officer, Cyber Security Program, Inter-American Committee against Terrorism (CICTE), Organization of American States and Mariana Cardona, Project Officer, Cyber Security Program, Inter-American Committee against Terrorism (CICTE), Organization of American States

Setting the Stage: the Latin American Context

Latin America has a great untapped potential: youth. With 25% of its population aged between 15 and 20 years, the region has a large working age population and a promising future in regards to its labor force. How-

ever, Latin America faces two major challenges that restrict economic growth; the prevalence of undeclared work and the lack of technical skills. With 55% of the population working in the informal economy and 2 out of 5 young people neither studying nor working, Latin America is one of the regions with the highest shortage of skilled labor. According to the Inter-


national Finance Corporation (IFC), 55% of Latin American companies have difficulties recruiting skilled labor, specifically in technology related fields. In Colombia, the Ministry of Information Technology and Communications (MINTIC) has identified a deficit of 15,000 software and telecommunication engineers, and in Peru, 67% of employers report having




Creating a Career path in digital security

Students trained : **127**

26% female  74% male 

38 in Colombia 

40 in Peru 

26 in Panama 

23 in Trinidad and Tobago 

10

Universities engaged

Age:

17-25
years old

#pathways2progress

—

“55% of Latin American companies have difficulties recruiting skilled labor, specifically in technology-related fields.”

difficulties recruiting skilled labor.

According to a study developed by the International Data Corporation, one of the largest skill gaps identified in Latin America is in emerging networking technology skills and essential networking skills, which includes cloud, Internet of Things, cybersecurity, software development, and network security. In addition to the overall lack of technical skills in the region, there is a wide gap between the technical skills available and those that are in demand in

the current labour market. This can partially be explained by the lack of formal training and education in cybersecurity and IT that exists in Latin America. According to the report “Cybersecurity: Are we ready in Latin America and the Caribbean?” published in March 2016 by the Organisation of American States (OAS) and the Inter-American Development Bank (IDB), 26 countries from the region do not have structured educational programs related to cybersecurity. For instance, in Trinidad and Tobago some universities offer courses on ethical hacking but there are no official cybersecurity degrees or certification programs. In other countries like Peru, there are many national universities and private companies that offer trainings in cybersecurity, but they lack adequate technology and experienced teaching staff.

On the upside, there has been a marked growth of national cybersecurity education development in Colombia and Panama, where numerous universities, agencies and institutions provide training, accreditation programs and advanced degrees in cybersecurity.



Creating a Career path in digital security

The Program Creating a Career Path in Digital Security, financed by Citi Foundation and implemented by the OAS and the Young Americas Business Trust (YABT), is a clear example of an initiative that is working towards bridging the technical skills gap in Latin America and the Caribbean. The goal of this program is to empower youth from low-income households and foster career readiness in the region. The program provides digital security training for over 120 young people aged between 17-25 years and sources internship opportunities for program beneficiaries in Colombia, Panama, Peru and Trinidad and Tobago.

The curriculum consists of technical theory, hands-on exercises and job readiness training. Various topics are discussed: digital security principles; information security wi-

thin lifecycle management; risks and vulnerabilities; incident response; and future implications and evolving technologies. The training allows students to acquire the basic knowledge needed to access entry-level positions in the field of digital security, obtain a recognized certification and participate in an internship program. The internship program offered helps qualified students get acquainted with a formal work environment, gain knowledge on the technical aspects of incident management in cybersecurity and learn from experts in the field. This way, students are well prepared for when they enter the workforce in the field of digital security.

Citi is not the first company to develop programs that intend to address the technical skills gap in the region. Since 2000, Cisco and USAID have joined forces to sponsor Networking Academies in over 40 countries all around the world. These academies partner with governments, learning institutions and community centers in order to promote entrepreneurship, offer technical trainings and foster the development of professional skills with a focus on topics such as networking, security and Internet of Things (IoT) technologies.

Tangible Solutions

Academia, private companies and government organisations should work together to build up technical skills and experience among young people that complement the needs of the current economy. To bridge the technical skills gap, first and foremost the educational systems in Latin America must be improved.

“Academia, private companies and government organisations should work together to build up technical skills and experience among young people that complement the needs of the current economy.”

While the labor demand for jobs in telecommunications, cybersecurity and IT increases, young people should also be encouraged to study these professions which can be done through the development of incentives, training programs and apprenticeships. With a large young population, Latin America has great potential for building a skilled and prepared labor force in cybersecurity and IT.

Brief history of the extinct National Computer Security Network of Mexican Universities

In 2003 RENASEC was established in Mexico to form a National Network of Computer Security, which would protect and respond in an effective manner to cybersecurity incidents. However, RENASEC disappeared in 2013, so Mexican universities are now regrouping in the Committee on Information Technology and Communications (ANUIES-TIC Committee) where the issue of cybersecurity is being promoted again.

Written by: José Luis Ponce López, Director of Information and Communications Technologies of the National Association of Universities and Higher Education Institutions of Mexico.

Background

Over the past decade, the way societies communicate and share their information has drastically changed. The development of new information and communications technology has brought many advantages, making communication fast and convenient. However, as with any new technology, there are numerous risks arising from its use. These range from exposure, modification and manufacturing sensitive information on both individual or organizational level.

That is why in 2003 the National Computer Security Network, RENASEC, for its acronym in Spanish, was founded in a joint effort by the top Mexican universities, the National Association of Universities and Institutions of Higher Education (ANUIES) and the Computer Emergency Response Team of the National Autonomous University of Mexico (UNAM-CERT). The UNAM-ANUIES aimed to form an Academic Network that will consolidate a national front in Mexico to counteract problems related to Computer Security.

The objectives

The objective of RENASEC was to form a National Computer Security Network of Mexican universities that would adequately protect and respond to emergencies in information technologies in the country's higher education institutions.

Among its objectives, several things were highlighted, such as: the promotion of collaboration between the universities of the country in the field of Computer Security, culture towards Information Security, aware-

National Network and Regional Networks of Computer Security (2003-2013)



National and Regional Networks of Computer Security (2003-2013)

ness of academic communities, integration of issues related to Computer Security in the plans and curricula of the universities and the promotion of training in Computer Security of all the members of RENASEC.

The work of the National Network and the Regional Networks of Computer Security

The elementary strategy of the national network was the inter institutional collaboration through Regional

Networks. This led to the creation of a National Network (RENASEC) and six Regional Networks of Computer Security, which reported a work plan and results in the coordination of RENASEC.

The Regional Computer Security Networks were divided as follows: Northwest, Northeast, Central-West, Central-South, Metropolitan and South-Southeast of ANUIES. Each Regional Computer Security Network had a coordinator who was chosen by the heads of the universities in their region.

Initially, RENASEC was coordinated on a national level. Regional coordinators came together in Mexico City and discussed ongoing projects,

“A National Computer Security Network of Mexican universities that would allow to adequately protect and respond to the relative emergencies in of information technologies in the country’s higher education institutions.”

some examples are given below.

- Computer Security Diagnoses in the Mexican Universities (2004, 2005, 2011 and 2013). Its objective was to carry out annual diagnoses about the situation of Computer Security on a national level and tailor the work of RENASEC according the needs of Mexican universities.
- RENASEC web portal, where acquired knowledge of different regions was combined. Its objective was to report on the work of the National Network and the regional networks on the threats related to the matter.

- Updated directory of institutional and technical leaders. Its objective was to have an updated directory of contact points in the national level of all those responsible for Computer Security at RENASEC, thus fostering communication and collaboration.
- Regulations in "RENASEC STATUTE". Its objective was to lay the foundations of a norm for RENASEC to regulate its operation.
- Positioning of RENASEC. Its objective was to ensure that RENASEC, was recognized by all Mexican universities as a collaborative network in the field of Computer Security.
- Training program. Its objective was to make proposals for comprehensive training on Computer Security for all members of RENASEC.
- Designation of Computer Security Officers of the universities. Its objective is to appoint a formal point of contact in all affiliated universities of Mexico under a professional profile in the field of computer security.

Conclusions

The actions promoted by RENASEC where the first joint effort to promote collaborative work among Mexican universities, and immediately achieved very good results, highlighting the consolidation of the National Network, the beginning of the formalization and training of specialized human resources, the consolida-

tion of a central website, and various communication mechanisms such as mailing lists, podcasts, participation in the Computer Security Congress of the UNAM, participation in regional meetings of computer security, etc. Furthermore, RENASEC worked on constantly updating all contact points responsible for computer security of Mexican universities.

However, by the year 2013, before an institutional decision of the ANUIES, it was decided to annul the National Network of Computer Security, and only the Regional Networks remained. Over time these regional networks weakened and eventually most dissolved as well. Now, only the ANUIES Center-South Region Computer Security Network stands.

Since 2015 ANUIES created the Committee on Information Technology and Communications, or ANUIES-TIC, for its acronym in Spanish, the issue of cybersecurity is being promoted and Mexican universities are regrouping. This will bring new challenges, it will require alliances and collaborative work to consolidate and captivate the universities of Mexico.

The ANUIES-TIC Committee promotes collaborative work among partner universities, dissemination and awareness of IT managers in topics as governance and security matters, as well as in training, training and updating, and creating global agreements about projects, initiatives, products and services.

References:

Aquino et al. Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior. ANUIES, México. 2013. <http://publicaciones.anuies.mx/libros/166/resultados-de-la-encuesta-de-seguridad-de-la-informacion-2011-en-las>

Ponce et al. Estado Actual de las Tecnologías de la Información y las Comunicaciones en las Instituciones de Educación Superior. Estudio Ejecutivo 2016. p. 47-53. ANUIES, México. 2016. http://anuies-tic.anuies.mx/web/encuentro2016/wp-content/uploads/pdf/EstadoActualTIC_en_las_IES.pdf

Other links:

<http://anuies-tic.anuies.mx>
<http://encuentro-tic.anuies.mx>
<http://www.anuies.mx>

UNODC: Countering cybercrime in Southeast Asia and beyond

Capacity Building to counter cybercrime and enhance cybersecurity takes a multitude of forms; from policy analysis to preventive diplomacy, legislation to enforcement. This article provides an overview of UNODC's work, capabilities and partnership approach.

Written by: Neil Walsh, Head of the United Nations global programme on cybercrime.

Diplomatic context

Within the United Nations, and particularly within the Office on Drugs and Crime (UNODC), the counter-cybercrime capacity building approach responds to requests from Member States and is intentionally politically neutral.

In 2013, UNODC published the draft Comprehensive Study on Cybercrime. The study, conducted under the auspices of UNODC's Intergovernmental Expert Group (IEG), presented an analysis of cybercrime (as it was in 2011/12) and paved the way for future diplomatic cooperation to counter the threat at the policy level [1].

In April 2017, the IEG met again in Vienna to discuss the Study and ways forward for cooperation. The UNODC recognizes that there is a divergence of opinion on many key issues regarding cybercrime from definition, to legislation and methods of international cooperation. However, we also recognize that, from these different positions, we can identify areas of agreement and consensus. At the 2017 IEG meeting, there was a broad, apolitical consensus regarding the need for increased capacity building globally to enable law enforcement, prosecutors and judges to counter the threat of cybercrime.

Capacity Building

Capacity building to counter transnational organized crime and terror often begins with a focus on legislation. With cybercrime, however, there is sometimes a need for a more nuanced approach. There are still, amazingly, some governments who do not feel that cybercrime either exists or is a threat to them. Those of you reading this article recognize the folly of that approach - and this is where UNODC can have a direct impact.

When representatives of UNODC meet with Heads of State, brief parliamentarians, give evidence to over-



UNODC Train the Trainer Cryptocurrencies Investigations in UNODC HQ , Vienna, Austria 11 - 13 April 2017

—

“Counter-cybercrime capacity building approach responds to requests from Member States and is intentionally politically neutral.”

sight committees and discuss the threat through media outreach, it has an immediate and longstanding impact. In this endeavor, it is imperative to start and lead discussions that help Administrations to form a cross-government response to cybercrime - the core premise of UNODC’s Global Programme on Cybercrime. Tools such as the World Bank assessment toolkit, and a little technical capacity building for criminal justice actors, help to pave the way for a new policy - and legal - response to cybercrime.

The following is a list of examples of capacity building that the

UNODC has delivered in 2016/17, through the regional Southeast Asia Cybercrime Coordinator in Bangkok:

25 - 27 April 2017, Colombo, Sri Lanka - Cybercrime investigations and digital forensics joint training
Funding: World Bank

Executed in partnership with the World Bank as part of the StAR (Stolen Asset Recovery) programme, to officers from various institutions charged with cybercrime investigations and digital forensics.



UNODC Cryptocurrencies Investigation Training for Thai Officials in , Anti Money Laundering Office AMLO Building, Bangkok Thailand 18 - 20 July 2017

01 - 05 May 2017, Gold Coast and Canberra, Australia - Youth Technology and Vulnerable Communities Conference

Funding: Norway

UNODC delivered an awareness session, attended by Southeast Asian Law Enforcement Agencies (LEAs) on the role of cryptocurrency within live-streaming online infant and child sexual abuse. A full training session will be delivered in 2018.

25 - 26 May 2017, Vientiane Lao PDR - 17th ASEAN SOMTC Meeting (Senior Officials Meeting on

Transnational Organized Crime) Funding: USA

UNODC contributed strongly to the ASEAN policy discussion regarding the SOMTC Cybercrime Working Group and future collaboration.

18 - 20 July, Bangkok, Thailand - Cryptocurrencies Investigations Training for Thai Officials

Funding: UK, Australia and Japan

The training was attended by 25 investigators and analysts from cybercrime, counter-terrorism, FIUs and anti-money laundering departments of the following Thai institu-

—
“There are still, amazingly, some governments who do not feel that cybercrime either exists or is a threat to them.”

—

Cybercrime and cybersecurity, as we have seen, are often politically charged topics: from democratic elections and energy security to online radicalization of terrorists.”

tions: Bank of Thailand, Anti Money Laundering Office, Royal Thai Police, Royal Thai Cadet Academy, Department for Special Investigations, National Security Council, Electronic Transactions Development Agency and the Office for Narcotics Control Board. Attendees now have the capability to identify and follow blockchain transactions and exploit evidential opportunities internationally.

06 - 12 August, Kathmandu, Nepal, - Joint ITU, INTERPOL and UNODC Engagement

Funding: ITU (Nepal)

Joint engagement to provide Nepal with a draft cybercrime law and to deliver trainings based on intermediary cybercrime investigations and digital forensics training.

Throughout the biennium: ongoing mentoring for cybercrime law enforcement, prosecutors and judges

Funding: Canada and USA

This includes malware proliferation and live streaming of child sexual abuse. In addition, many training sessions on victim identification, the #WePROTECT Model National Response and psychological profiling have been carried out with ICMEC (the International Centre for Missing and Exploited Children), HSI (ICE) and INTERPOL.

Conclusion

—

Cybercrime and cybersecurity, as we have seen, are often politically charged topics: from democratic elections and energy security to online radicalization of terrorists. UNODC's work, and that of partners like the GFCE, makes a tangible difference in cyberspace: Member States work closer together to counter the most advanced and persistent threats originating from cybercriminals and grow trust through international investigations.

By working even closer together, the UN system stands ready to counter the highest risk threats faced by society today. Together we are stronger. Together we can ensure a free, open internet and reduced cybercrime, which is critical for delivering the Sustainable Development Goals.

More information:

[1]https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Australia's inaugural International Cyber Engagement Strategy: global in perspective, regional in focus

A comprehensive and coordinated approach to cyber affairs

The growing complexity of cyberspace means cyber affairs are increasingly significant in international relations. Australia's inaugural International Cyber Engagement Strategy champions an open, free and secure cyberspace. The forward leaning Strategy recognises the breadth of international cyber issues and adopts a comprehensive and coordinated approach led by the Australia's Ambassador for Cyber Affairs. The ambitious agenda is complemented by capacity building and creative partnerships between governments and the private sector, with a view to promote regional prosperity and a peaceful and stable online environment.

Written by: Dr Tobias Feakin, Australia's Ambassador for Cyber Affairs

Cyber Affairs

We live in the most interconnected era in human history. Instantaneous communications, transactions, and access to information keep our economies growing, infrastructure working, governments enabled and people connected. The connections between governments,

businesses and individuals are more significant than ever before.

As the complexity of cyberspace is growing, cyber affairs demand increased international attention and cooperation. We must actively engage with the international community, as exciting opportunities emerge, critical debates unfold and global rules are agreed.

Australia's Response

Australia recognises this important opportunity and challenge. Our standing as a responsible contributor to the international community gives us a platform to engage in constructive conversations on cyber policy issues with global partners. Active participation in



Australia's Foreign Minister, The Hon Julie Bishop MP, launched Australia's first International Cyber Engagement Strategy on 4 October 2017 in Sydney.

global cyber cooperation efforts affords Australia a leading international role in shaping the future of cyberspace.

Australia's first *International Cyber Engagement Strategy* (the Strategy) articulates Australia's cyber affairs agenda to the world. The Strategy outlines the principles, interests and goals that guide Australia's international engagement on cyber issues.

Australia embraces an innovatively broad approach to international cyber issues. The Strategy presents Australia's public and private sector pursuit of an open, free and secure

Internet across seven distinct areas. Together, these themes comprise Australia's comprehensive and coordinated cyber affairs agenda, led by the Ambassador for Cyber Affairs:

1. **Digital trade:** the digital technology revolution is fundamentally a story of prosperity. Increasingly, cyberspace acts as an economic enabler. Australia will shape an enabling environment for digital trade and promote trade and investment opportunities for digital goods and services.

—

“Active participation in global cyber cooperation efforts affords Australia a leading international role in shaping the future of cyberspace.”

2. **Cyber security:** the spread of digital technologies creates profound economic opportunities, but simultaneously creates new vulnerabilities. Governments and the private sector working together to develop a strong cyber security posture is essential to ensuring we can all safely capitalise on the benefits of increasing connectivity.
3. **Cybercrime:** Improving cyber security is an important way of mitigating the risk of cybercrime. Left unchecked, criminal use of the Internet threatens to undermine the economic opportunities offered by the digital domain. Collaboration with international partners and assistance to countries in our region improves their capacity to address cybercrime, which will improve worldwide cybercrime prevention and prosecution mechanisms.
4. **International security & cyberspace:** Developments in cyberspace have created a new arena in which states can exert influence. We will cooperate with international partners to deter and respond to cyber activity that endangers a stable and peaceful online environment. Reaffirming the application of international law adhering to norms of responsible behaviour, and implementing confidence-building measures in cyberspace will shape it as a landscape for international cooperation and mutual benefit.
5. **Internet governance & cooperation:** A multi-stakeholder approach, which places all stakeholders on an equal footing in Internet governance debates, best

facilitates an open, free and secure Internet. Better multi-stakeholder cooperation domestically, regionally and internationally will preserve decentralised control of the Internet, allowing all voices to be heard when decisions over the policy and technical management of the Internet are made.

6. **Human rights & democracy online:** The Internet itself has provided an unparalleled opportunity for democratic participation and the promotion, protection and fulfilment of human rights. Governments, the private sector, civil society and academia must continue to work together to uphold and defend human rights online, just as they do offline. This contributes to lasting peace, security, freedom and dignity for all.
7. **Technology for development:** Digital technologies act as enablers of sustainable development and inclusive economic growth. However, dividends of the digital age are currently not evenly experienced. Australian efforts to increase connectivity and help countries harness digital technologies safely will accelerate the attainment of sustainable development objectives in the region.

Australia's approach to international cyber issues is also underpinned by cross-cutting concepts of partnership, a regional focus and capacity building

Creative Partnerships

Australia's ambitious cyber affairs agenda is impossible to achieve

“We will cooperate with international partners to deter and respond to cyber activity that endangers a stable and peaceful online environment.”

alone. This is a shared challenge and a shared responsibility. All of our efforts, both globally and regionally, will be delivered in partnership, harnessing unique and complementary skills of other countries, the private sector, civil society and academia.

The Indo-Pacific

The Strategy has a strong Indo-Pacific focus. Collaborating with countries all over the world forms the foundation of our cyber posture, but our diverse neighbourhood is where we can have the greatest impact. Australia's regional knowledge, trusted national brand, strategic economic and security interests and long-standing development partnerships leave us well placed to influence the evolution of cyber affairs in the Indo-Pacific region.

Capacity Building

Australia is significantly increasing its investment in regional capacity building across all of the Strategy's themes. This will improve



Australia's Foreign Minister The Hon Julie Bishop MP and Australia's Ambassador for Cyber Affairs Dr. Tobias Feakin at the launch of the International Cyber Engagement Strategy.

“Australia is significantly increasing its investment in regional capacity building across all of the Strategy’s themes.”

confidence in the online environment, increase economic opportunities, reduce financial losses to cybercrime, minimise the regional risks of strategic miscalculation, promote multi-stakeholder Internet governance, protect human rights online and deliver sustainable development outcomes.

Australia's International Cyber Engagement Strategy presents a forward leaning pursuit of an open, free and secure cyberspace. Our cyber cooperation and capacity build-

ing will promote regional prosperity and ensure we all continue to benefit from a peaceful and secure online environment.

GFCE: Moving forward

Putting Principles into Practice

Over the past year, the Global Forum on Cyber Expertise (GFCE) community has taken leadership in developing a Global Agenda for Cyber Capacity Building (GACCB) through extensive research, consultation and discussion. At the Global Conference on Cyberspace 2017 in New Delhi, the GFCE community will present a Delhi Communiqué which serves as a formal announcement of the GACCB to the GCCS community. The aim of the document is to give a political impulse to the importance of cyber capacity building.

Written by: Manon van Tienhoven, GFCE Secretariat

When the Global Forum on Cyber Expertise (GFCE) was launched at the GCCS2015 in The Hague, it set out to be a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The GFCE serves as a knowledge hub and a platform to exchange ideas on good practices. By matching demand and supply, the GFCE functions as a clearing house that helps match members looking to share ideas and good practices with members looking to implement projects or host projects. The GFCE contributes to a better overview of

existing and planned capacity building initiatives; this minimizes duplication and conflict of actions, wherever possible promotes synergies and cooperation among (regional) stakeholders. These are all examples on how the GFCE has taken on a coordinating role in the field of cyber capacity building, which has led to the development of a Global Agenda with priorities and ambitions on cyber capacity building as well as the GFCE Global Good Practices.

Call for action

The Global Agenda for Cyber Capacity Building is a collection of shared ambitions on the priority setting of cyber capacity building topics. The aim of the GFCE community (GFCE Members, Partners and the Advisory Board) is to steer the development of an internationally coordinated response to cyber capacity building. Therefore it is essential to address the sense of urgency and to call for action to jointly strengthen cyber capacities. A Global Agenda is being developed with the objective



GCCS 2017

GLOBAL CONFERENCE ON CYBERSPACE

The Global Conference on CyberSpace 2017 takes place on November 23-24 in New Delhi, India.

“The Global Agenda is a collection of shared ambitions on the priority setting of cyber capacity building topics.”

to assist the global community with identifying future priorities for cyber capacity building and to recognize the need for practical guides, frameworks and practices on the topic. The GFCE aims to encourage to the global community with the GACCB to:

- Promote existing good practices;
- Strengthen international cooperation;
- Identify knowledge, technical or expertise gaps;
- Make more efficient use of available resources.
- Establish a concrete set of ambitions and concrete actions.

Taking a bottom-up, multistakeholder approach

The GFCE community has taken leadership in developing a Global Agenda. At every step of this development process, a broad range of stakeholders in cyber capacity building: national governments, technical community, private companies, international organizations, knowledge partners and civil society have been invited to provide input and feedback to ensure that the Agenda supports global and shared ambitions. Throughout the entire bottom-up process, the GFCE community had the opportunity to reflect on the various Global Agenda drafts during meetings; using feedback forms and questionnaires; as well as in individual and multistakeholder group conference calls. During the GCCS2017, the ambitions of the Global Agenda will be shared with the wider community by means of the Delhi Communiqué.

Next step: implementation

The GCCS2017 is a milestone in the existence of the GFCE; gaining support for the Delhi Communiqué and therewith the ambitions of the Global Agenda on high political level will give a political impulse to the importance of cyber capacity building. The call for action will lead to the development of an international response to cyber capacity building, which will need to be coordinated. In this regard, the existing GFCE initiatives work on formulating a set of GFCE global good practices (GGP). A GGP can be understood as a practice, recognized by experts in the field, which has proven to work and produce good results, and may be generically applicable for the global community. Examples of GGP include a practical tool, a set of related standards, or a guideline document. For practical purposes, a GGP includes specific recommendations regarding implementation. The development of the GFCE GGP is bringing the clearing house function of the GFCE to the next level by sharing the best



GFCE Annual Meeting 2017 in Brussels.

**“At the GCCS2017,
the ambitions
and of the Global
Agenda will be
shared with the
wider community by
means of the Delhi
Communiqué.”**

— practices and lessons learned with the GFCE and broader community. By taking this approach the GFCE avoids duplication and unveils gaps, improving efficient cyber capacity building.

Over the past two years, the GFCE has accomplished to expand its network and its role in cyber capacity building. Now the time has come to raise the stakes. The result of the bottom-up process over the past year has set out a clear path for the coming years for the GFCE. Moving forward the GFCE will continue to work on priority-setting in cyber capacity building, identifying global good practices and develop a concrete action plan for the GFCE community.

Developing the building blocks for a global Incident Response Capability

Every year, the internet community faces an ever growing number of data breaches and security incidents. Modern society, growing increasingly reliant on ICT and internet technologies, seems to be at ever greater risk. Just last year, an outage at a DNS provider showed how major sites can be affected by much smaller providers and network operators. This article describes how the Forum of Incident Response and Security Teams (FIRST) is investing to create a more capable incident response community.

Written by: Forum of Incident Response and Security Teams (FIRST)
Maarten Van Horenbeek, Board Member; and Damir Rajnovic, CFO.

The need for global incident response capability

Security incidents are rarely limited in geography. Last year's major DDoS attack on the Dyn DNS service saw tens of millions of IP addresses hitting a small set of services, resulting in outages for a large number of major internet properties [1]. The Wannacry malware was reported in at least 150 countries [2].

In order for corporations and economies to defend themselves suc-

cessfully against these attacks, some form of coordination with their peers abroad is required. It does not make sense for countries with varying capabilities to autonomously identify, investigate and respond to every single attack from scratch. There is a need for more global awareness of emerging incidents and the ability to share best practices while responding to an incident. Moreover, there is an opportunity for expertise to be pooled across regions, when it is more difficult to build and maintain.

This type of cooperation does

not happen by accident, but needs to be architected and planned, leveraging experts across the globe. The Forum of Incident Response and Security Teams FIRST, a leading association of computer security and incident response teams, was founded in 1989 shortly after the first Internet worm. Over the last few years, FIRST has identified and invested in some of the key building blocks we need to make a well-coordinated global Incident Response Capability a reality.



FIRST Trainer Michael Hausding teaches Incident Response skills in Puerto Rico.

Key building blocks for incident response

A global community

As a community, we can only be effective when all major networks, all countries and all industries are represented. That may seem like an ambitious goal, but it is a necessity to deal with attacks that may originate from anywhere. FIRST has actively grown its community in recent years through the Suguru Yamaguchi

Fellowship program, which provides subsidized access to our community for incident response teams from the developing world. In recent years, teams from Vietnam, Moldova, Myanmar, Ghana and Mongolia and several other countries have participated in our conference and trainings leveraging this program.

A common understanding

It is also critical that incident response teams have a mutual understanding of what it means to provide incident response services. FIRST

“There is a need for more global awareness of emerging incidents and the ability to share best practices while responding to an incident.”

—

“Over the last few years, FIRST has identified and invested in some of the key building blocks we need to make a well-coordinated global Incident Response Capability a reality.”

helps teams exchange experiences through no less than 28 annual events and trainings globally.

However, in order for these efforts to be successful, it is important to generate a mutual understanding of the work we do. Since 2015, FIRST has convened a global group of incident responders, academics, national government representatives and interested parties to collaborate on a Services Framework for CSIRT. This framework specifies typical services CSIRT provide, and details the work incident responders typically deliver under these services.

A similar effort has been started for Product Security Incident Response Teams (PSIRT), which focuses on addressing security incidents affecting software and hardware products.

Based on these frameworks, FIRST initiated the development of training programs for the key ser-

vices they describe. Each of these programs is released under a Creative Commons license, and can be used by members, non-members and partners to train new CSIRT teams.

High volume information sharing and coordination

Finally, incident response efforts will only become more effective when they can operate at machine speed. While humans are necessary to gain situational awareness, and make accurate decisions, those decisions need to be executed at speeds only machines can accomplish.

As a result, FIRST has invested in the development of standards that help incident response teams analyze and share information. FIRST Standards include the Common Vulnerability Scoring System (CVSS), a mechanism that incident responders can use to rapidly assess the impact of software vulnerabilities, and the Traffic Light Protocol (TLP). In addition, FIRST community members also work on machine sharing specifications, such as a protocol for exchanging Passive DNS information.

FIRST also enables incident response teams to connect to a threat intelligence sharing mechanism through a Malware Information Sharing Platform (MISP), which allows members to gain a first appreciation of connecting to a threat intelligence exchange.

Ongoing development of the CSIRT community

—

Leveraging investment in these building blocks, FIRST contributes to

build a more mature, and more integrated incident response community. We make these tools and mechanisms available both to our members, to help train their own team members, peer teams and partners who can help us bring these materials to a wider audience. In 2016, FIRST partnered with organizations such as LACNIC, ITU and AfricaCERT to train incident responders and help develop teams across the world.

Moreover, FIRST aims to help other communities, such as civil society and policy makers, to better understand and be comfortable interacting with Incident Response teams. In order to do so, FIRST has become a contributor to internet governance fora such as the IGF and the Global Conference on Cyberspace through their intersessional working groups, as well as in person participation.

By creating a well understood and capable incident response community, the internet community as a whole will be in a better place to respond to the next major incident. This capability will be an important element of ensuring the Internet can fulfill its full potential.

References:

[1] Kyle York (2016), Dyn Statement on 10/21/2016 DDoS Attack. Retrieved August 2nd, 2017 from <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>

[2] Reuters (2017), Cyber attack hits 200,000 in at least 150 countries: Europol. Retrieved August 5th, 2017 from <http://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX>.

GFCE and Meridian: Combining forces on CIIP

Critical Information Infrastructure Protection (CIIP) was a fashionable topic for governments when Meridian launched its international conference series in 2005, but CIIP has since been eclipsed by Cyber Security as the key subject on government agendas. Careful analysis, however, will show that CIIP is just as vital today, if not moreso, as critical services move online. It is therefore vital that Cyber Security Capacity Building does not neglect this crucial element in developing countries, particularly as it becomes increasingly difficult to implement CIIP successfully. GFCE and Meridian have combined forces to assist this challenging endeavour.

Written by: Peter Burnett, Meridian Coordinator

The historic setting of the 16th century Hostal de San Marcos in León was the birthplace for this initiative. It was conceived following the Meridian CIIP Conference, which was hosted by Spain in October 2015. The GFCE had played a major role in the event and the Meridian Steering Committee considered it a 'no-brainer' to invite the GFCE to collaborate with Meridian. A common cause was found on the issue of Critical Information Infrastructure Protection (CIIP), which Meridian has been promoting since its own birth in the equally historic setting of Greenwich, London, 10 years earlier. The aim of the GFCE-Meridian initiative was to draw

upon the established global network of knowledge and experience of the Meridian members, thereby stimulating new activities to enhance Cyber Capacity Building.

From León to Mexico City

A broad range of countries became involved in discussions on CIIP, and the first results were delivered in another historic setting at the 2016 Meridian Conference in Mexico City. The 1st product was a remarkably successful 'Primer Day' aimed at new delegates to help them get 'up to

speed' and feel comfortable engaging in the discussions and workshops of the main event - attended by 70% of the delegates. This was an optional session and included a description of the basic terminology and concepts commonly used in CIIP as well as an innovative ice-breaking session. It also involved panels of experts to introduce some of the key international organisations active in the CIIP field (such as the OAS, World Bank, and the GFCE), and a chance for delegates to ask another panel of experts about any aspects of CIIP.



MERIDIAN Community Members 2016

“It is also clear that, despite the ascendance of Cyber Security as a key topic on the agenda of every government, the subject of CIIP is still as important as it was 12 years ago ”

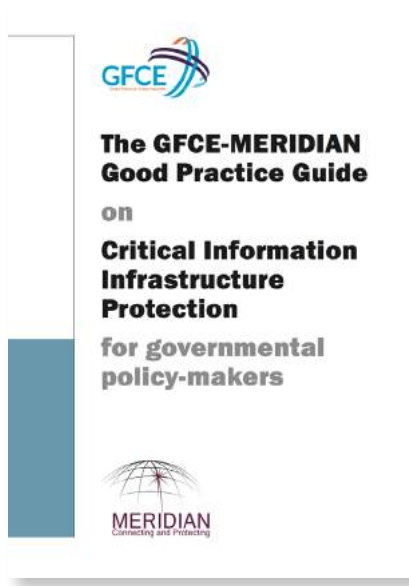
Identifying Good Practices

The 2nd deliverable of the Initiative was also aimed at new delegates and countries who are finding their way in the field of CIIP. This was a back-to-basics Good Practice Guide (GPG) to CIIP. It explains the fundamental principles and processes of developing a regime for Protecting the CII, from the precursors of Critical Infrastructure Identification, to the more advanced phases of monitoring and review, and information sharing. The Guide was designed to be brief and easy to read, to get a good overview of the elements, but it also has a well-researched list of references and further reading. It is freely available

to download from the GFCE- or the Meridian website (www.meridianprocess.org) and is considered essential reading for anyone involved in Cyber Capacity Building as well as CIIP.

Preparing for the Future

The GPG was launched and discussed widely at Meridian 2016 and some of the feedback from the more developed and developing countries was that there were some aspects that could benefit from a more in-depth discussion. These additional aspects reflect the challenges of keeping up with what is critical, against the background of a continuously



The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection

changing cyberspace, and how to maintain protection when services, some of them essential, are migrating towards digital and often offshore environments. These developments can undermine previous assumptions about what is critical and how it needs to be protected. This is just as much a challenge for the development of National Cyber Security Strategies, but when it comes to the CIIP, the stakes are very high; it is, by definition, the most important element of a nation's cyberspace, since it supports all critical services.

The evolution of terminology also needs to be kept under review, to ensure that the fundamentals of CIIP are still being addressed, even if new terms such as 'cyber resilience' come to replace CIIP. These will be discussed in a 'Next Steps' successor to the original GPG being developed for Meridian 2017, which will take place in Oslo on October 24th - 25th.

The CIIP Initiative has a 'Budd-

ying' programme, which is aimed at all Meridian countries, whether developed or developing, as it has a peer model as well as the more traditional hierarchical relationship pattern. This is being tested this year and will be further developed at Meridian 2017. Other elements of the Initiative include plans to develop a free-standing CIIP Training Package based on the GPG and the Primer Day, in conjunction with a UK Cyber Capacity Building project, which will trial it in Africa. Further developments of the Initiative are also under discussion.

Meridian & GFCE

There is no doubt that that the collaboration between GFCE and Meridian has been a great success so far, and has plenty of potential to go much further if the resources are forthcoming. It is also clear that, despite

the ascendance of Cyber Security as a key topic on the agenda of every government, the subject of CIIP is still as important as it was 12 years ago when Meridian was conceived. Consequently, the issue of CIIP will continue to have a key place in the GFCE portfolio.

More information:

Council of Europe/Global Project on Cybercrime 2013: Capacity building on cybercrime <https://rm.coe.int/Co-ERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6>

Council of Europe/European Union: GLACY project on Global Action on Cybercrime <http://www.coe.int/en/web/cybercrime/glacy>

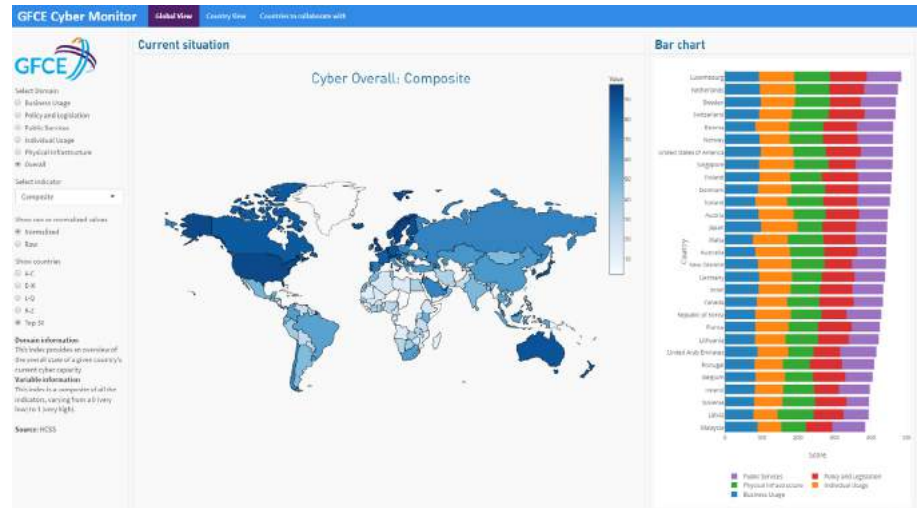
Council of Europe website on cybercrime www.coe.int/cybercrime

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



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



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

Colophon

Editorial board	Manon van Tienhoven (GFCE) Belisario Contreras (OAS) Panagiota-Nayia Barmaliou (EU) Souhila Amazouz (AU)
Guest editors	Kaleem Ahmed Usmani Jennita Appanah Appayya Johanna Vazzana Gonzalo García-Belenguer Mariana Cardona José Luis Ponce López Neil Walsh Tobias Feakin Damir Rajnovic Maarten van Horenbeeck Peter Burnett
Artwork & design	Ivonne Vivanco (OAS)
Chief editor (rotating)	Manon van Tienhoven (GFCE)

Publishers

African Union, www.au.int,
contact@africa-union.org, @_AfricanUnion

European Union, www.europa.eu,
SECPOL-3@eeas.europa.eu, @EU_Commission

Global Forum on Cyber Expertise, www.thegfce.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 5:
March 1st, 2018