Volume 1, June 2016

Global Cyber Expertise Magazine

Cybersecurity trends in Africa

Malware on 1 in 7 mobile devices
-page 4-

AFRICAN UNION

GFCE
Global Forum on Cyber Expertise

Organization of American States | More rights for more people

Volume 1, June 2016

Global Cyber Expertise Magazine

Editorial

“This Magazine offers cyber policymakers and stakeholders a forum to exchange experiences and stay up-to-date on latest developments”

Welcome to this first issue of the Global Cyber Expertise Magazine!

In the fast evolving field of cyber policies and capacity building this new Magazine offers policymakers and stakeholders a forum to exchange experiences and to stay up-to-date on latest developments. By utilizing the network and resources of some of the largest regional and global players the Magazine provides a unique inside perspective.

This first issue gives an overview of the current state of play around the world. Our cover story on Africa shows both the enormous economic potential of cyber and the risks cyber threats pose to this growth agenda (page 5). A similar message comes back in the articles about Latin America and the Caribbean with a call to action for states to invest in cybersecurity strategies and structures (page 13 and 16). The articles about Europe provide an overview of the latest EU policy instruments in cyber capacity building and international cyber policies (page 23 and 26). In his contribution a Malaysian Cybersecurity Official calls for a more regional approach to cyber capacity building in Asia (page 19). This first issue also demonstrates some inspiring experiences in cyber capacity building: workshops in Africa (page 8 and 10), best practices on Responsible Disclosure (page 33) and an interview with the director of the new CyberGreen initiative (page 21).

While you are reading this issue, we are already working on the next. We are very interested in your contributions! We are especially interested in experiences in cyber capacity building which might be useful to other global players and analysis of new policy initiatives (new legislation or strategies). Let us also know about your upcoming events (conferences, workshops, trainings) for a global audience which we can include in our future global agenda.

On behalf of the Editorial Board: enjoy reading!

Anne Blanksma Çeta

Cybercrime and Cybersecurity Trends in Africa

A new study by Symantec and the African Union provides a detailed analysis of the latest trends on cybercrime and cybersecurity on the African Continent. The report reveals both the economic potential of cyber in Africa with an estimated market value of 75 million USD in 2025 and the extent of cyber threats, especially with regards to mobile malware and money transfers. The report is based on a survey among African nations and a regional threat analysis. The study was conducted with support from the United States Department of State and has been adopted as an initiative within the GFCE community. The study will be presented during the next African Union Assembly session and made available via the GFCE website.

Written by: Ms. Cheri McGuire, Vice President of Global Government Affairs and Cybersecurity Policy at Symantec

Why cybercrime matters to Africa

Africa is a continent on the rise. It is growing quickly in terms of population, the economy, and global influence. Today, Africa is home to 1.21 billion people (up from just 800 billion in 2000), with a median age of just 19.5 years, the youngest population in the world. With this prominence of youth comes a diverse population that is looking for productive employment, social engagement, free expression, and increased global connectivity. While the downturn in world commodity prices has hit African economies hard, nearly every African nation is poised to grow over the coming years. Some will continue on a trajectory putting them among the fastest growing economies in the world. Technology adoption continues to rise as well, with mobile device ownership growing exponentially, social media use increasing, and the Internet of Things (IoT) quickly becoming a reality. Even the most conservative metrics show that Africa is poised to make great gains and help fuel global growth into the future. Along with this rapid economic growth comes a burgeoning e-commerce industry that is poised to expand to an estimated 75 billion USD by the year 2025.

With this growing prosperity and digitization however new risks and vulnerabilities arise that could undermine progress. Chief among these risks is the global rise of cybercrime. As the African Continent's economy moves online, citizens, their computer systems, and the Continent's information technology (IT) infras-

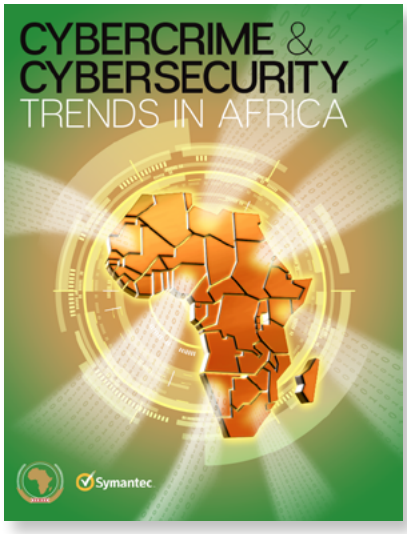
"More than one out of every seven mobile devices in Nigeria is currently infected with mobile malware"

tructure become enticing targets for an increasingly professional cadre of cybercriminals. The growth of cybercrime is by no means just an African problem. In fact, in 2013, the total global direct cost of cybercrime reached an estimated 113 billion USD. In South Africa alone, 73% of adults reported experiencing cybercrime, which is estimated to have cost the South African economy 337 million USD. Compounding the problem is the fact that many Africans are still using outdated, or in many cases pirated, software. Nearly one quarter of users in Africa are currently using the operating system Windows XP that was first released in 2001, and for which software patches were discontinued in 2014.

Understanding the Threat Landscape

In order for Africa to realize its full potential, policymakers will need to implement effective policies and awareness initiatives to stem the rising tide of cyber threats. Unfortunately, these same policymakers, technicians, and other experts have long noted the lack of detailed and reliable threat information regarding cybercrime threats in the region. Such information is invaluable in assessing and managing cyber risks by providing governments a more complete and nuanced understanding of how criminals and other actors are targeting and exploiting cyber-related vulnerabilities.

To help address this information gap, the African Union (AU) and Symantec Corporation, through the Global Forum for Cyber Expertise (GFCE) and with the support of the U.S. Department of State, are engaged in a public-private partnership to develop a report that collects and presents detailed policy and technical data on the state of cybersecurity in Africa. The research includes surveys sent to every African nation on current cyber capabilities and trends, as well as regional cybersecurity threat data from Symantec's Global Intelligence Network. Governments



The study by Symantec will be presented during the next African Union Assembly session and made available via the GFCE website www.thegfce.com

and other interested parties can utilize this information to identify gaps and to strengthen protection, prevention and response mechanisms to confront the diverse range of cyber threats. This report also will be an excellent opportunity for AU Member States to illustrate the significant advances and accomplishments in the areas of cybersecurity and combating cybercrime. Moreover, the results of the research will serve to guide future capacity building efforts for AU members.

The Threat of Mobile Malware

Initial findings from the AU-Symantec initiative indicate that due to the borderless nature of cybercrime, many of the trends we see globally also are affecting Africa, including the explosion of ransomware and social media scams, and the proliferation of new malware and website vulnerabilities. However, because of how the IT infrastructure is evolving in Africa, several of these cybercrime trends will become especially acute and pose a significant danger. Mobile malware, for instance, is a huge problem in Africa today and will continue to be a major threat into the future. Globally, the number of new vulnerabilities identified in mobile software grew a staggering 214% in 2014. Over the past decade, Mobile phone networks have transformed communications in Africa. Most importantly, mobile phones have allowed African communications networks to leapfrog the entire landline generation of development and go directly to the digital age. Globally, smartphones are an increasingly attractive target for cybercriminals who are investing in more sophisticated attacks that are effective at stealing personal data or extorting money from victims. The steady rise of mobile malware that mainly targets Android systems is also of concern given 89% of the smartphone market share in Africa runs on that platform. For example, according to Symantec data, more than one out of every seven mobile devices in Nigeria is currently infected with mobile malware. Africa also leads the world in money transfers using mobile phones, with 14% of all Africans receiving money through mobile transfers. And, with some of the world's largest mobile money transfer services, such as Kenya's Mpesa, cybercriminals will continue to heavily target mobile devices in Africa.

With a young population that is rapidly adopting new technologies, Africa is on the verge of an Internet boom. These advances also bring with them new risks. To keep pace, initiatives by African Nations should seek to combat cybercrime and improve their overall cybersecurity posture. It will take a concerted effort from governments in countries within and outside Africa, industry, and civil society to reduce cybercrime and improve cyber protection and resilience so that Africa can reach its full potential in the global economy.

More information:

GFCE Initiative 'Cybersecurity and Cybercrime Trends in Africa'

McKinsey Global Institute Report 2013, Lions go digital: The Internet's transformative potential in Africa

Pew Research Centre, April 2015, Cell Phones in Africa: Communication Lifeline

Symantec Internet Security Threat Report, Volume 21 2016

United Nations Conference on Trade and Development (UNCTAD), Information Economy Report 2015

United Nations Economic Commission for Africa, Policy brief 2014,Tackling the challenges of cybersecurity in Africa

African diplomats train to stand their ground in cyber negotiations

On the 15th and 16th of February 2016, the Capacity Building Workshop for Diplomats took place in Addis Ababa (Ethiopia) jointly organized by the African Union Commission (AUC) and ICT for Peace foundation (ICT4Peace). The workshop aimed to promote confidence in the use of ICTs among African diplomats and was focused on international cybersecurity consultations and negotiations. It was attended by 45 diplomats and government officials involved in foreign policy development and/or cybersecurity diplomacy from 28 African Countries, as well as representatives from three regional and specialized organizations of the African Union.

Written by: Ms. Souhila Amazouz, Senior Policy Officer, Information Society Division, Infrastructure and Energy at the African Union

Unlocking prosperity and freedom

The workshop provided an introduction to the subject of international cybersecurity policy and current consultation and negotiation efforts, and was an opportunity for the participants to be exposed to the context in which cybersecurity is being addressed in global and regional forums – notably, the United Nations Group of Governmental Experts (UNGGE), the Organization for Security and Cooperation in Europe (OSCE) and the Global Conference on CyberSpace (GCCS). The workshop familiarized African diplomats with the ongoing international discussions in order to help them acquire a deeper understanding of the most important areas of diplomatic negotiations for a secure and open cyberspace, such as the application of the international laws for the cyberspace, norms of responsible state behavior as well as confidence-building measures (CBMs) in cyberspace.

Addressing the participants, Mr. Moctar Yedaly, Head of Information Society Division, Infrastructure and Energy at the African Union Commission, underlined the importance of such workshops for Africa and policymakers. He argued that digital technologies and the Internet are the backbone of our society and economies. He said that "Digital technologies are key enablers of prosperity and freedom". As African countries expand their access to Internet networks information systems, they are increasingly vulnerable to cyberattacks.

Participants to the Cybersecurity Policy and Diplomacy Workshop for African Countries

Investing in cyber capacity building

In his address, Mr. Daniel Stauffacher, President of the ICT4Peace foundation, stated that over the past five years states have become increasingly engaged in regional and international policy discussions and debates over cybersecurity issues. He also highlighted that we are now living in a world of hyper-connectivity and that many countries have already placed cybersecurity or information security under their national security agenda. The workshop on cyber diplomacy was part of a series of capacity building workshops that ICT4Peace is organizing for diplomats to develop capabilities for international negotiations.

The participants agreed on crucial measures, including the importance of developing national cyber strategies, fostering domestic and regional coordination, developing Computer Security Incident Response Teams (CSIRTs), and signing and ratifying the African Union Convention on Cybersecurity and Personal Data Protection.

Mr. Daniel Stauffacher President of the ICT4Peace foundation (left) and Mr. Moctar Yedaly Head of Information Society Division, Infrastructure and Energy at the African Union (right)

More information:

The African Union Convention on Cybersecurity and Personal Data Protection

Regional Expert Meeting on Cybersecurity in West Africa

From 12 to 13 April 2016, a regional meeting on Cybersecurity in West Africa was held in Dakar, initiated by the Government of Senegal and the Kingdom of the Netherlands, in partnership with the United Nations Office on Drugs and Crimes (UNODC). The event was attended by approximately 200 national, regional and international experts and focused on the main theme "Awareness and experience feedback on cybersecurity." The meeting took place as part of the GFCE initiative 'progressing cybersecurity in Senegal and West Africa'.

Written by: Ms. Thiam Ndèye Fatou Coundoul, Technical Computing Advisor at the Ministry of Post and Telecommunications of the Republic of Senegal

Cyber awareness among West African decision makers

The regional meeting, placed under the patronage of his Excellency the Prime Minister of Senegal, Mr. Mahammed Boun Abdallah Dionne, was opened by Doctor Yaya Abdoul Kane, Minister of Post and Telecommunications, who expressed the pride of Senegal to host this important meeting, as well as the readiness of his country to provide all things necessary for a safe, secure, and free Internet.

Professor Abdallah Cissé, legislative drafters and specialist in cyber law, opened the meeting with an inaugural lecture on opportunities and threats in cyberspace. He sensitized authorities and meeting participants present on the importance of cyber awareness-raising efforts, especially among West African decision makers. He argued that African countries are highly vulnerable to cyber threats and, therefore, need to get involved in cybersecurity initiatives to ensure and promote confidence in cyberspace. Mr. Cissé highlighted the urgent need for ratifying regional legal instruments within an operational and strategic approach, such as the Malabo and Budapest Conventions, as well as implementing a set of measures that could promote the attainment of opportunities in cyberspace, but also to support initiatives in the fight against cybercriminals.

On the theme dedicated to national cybersecurity strategies, the presentation on cybersecurity referenced situations in Senegal and Burkina Faso, showing the urgent need for (West) African countries to consider cybersecurity as a priority in national development policy. Several activities and specific actions have been conducted and organizations' been founded; however, coordination, leadership and capacity building in cybersecurity capabilities are still insufficient.

Other topics such as the development of Computer Security Incident Response Teams (CSIRTs), legislative frameworks, education and cyber awareness were debated among experts and the general audience. Attendees to the meeting comprised a wide

Opening session with Mr Pierre Lapaque (UNODC Regional Representative on West- and Central Africa), H.E. Mr. Sherif Bodian (Minister of ICT in Gambia), H.E. Dr. Yaya Abdoul Kane (Ministry of Post and Telecommunications of the Republic of Senegal), H.E. & Theo Peters (Ambassador of the Netherlands in Senegal) and Prof. Abdallah Cissé

swath of West African stakeholders, including many participants from the public and private sectors, civil society, NGOs, academics and the security and justice sector.

Recommendations

The "Dakar Declaration on Cybersecurity," based on the recommendations during the expert meeting, will be drafted in the coming months. The main recommendations included:

1. The need to assist African countries in their efforts to implement national cybersecurity strategies;
2. The sustainability of this regional meeting, in rotation within the Economic Community of West African States (ECOWAS) countries initially and the whole of Africa later, for improved awareness of opportunities and threats in cyberspace;
3. The need for harmonization of legal frameworks through the channel of Community texts of ECOWAS, but also based on the implementation of cooperation through regional legal instruments such as the Malabo and Budapest Conventions;
4. The creation or maturation of efficient CSIRTs in Africa, and the relevance of the definitions of roles and missions clearly documented in procedure manuals, with a view to strengthen the ability of crises-management procedures and to build a culture of trust among CSIRTs, calling for more cooperation, colla-

Group photo of the speakers and organizers of the Regional Expert Meeting on Cybersecurity in West Africa

Plenary room of the Regional Expert Meeting on Cybersecurity in West Africa

boration, coordination and complementarity;

5. With regard to education and expertise, the need to have their own area of specialization specific to the security needs of the digital industry; hence, the states are called to reflect the promotion and integration of new sectors in education while ensuring the harmonization of cybersecurity trainings;
6. Finally, the development of a culture of digital trust and secure Internet use, through awareness and strengthening cybersecurity capabilities, especially towards investigators and security teams, child online protection, specialization of teachers, sharing best practices on cybersecurity and public-private partnership .

More information:

African Union Convention on Cybersecurity and personal data protection

Budapest Convention on Cybercrime

ECOWAS Directive on Fighting against Cybercrime adopted by the ECOWAS Council of Ministers on 19th August 2011 in Abuja, Directive C/DIR. 1/08/11 on Fighting Cyber Crime Within ECOWAS

ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection

ECOWAS Supplementary Act A/SA.2/01/10 on Electronic Transactions

GFCE Initiative progressing cybersecurity in Senegal and West Africa'

Latin America and the Caribbean: climbing the cybersecurity ladder

The fast-evolving integration of cyberspace into the daily lives of the people in the region and countries' critical infrastructure offers numerous social and economic opportunities. It also poses significant challenges, particularly for countries with nascent digital economies. Latin America and the Caribbean are experiencing an Internet boom, with a growth of 1,808.4 percent in the last decade alone (source: Internet World Stats). Yet 45% of the region's population is not yet online and significant investments in broadband and infrastructure will be required for the region and its population to more fully reap the benefits of the digital economy. It is estimated that a 10% increase in broadband penetration in the region could boost GDP by an average 3.2% and increase productivity by 2.6% (source: IDB).

Written by: Mr. Alfred Schandlbauer, Executive Secretary, Inter-American Committee against Terrorism, Organization of American States

Risks to data integrity, availability and confidentiality

Based on a survey on cybersecurity and critical infrastructure conducted by the Organization of American States (OAS) and the cybersecurity company Trend Micro in 2015, 53 percent of respondents noticed an increasing tempo of attacks on their computer systems, and 76 percent stated that cyberattacks were getting more sophisticated. The risk to data integrity, availability and confidentiality could negatively affect the productivity and economic growth of a region that is still struggling to propel itself into the digital age. A digital economy can only flourish in an open, stable and secure environment trusted by its users; hence, it is critical that ICT investments are matched with similar investments in cybersecurity. The latter requires a comprehensive approach, ranging from technological investments to policies aimed at fostering a culture of digital safety.

Bearing this in mind, the OAS, in collaboration with the Inter-American Development Bank (IDB), recently published a comprehensive report on the state of cybersecurity preparedness in the 32 countries of Latin America and the Caribbean entitled: 2016 Cybersecurity: Are We Ready in Latin America and the Caribbean?

Cybersecurity: Are we ready in Latin America and the Caribbean 2016

Cyber readiness across five dimensions

The report provides an in-depth assessment of the cybersecurity capabilities of the countries of the Western Hemisphere, based on the Capability Maturity Model (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. That model, employed for the first time in the world in this study on Latin America and the Caribbean (LAC), provides analysis based on five dimensions: (i) National Cybersecurity Policy and Strategy; (ii) Cyber Culture and Society; (iii) Cybersecurity Education, Training and Skills; (iv) Legal and Regulatory Frameworks; and (v) Standards, Organizations and Technologies. Each dimension encompasses a number of indicators, which are graded according to five "maturity" levels, from an initial stage of maturity –in which a country may have just started discussing cybersecurity matters– to a stage in which a country is able to rapidly adapt to changes in the cybersecurity landscape.

By indicating the level of cybersecurity maturity in these different dimensions, our study highlights current advances in 32 LAC countries, as well as insights with respect to prioritizing cybersecurity investments, providing national stakeholders with a complete understanding of their country's cybersecurity situation.

The report concludes that of the countries in the region, Argentina, Brazil, Chile, Colombia, Mexico and Uruguay have relatively more developed cyber regimes. However, despite having fewer resources to direct at the issue, the Caribbean and Central American countries are as advanced in their legal frameworks. Overall, Latin American and Caribbean countries have made significant efforts in updating domestic legislation to combat cybercrime. Despite these advances, though, procedural cybercrime legislation requires reform to allow for the adequate prosecution of cybercrimes. Likewise, privacy and data protection frameworks could be improved and benefit from the participation of civil society actors in this discussion.

Similarly, Brazil, Colombia, Mexico and Uruguay perform strongly in the areas of developing a cyber culture and educating their populations about its importance. Other countries in the region could benefit from greater investment in those areas. To that end, governments, the private sector, and civil society should work together to increase national awareness of cyber risks and the potential impact of cyberattacks. Public-private partnerships must be formed and utilized to gain better understandings of each country's urgent needs in the marketplace as it relates to cybersecurity. An early introduction of computer science and information security courses at all levels of the education system throughout the hemisphere would better prepare the next generation workforce.

Observatory of Cybersecurity in Latin America and the Caribbean

A need for national cybersecurity strategies

The two least developed of the dimensions examined by the survey for the entire LAC region were "Policy and Strategy" and "Technologies," With the latter dimension being essential to ensure the resilience of national critical infrastructure against cyberattacks. To strengthen that dimension, many countries would benefit from inventories of their essential services, critical assets and critical information infrastructure in terms of cybersecurity for the purposes of conducting risk assessment and implementation of mitigation measures. Many countries in the region, particularly in the Caribbean, have yet to create and implement national Cyber Security Incident Response Teams (CSIRTs), which are essential to coordinate incident response at the national level and to serve as points of contact for international incidents.

Finally, slow implementation and development of well-coordinated critical cybersecurity policies in the region significantly affects maturity levels in the "Policy and Strategy" dimension. In many cases this is attributable to an unclear governance structure to address cybersecurity at the national level. A clear coordination structure for cybersecurity is one of the first steps a country must take to move further up the cybersecurity ladder. This also allows progress in the other four dimensions; as such a structure would clarify lines of action and the roles that must be played by the different stakeholders to strengthen national cybersecurity.

We believe reports of this nature are important to provide a comprehensive understanding of not only the challenges and gaps in cybersecurity, but also the opportunities and strengths that each country can explore to continue to improve its cyber capacities. In particular, it is our view that this report contributes to the cybersecurity literature by providing a more complete perspective of the LAC region. Given the dynamic nature of cybersecurity, the reapplication of the model utilized in our report on a periodical basis is critical to verify the region's improvements and assess what still needs to be done.

More information:

2016 Cybersecurity: Are We Ready in Latin America and the Caribbean?

Report on Cybersecurity and Critical Infrastructure in the Americas" (2015)

Internet World Stats

Inter-American Development Bank (2012): Bridging Gaps, Building Opportunities

A Latin America and Caribbean's view on national cybersecurity strategies

There is always a dichotomy as to what should be included in a National Cybersecurity Strategy (NCSS) with the discussion often hinging on whether it should be called a Policy or a Strategy. Globally, there are over 70 national cybersecurity strategies publicly available; in Latin America and the Caribbean a total of 4 have been approved and 6 are in various stages of development. These strategies have been called various names, such as National Strategy for Cyber and Information Security (Denmark) or Programme for the Development of Electronic Information Security (Cyber Security) for 2011-2019 (Lithuania).Some countries have taken another approach and have also included cybersecurity components in their national security strategies, such as Russia (2013) and Denmark (Denmark Defense Agreement 2013-2017).

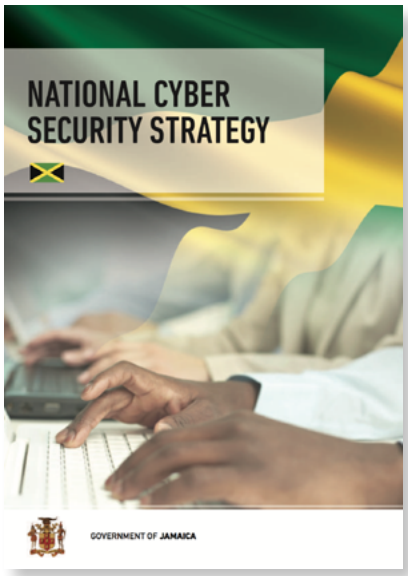
Written by: Ms. Kerry-Ann Barrett and Ms. Barbara Marchiori de Assis, Cybersecurity Program at the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States (OAS)

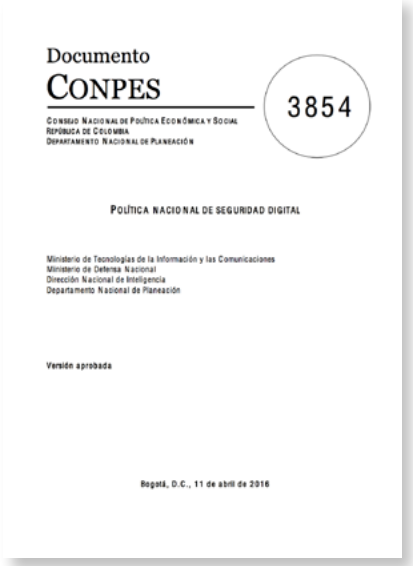
Key ingredients of a National Cybersecurity Strategy

In terms of what should be included in an NCSS, several common themes have been covered globally, such as:

a. Governance Frameworks (e.g., national coordination)
b. Legal Frameworks (e.g., Cybercrime legislation and publication of technical standards)
c. Public Awareness Raising (e.g., national or sector specific campaigns)
d. Technical Capability/ Capacity-building (e.g., establishment of a national CSIRT, critical infrastructure protection, and academic programs)
e. Public-Private Partnerships and International Cooperation (e.g., information sharing arrangements)
f. Defense and Cybersecurity (e.g., establishment of a national command cyber defense center)

Finally, the development of a culture of digital trust and secure Internet use, through awareness and strengthening cybersecurity capabilities, especially towards investigators and security





Left: Jamaica's National Cybersecurity Strategy (2015)

Right: Colombia's National Digital Security Policy (2016)

teams, child online protection, specialization of teachers, sharing best practices on cybersecurity and public-private partnership. Many countries have also recognized the need to separate the roles for strategy development and operational response. For example, in Australia, there is the Cyber Security Policy and Coordination Committee, which is an interdepartmental committee that coordinates the development of cybersecurity policy for the Government, determines priorities and is responsible for international collaboration, while on the technical side there is both a. CERT Australia, which is the national coordination point for the Australian Government for provision of cyber security information and advice, and b. the Cyber Security Operations Centre (CSOC). Using Colombia as an example for the LAC region, policy is determined by the National Council of Economic and Social Policy, which usually approves what is known as the 'CONPES' (i.e. a high-level policy document that provides guidelines on socio-economic strategic issues for the country), while the Colombian Cyber Emergency Response Team (ColCERT) is a response mechanism for organization-specific cyber incidents.

Action and implementation

The approach of the Organization of American States (OAS) General Secretariat has been to prevail upon our member states to recognize that once a high level policy directive is given regarding cybersecurity, there must be an associated strategic plan of action to achieve that directive and its goals. The process for its development should always involve all relevant stakeholders (government, private sector, civil society, academia, et al.) and culminate in a document that is clear in its scope, addresses specific national threats, and articulates clear goals, objectives, as well as the steps needed to achieve those goals in light of identified priorities and indicators to measure progress. In relation to its implementation, once approved, the associated costs and available resources must be identified and included in the budgets of implementing agencies or entities.

The development process for NCSS in the LAC region has shown promising prospects, as each country has recognized the need to have a structured and coordinated approach to developing their NCSS. When requesting the support of the OAS General Secretariat to develop an NCSS, each member state is asked to establish a national multi-stakeholder working group to be part of the development of the strategy and to open a roundtable dialogue on the specific cybersecurity challenges facing their country. This open dialogue also facilitates feedback during the drafting stages of the document.

The challenges of ownership and sustainability

The experience in LAC, however, has not been without challenges.

There are so many factors external to the development process that affects its success. The identification of an owner/owners for the development and implementation of the NCSS, change in the national priorities as a result of unforeseen events such as a national disaster or change in Government, competing agencies vying for leadership, economic constraints, failure to obtain executive buy-in, among others. On the other hand, we have seen some uncommon and unprecedented approaches that have augured well for sustainability. For example, in one member state, the draft NCSS was shared with opposition parties before approval and their input and comments were taken into account, which aided in the document being approved seamlessly. In another, the directive to review the cybersecurity situation was given from the level of the Presidency. This ensured coordination of the process with all stakeholders, timelines being met and, ultimately, development and approval within a year of the process's beginning.

In this context, it is still undeniable that NCSS are critical documents for coordinating national efforts to combat a threat that has international impact. The NCSS can only be successful if identified as an area of priority at the national level with a dedicated and well-resourced champion. This is particularly challenging in the LAC region, where countries are still struggling to achieve economic stability and increase Internet penetration. When countries are faced with pressing social and economic issues, it is only natural that an investment in cybersecurity risk reduction is placed on the backburner. Investment in the Internet contributes to economic growth and social development, and if the Internet is to reach its full potential in this regard, it must be secured. Therefore, it is imperative that cybersecurity be considered at the onset.

More information:

ENISA's National Cyber Security Strategies (NCSSs) map

ITU's National Security Repository

The lack of cybersecurity capacity building frameworks in Asia

Written by: Dr. Amirudin Abdul Wahab, Chief Executive Officer at Cybersecurity Malaysia, the National Cybersecurity Centre under the Ministry of Science, Technology and Innovation (MOSTI) in Malaysia (http://www.cybersecurity.my)

Asian nations are experiencing rapid development of ICT and are dealing with various cybersecurity threats on government computer network and critical sectors. According to the FireEye Advanced Threat Report for the Asia Pacific, Advanced Persistent Threat (APT) activity was consistently high in South Korea, Taiwan, Hong Kong and Japan during the first six months of 2014, which contributed to more than 80% of the total APTs in the region. The region was 35% more likely to be targeted by advanced cyberattacks compared to the global average. A customized regional capacity-building initiative for Asia is therefore crucial; however, a well-defined framework that focuses on Asian cybersecurity capacity building has yet to be developed.

Cyber capacity building via ASEAN

The issues of capacity building have been addressed in several discussions at the ASEAN Regional Forum (ARF). The Council for Security Cooperation in Asia Pacific, through its Memorandum No. 20 entitled "Ensuring a Safer Cyber Security Environment" has recommended ARF to implement capacity-building and technical-assistance measures. It re-

commended that priority should be given to strengthening cybersecurity crisis management in all states.

The ASEAN ICT Master Plan 2015 that was launched in 2011 provides a framework for the development of Information and Communication Technology (ICT) within the ASEAN region. It stated that the strategic thrust of human-capacity development is to develop competent and skilled human capital in ICT. The development of ICT Skill Standards definition and certification in information-system and network security has been initiated as one its prioritized projects. ASEAN has also established the ASEAN Network Security Action Council to establish a common framework for network security that includes capacity building and training programs for national CSIRTs.

Avenues for cooperation on cyber capacity building in Asia

Currently, a holistic cybersecurity capacity building initiative that can be deployed across the region within Asia is not available. The creation of an Asian platform for security cooperation should be an option to consider as Asian countries share common values, cultures and norms which are appropriate in cybersecurity capacity building collaboration. Existing capacity-building programs are not congruent to and streamlined with regional interests that share common cultural values and security interests. A holistic framework for cybersecurity professional certification is therefore required to address the needs in developing and nurturing expertise as well as technical know-how in cybersecurity human capital in the region, as well as enabling private-public partnerships, multi-level collaboration and creating skills pathways for the growth of the cybersecurity industry.

The Global Accredited Cybersecurity Education

Malaysia has established the Global Accredited Cybersecurity Education (ACE) Scheme, which is currently in the development stage. Interested parties can submit their interest to participate as a development team member. The objectives of the Global ACE Scheme are as follows:

1. To create a world-class competent workforce in cybersecurity;
2. To establish a professional certification programme that is recognized by the government, private sector, industries and NGOs within the OIC countries;
3. To promote the development of cybersecurity professional programmes within the region;
4. To provide cybersecurity professionals with the right knowledge, skills, abilities and experience;
5. To ensure that accredited personnel are independently assessed and committed to a consistent and high-quality service level;
6. To be the cybersecurity professional training centres/programme for OIC countries and ASEAN.

The development of skilled cybersecurity professionals cannot be attained overnight. It will take time to get the right people into this profession. To address the human capital gap requires a combination of strategic public-private collaboration and incentives from various parties, such as scholarships, mentorships or internships to guarantee employment. We need to create a knowledge generation capable of fending off the ever-evolving cybersecurity threats. Last but not least, we need to truly produce high-value and skilled digital citizens of the future that will keep our cyberspace safe as we head into a new digital economic order.

More information:

ASEAN ICT Master Plan 2015

Council for Security Cooperation in the Asia Pacific, Memorandum No. 20, Ensuring A Safer Cyber Security Environment

Interview with Yurie Ito, Executive Director of the CyberGreen Institute

Diagnosing and curing internet deceases

"The world needs to take a public health approach to cybersecurity"

Written by: Mr. Anne Blanksma Çeta, Senior Advisor at the Secretariat of the Global Forum on Cyber Expertise

Yurie Ito is Director of the Global Coordination at Japan's National Computer Emergency Team (JP-CERT/CC) and leads the CyberGreen Initiative to mitigate cyber diseases and improving Internet healthiness through measurement and global collaboration. CyberGreen enables a global community of organizations that gather and measure cyber risk conditions such as computer infections and vulnerable network nodes. Based on these metrics and mitigation practices, CSIRTs, ISPs and web hosts are able to clean systems and mitigate vulnerabilities. During the GFCE Annual Meeting in June, Cybergreen will be proposed as a GFCE initiative.

Q: How did the CyberGreen initiative come about?

"During my days as Director of Global Coordination JPCERT/CC and while serving as Chair of the Asia-Pacific CERTs (APCERT) Forum, I became convinced the world must take a public health approach to Cybersecurity.

Our traditional law-enforcement and security perspectives are necessary, but it is even more important that we view the Internet as a community with health concerns just as in the physical world. When viewed as such, clear responsibility lies with all stakeholders, not only CSIRTs but also service providers, vendors, policy and budget makers, employers and users to take steps to ensure cyber health.

Based on this vision, CyberGreen seeks to provide a trusted and neutral international body to collect and share cross-comparative measurements and best practices on mitigation. This also improves decision making about the allocation of international and national resources to identify and treat the parts of the Internet most at risk."

Q: Are you diagnosing and curing cyber diseases?

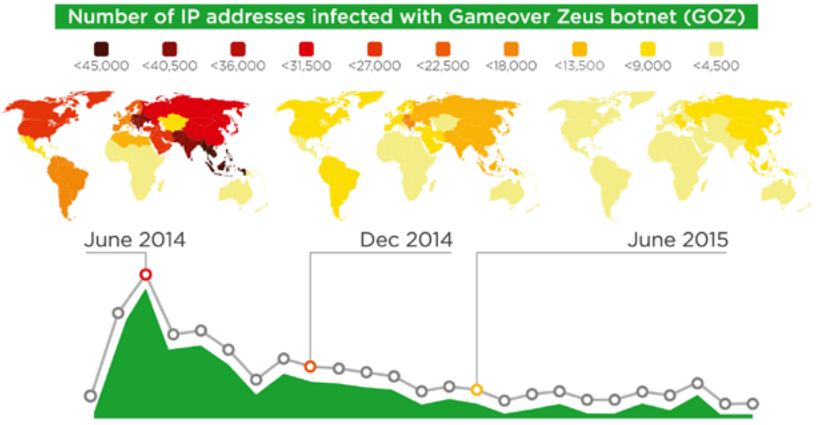
"We are not only focused on curing the symptoms of diseases; we analyze the root causes of cyber diseases and address the systemic level of underlining environmental problems. The Internet has become an infested swamp, fenced off with firewalls that do little to prevent users from visiting malicious sites and exposing their devices to infection and compromise. If policymakers want to do a better job of making the Internet healthier in terms of safety and resiliency, they need a better understanding of what the dangers are and where they are hiding.

As with any infectious disease, malware will continue to spread through contact unless concerted steps are taken to drain the root cause of untreated swamps and deny malicious actors freedom of movement."

Q: How does it work?

"CyberGreen's experts have worked hard to develop metrics that are technical in nature but give non-technical decision makers accurate, easy-to-understand metrics that measure the health of the Internet ecosystem. Primarily, we measure levels of infection and the existence of various types of vulnerable nodes that enable malicious activity. During our initial phase of operation, we began the task of defining those metrics as well as finding sources around the world from which to aggregate risk data necessary to populate them.

A good example is the way the Internet community fought the Gameover Zeus Botnet (GOZ) in 2014 and 2015. Through an international collaborative effort, hundreds of thousands of computers were cleaned of infection to prevent further spread of GOZ. CyberGreen's ability to measure and track the spread of root cause conditions and measure progress as we mitigate will facilitate the operational cleanup of systems. Policy development and capacity building will also have the insight to focus on the reduction of systemic risk conditions. The risk condition data are from proven sources with 10+ years of remediation history, such as from the Shadowserver Foundation.



(Data provided by The Shadowserver Foundation)

Q: Why is it important?

"The key is transparency. Evidential data, cross-comparable robust metrics and measurement reveal the sources of systemic risk conditions and foster improvement.

We need a common understanding of cyber health and risks through a widely accepted way of measuring national, service provider, and enterprise cyber health and risks. A common understanding and insight will enable global policy development and capacity building focused on the reduction of systemic risk conditions."

Q: Why do you want to go global with this initiative?

"Worldwide cyber health varies by region and enterprise – some are doing well, but there are many vulnerable and compromised computer and network devices. However, we don't know how much risk we are exposed to, neither globally nor by country or service provider.

You cannot protect yourself by only securing your internal systems. Your customers, peers and business partners are all connected globally, and they might be compromised and used to launch attacks without their knowledge. Therefore, this mitigation initiative needs to be global.

We need to build international norms and social responsibility around cyber ecosystem health improvement. The mission and mindset to improve Internet health needs to become the measure of cyber sophistication and stewardship for individuals, organizations and nations."

More information:

About the Cybergreen initiative:
www.cybergreen.net

EU international cyber policy: promoting a free and secure global cyberspace

Since the adoption of the EU Cybersecurity Strategy in 2013, the EU has invested heavily in cyber stability and resilience internally and globally. Many new EU policy initiatives have advanced cybersecurity of companies and public organizations within the EU. The European Cybercrime Center was established to facilitate cooperation in fighting cybercrime, and new European legislation will take effect in 2016 to improve the cybersecurity of critical infrastructures. Internationally, the EU is promoting a free and open cyberspace, where norms and existing international law should apply. In recent years, the EU has launched many cyber capacity building programmes to address cybercrime and cyber threats globally.

Written by: Ms. Heli Tiirmaa-Klaar is Head of Cyber Policy Coordination at the European External Action Service (EEAS) of the European Union

EU commitment to cyber capacity building

Cyberspace is growing exponentially. Fast growth and technological development will shape this new global policy area for decades to come. The number of Netizens will double over the next 5 years, soon to reach 5 billion. A vast majority of these new Internet users will come from Asia, Africa and Latin America as European countries, the US and Japan are nearing their maximum saturation point for Internet connectivity. In the background of these dynamics, industry reports claim that there is a global shortage of 1 million cybersecurity experts. That is why in parallel to internal cyber resilience, the EU invests in international cyber cooperation and has included cyber policy issues into the European Common Foreign and Security Policy agenda. Part of this approach includes the EU's membership in the Global Forum of Cyber Expertise (GFCE) and its commitment to global cyber capacity building.

EU achievements in international cyber cooperation include the launch of cyber dialogues with many EU key strategic partners – the US, Japan, South Korea, India and China. A new dialogue with Brazil will soon begin. In addition to dialogues with strategic partners, the EU is also holding regular cyber consultations with other international organizations.

Cyber capacity building in developing and transitioning countries is high on the EU agenda. An increasing share of EU development assistance funds will address cybercrime and

Launch of the EU Cybersecurity Strategy in 2013 by EU Commissioners Neelie Kroes (Digital Agenda), Catherine Ashton (Foreign Affairs and Security Policy) and Cecilia Malmström (Home Affairs)

cyber threats globally. Since 2013, the EU has launched several global projects to advance cybersecurity and fight cybercrime.

Cyber diplomacy

In January 2015, the EU Member States adopted the Council Conclusions on Cyber Diplomacy. This document established major policy guidelines for developing EU international cyber efforts. As a cornerstone of cyber diplomacy, the EU will continue to promote the understanding that there is a need to apply laws and norms in cyberspace. The EU has supported the international discussions on developing norms of responsible state behavior. Agreed international rules will help to enhance transparency and predictability of state behavior in cyberspace. Several reports of the UN Group of Governmental Experts in cyber security have agreed on norms such as refraining from attacks against critical civilian infrastructure, cooperating during cyber incidents and not engaging in malicious cyber activities against Computer Security Incident Response Teams (CSIRTs).

One of the major achievements in international cyber policy has been the development of cybersecurity confidence-building measures, where the EU has played an important coordinating role in the Organization for Security and Co-operation in Europe (OSCE) discussions. Two sets of OSCE cyber confidence building measures will address how to increase transparency and cooperation between states. There is a key role for regional organizations in this field as they provide a forum for neighbors to talk and, ideally, resolve their grievances. Such mechanisms can help resolve any incipient disputes, reducing the danger of escalating tensions over hostile cyber action. The EU also supports cyber confidence-building measures between the Association of Southeast Asian Nations (ASEAN) Regional Forum members.

The Internet should remain free, open and secure

As an important element for cyber diplomacy, the EU is of the opi-

nion that the Internet should remain a free and open platform accessible to all. The Internet is governed by a model in which the private sector, civil society and governments all are engaged and feed in with their expertise. The EU High Representative for Foreign Affairs and Security Policy, Ms. Frederica Mogherini emphasized this EU commitment to a free, open and secure Internet during the Global Conference on Cyberspace in 2015: "We are working to provide a better life for future generations, where the safe and peaceful use of technology facilitates the free flow of information and ideas."

States are also bound by international legal obligations related to Human Rights. State behavior should follow the long established principles of existing international human rights law, such as the legal obligations enshrined in the International Covenant on Civil and Political Rights, and other human rights laws. To protect freedom of expression online, the EU Foreign Affairs Council adopted EU Human Rights Guidelines "on freedom of expression online and offline" in 2014.

The EU will continue its efforts to improve security and freedom in cyberspace.

More information:

CISCO Annual Security Report 2014

Council Conclusions on Cyber Diplomacy

EU Cyber Security Strategy

EU Human Rights Guidelines on Freedom of Expression Online and Offline

OSCE Cyber Confidence Building Measures

EU High Representative for Foreign Affairs and Security Policy, Frederica Mogherini, and Dutch Foreign Minister, Bert Koenders, during the Global Conference on CyberSpace 2015 in The Hague

The EU experience in global cyber capacity and institution building

In recognizing the intersection between cyber resilience and development, the EU has defined cyber capacity building in third countries as a strategic building block of its 2013 Cybersecurity Strategy. Based on lessons learnt from traditional development cooperation and its internal experience and best practice, the EU has tailored a cyber capacity building model that aims at increasing the cyber resilience of partner countries while integrating a multistakeholder and rights-based approach. The challenges are numerous, as are the needs, and require innovative, cross-sectoral and integrated cooperation.

Written by: Ms. Panagiota-Nayia Barmpaliou, Cybersecurity and Organised Crime Programme Manager at the Directorate General for International Cooperation and Development of the European Commission

The intersection of cyber resilience and development

Two thirds of Internet users live in the developing world where access to the Internet is growing almost four times faster than in developed countries. Broad ICT strategies are rolled out especially by developing nations which seek to reap the digital dividends. The importance of ICT as an enabler for sustainable development and a means for governance accountability has been long recognized by the development community and further confirmed in the 2030 Agenda for Sustainable Development.

In recent years this process has been accompanied by increased awareness of the need to have a safe and secure underlying digital environment, or cyberspace. Threats posed by malicious cyber activities, such as cybercrime and attacks to digital services and infrastructure, or accidental failures, demonstrate that the economic and social benefits of ICT cannot materialize in a vacuum. Instead, the incorporation of cyber resilience aspects is a prerequisite for any such effort to be constructive and sustainable.

Anchored in its development cooperation commitments, the EU has recognized the need to foster open and prosperous societies through cyber capacity building measures in third countries that pursue a whole-of-government approach and enable citizens to fully enjoy the social, cultural and economic benefits of cyberspace. The EU started its programmatic approach by supporting justice sector reforms in the fight

European Commission – EU Institute for Security Studies International Conference on Cyber Needs and Development, 23-24 February 2015, Brussels, Belgium (Credits: © Bernal Revert)

against cybercrime in the Western Balkans in 2010 and a year later also with Eastern European partners in joint programmes with the Council of Europe. Building on this experience, the EU commenced a comprehensive cyber-specific capacity building engagement at a global level following the adoption of its 2013 Cybersecurity Strategy.

The EU experience and approach

The EU has tailored a cyber capacity building model that integrates its internal experience with lessons learnt from traditional development cooperation. The EU approach is based on the EU Member States' internal experience to enhance their cyber capabilities and best practice identified with the support of the European Cybercrime Centre (EC3) at Europol and the European Union Agency for Network and Information Security (ENISA). The EU's support focuses on:

- Facilitating the development or reform of appropriate regulatory and legal frameworks in compliance with international standards and in a manner that fosters greater international cooperation. In this context, the EU is committed in promoting the Budapest Convention on Cybercrime as the international legal framework of reference in the fight against cybercrime;
- Enhancing the capacities of criminal justice authorities, such as law enforcement, prosecutors and judges, in order to enable them to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence;
- Supporting the development of organizational, technical and cooperation mechanisms that increase cyber resilience and preparedness, such as: facilitating the development of national cybersecurity strategies, promoting effective inter-institutional, inter-agency and international cooperation as well as public-private exchanges and setting up functional national Computer Emergency Response Teams.

In order to pursue effective institutional and administrative cyber reforms and increased operational capacities of third countries, the EU draws on the overall aid effectiveness agenda and its experience in actions that are at the heart of the security-development nexus. The criteria used are: local ownership, transparency and accountability, result orientation, inclusive partnerships in the pursuit of sustainability and the application of an overarching rights-based approach.

Given the considerable disparities in the level and maturity of Internet, telecommunication, ICT infrastructure and criminal justice capabilities across countries, a tailored and demand-driven approach is necessary to address their divergent needs. Any engagement needs to be formulated around the three dimensions that form the tenet of any comprehensive cybersecurity conceptual framework: the adoption and implementation of a comprehensive set of policy, organizational, and technical measures that will increase their cybersecurity preparedness, following a multi-stakeholder and human rights compliant approach.

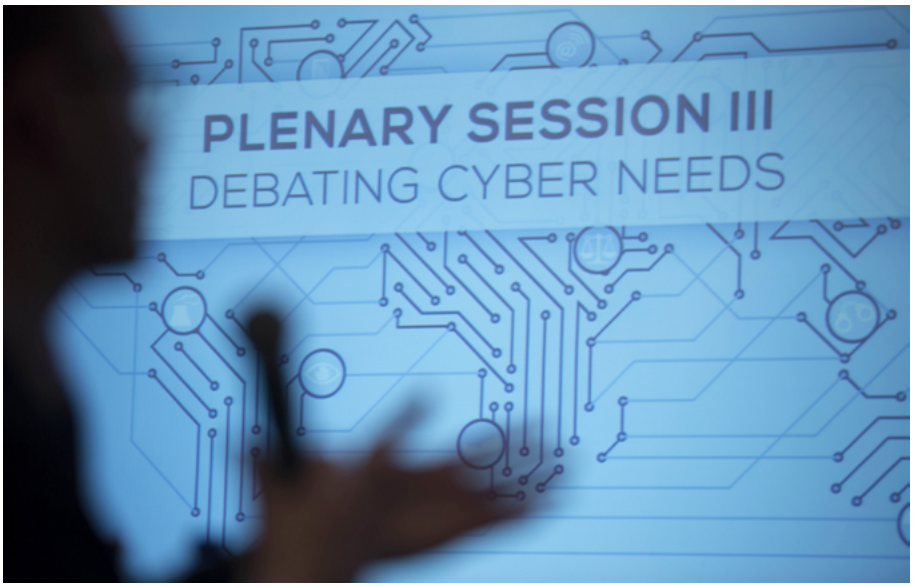
Challenges: scaling up and breaking silos

To date, the EU's experience confirms several key challenges that are specific to the cyber sphere. Firstly, the cyber needs of developing countries especially with regards to institutional capacities (law enforcement, judiciary, incident response agencies) are so high that effective and consistent cooperation in capacity building is the x factor in coordinating limited resources and avoiding fragmentation. For this reason, the creation of the Global Forum on Cyber Expertise can play a pivotal role as a platform for deconflicting and synergizing amongst the plethora of actors that are ushered in the cyber capacity building universe.

This aspect cannot be overstated, as the available expertise for delivery of technical assistance does not meet the demand of developing countries, whilst even developed countries are often struggling. Thereby, the scaling up of cybersecurity capacity building programmes that require long-term expert commitment could be positively pursued through the promotion of a regional approach in triangular cooperation that can lead to the creation of hubs of local experts in different regions.

A second challenge touches upon the persistent silos amongst different cyber communities within a given country. While in the area of cybercrime the stakeholders are clear thanks to the distinct criminal justice context, within the broader cybersecurity ecosystem the policy, technical, business and civil society communities most often do not cooperate. In

Joint EU-Council of Europe project "Global Action on Cybercrime - GLACY" (2013-2016)



European Commission – EU Institute for Security Studies, International Conference on Cyber Needs and Development, 23-24 February 214, Brussels, Belgium (Credits: ©Bernal Revert)

order to overcome the disconnect between these actors, the facilitation of functional multi-stakeholder and multi-dimensional engagement is fundamental.

Undoubtedly, these challenges also represent opportunities to drive the different communities to work together in innovative ways. Critical to this process will be the successful mainstreaming of cyber as a crosscutting issue across policies and practices both in developed and developing countries. We are not there yet.

More information:

ICT Facts and Figures: The World in 2015, ITU

World Development Report 2016, World Bank

Transforming our World: 2030 Agenda for Sustainable Development (especially relevant are Sustainable Development Goals 9 and 16, specifically targets 9c and 16a), United Nations

Cybercrime@IPA (2010-2013) was a joint regional project of the European Union and the Council of Europe. A more recent joint regional project is iPROCEEDS (2016-2019)

Cybercrime@EAP I (2011-2014) was a joint regional project of the European Union and the Council of Europe. Phase II and Phase III (2015-2017) are currently ongoing.

Global Action on Cybercrime 'GLACY' (2013-2016) and Global Action on Cybercrime extended 'GLACY+' (2016-2020) are joint global projects of the European Union and the Council of Europe

Cybersecurity Strategy of the European Union

Convention on Cybercrime ("Budapest Convention"), Council of Europe

EU approach to development effectiveness

Avoiding gaps and duplications in global cyber capacity building

The Global Forum on Cyber Expertise (GFCE) was established in 2015 as a platform for cyber capacity building worldwide. It provides an opportunity for GFCE members to promote capacity-building initiatives and exchange expertise. The forum's main ambitions: avoiding gaps and duplications in cyber capacity building and identifying successful initiatives to scale them to a global level. What has been achieved so far and what is in store for the years to come?

Written by: Mr. Anne Blanksma Çeta, Senior Advisor at the Secretariat of the Global Forum on Cyber Expertise

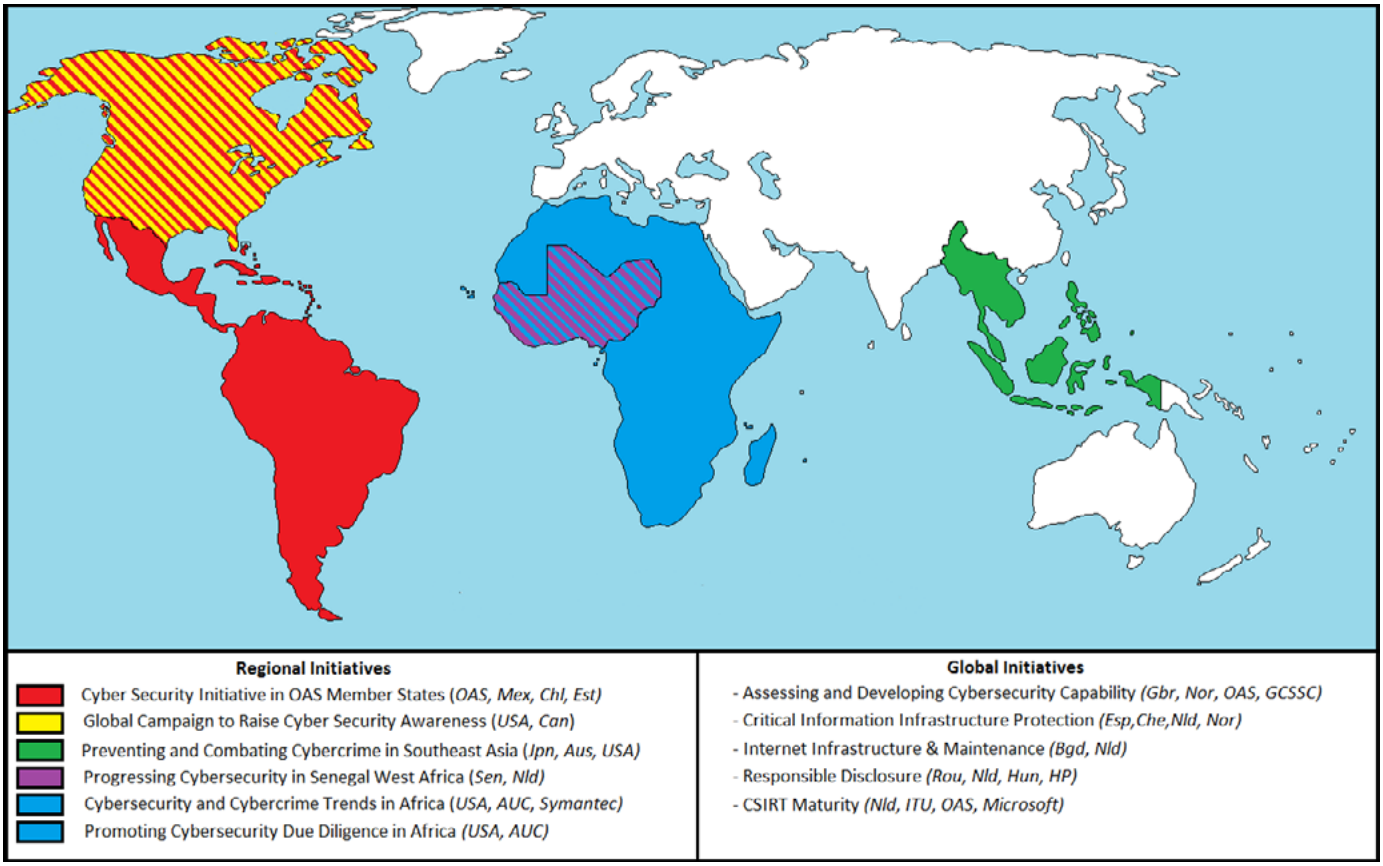
Collaboration on 11 capacity-building initiatives

Across the world, public and private organizations are investing in cyber capacities to reap the economic and social benefits that IT has to offer. Increased interconnectedness also necessitates the management of risks in cyberspace: strengthening cybersecurity, combating cybercrime and protecting online data. It is a global game, and the stakes are high. Weaknesses in cybersecurity can be exploited from anywhere; catching cybercriminals requires international collaboration and a new digital divide can stifle growth in developing economies. In the GFCE community, states, companies and intergovernmental organizations work together with NGOs, academia and the technical communities in the global effort to build cyber capacities. So far 25 GFCE members and partners collaborate on a total of 11 different cyber capacity-building initiatives.

The initiatives fall in two categories. First are the regional initiatives, which support capacity building in a certain geographical area. Three initiatives are focused on capacity building in Africa: obtaining research data on cyber trends and developments (see article on page 5), supporting national and regional cybersecurity strategies and incident response mechanisms and the training of cyber staff (see article on page 10). In the America's the Organization of American States (OAS) coordinates similar programs to develop local cyber capacity (see article on page 13 and 16), the US and Canada developed best practices for cybersecurity awareness campaigns, while an initiative in Southeast Asia focusses on collaboration to combat cybercrime.

Regional and global GFCE initiatives

A second category of initiatives operates on a global scale. Some initiatives focus on a policy domain such as the development of Incident Response Mechanisms/CSIRTs, Responsible Disclosure policies (see page 33), Critical Information Infrastructure Protection and Internet Standards. Other initiatives offer practical tools which can be used by other GFCE



Regional and global GFCE initiatives (Data provided by The Shadowserver Foundation)

members in their capacity-building efforts. Different members have already successfully assessed their level of Cybersecurity Maturity by using a model developed by the Global Cybersecurity Capacity Centre (GCSCC) at the University of Oxford. The new CyberGreen initiative helps countries and organizations assess the health of their overall cyber ecosystem (see article on page 21).

Further pitches for initiatives on cybersecurity in the banking sector and capacity building-related research are expected during the GFCE Annual Meeting on June 1st and 2nd in Washington, DC.

Exchanging cyber expertise at 11 international meetings

Collaboration on cyber capacity building primarily occurs within initiatives, but the GFCE also promotes the exchange of expertise across initiatives and with third parties during international cyber conferences. During the Annual Meetings, members have the opportunity to present initiatives to the GFCE Community during breakout and plenary sessions. GFCE members can also organize their own Expert Meetings, aided by logistical support from the GFCE Secretariat. So far, 4 expert meetings have taken place in Prague, Budapest and two in Dakar. During these meetings, experts exchange best practices on issues such as Responsible Disclosure and CSIRT maturity. These meetings are also interesting vehicles for the exchange of experiences across initiatives. For example, during the Expert Meeting on Cybersecurity in West Africa, the US was able to share their experiences on Cyber Awareness Raising, while the Netherlands introduced their approach to Responsible Disclosure.

Finally the GFCE also offers opportunities to promote best practices during International Cyber Conferences. In 2015 and 2016, the GFCE organized sessions during 5 such conferences: IGF (Brasil), the Meridian (Spain), Europol-Interpol Cyber

Exchanging cyber expertise during GFCE meetings and international conferences

Conference (the Netherlands), WSIS (United States) and the One Conference (the Netherlands).

Online database with over 100 projects worldwide

At the GFCE, members and partners can obtain practical documents and research data to make informed decisions about their capacity building investments. Each initiative is working towards concrete deliverables that can be used by other members, such as a best practice handbook, training program or research report. Apart from deliverables by initiatives, the GFCE also offers its own data. Commissioned by the GFCE, the Global Cyber Security Capacity Centre (GCSCC) has developed an online inventory of worldwide capacity-building projects. Funded by the EU, the GFCE is currently setting up an initiative for capacity building-related research. With these new investments, the GFCE aims to provide input for future High-Level Discussions (for example as part of a next Global Conference on Cyberspace) on strategic issues in global cyber capacity building.

Results, results, results

The GFCE is a nonpolitical forum aimed at achieving practical results. The current set of initiatives will start making deliverables available in 2016. Increased collaboration within the GFCE network will lead to more initiatives and activity by members and partners. The establishment of the GFCE Advisory Board consisting of 10 representatives from NGOs, the technical community and academia will provide new opportunities for multistakeholder collaboration and the impetus for new ideas. Initiatives are increasingly expected to move to the implementation phase, in which the GFCE can be used as a platform to find implementation partners and draw expertise.

More information:

About GFCE initiatives at www.thegfce.com/initiatives

Overview of global projects at the Cybersecurity Capacity Portal

Engaging with hackers in coordinated vulnerability disclosure

Private and public organizations are increasingly working together with ethical hackers to improve their cybersecurity architecture. In the GFCE initiative on Responsible Disclosure governments, companies and representatives from the technical community exchange their experiences and identify best practices. Under what conditions can ethical hackers be successfully integrated into national cybersecurity practices? What are the do's and don'ts in developing responsible disclosure capability?

Written by: Mr. Anne Blanksma Çeta, Senior Advisor at the Secretariat of the Global Forum on Cyber Expertise

Benefits and risks

The concept of Responsible Disclosure or Coordinated Vulnerability Disclosure (further RD) originated among cyber activists in the eighties and nineties. The original idea was that companies and governments should be publicly shamed into improving data protection by having weaknesses in their cyber infrastructure exposed. Since then, the thinking has evolved. 100 percent security does not exist, and it is generally accepted that organizations should have a chance to fix vulnerabilities before they are made public. RD policy sets the rules and guidelines which organizations and ethical hackers can use when investigating such vulnerabilities.

Jeroen van der Ham is Security Researcher at the Dutch National Cybersecurity Centre, which was one of the first Computer Security Incident Response Teams (CSIRTs) to adopt a national guideline on RD in 2013. He emphasizes the overwhelming benefits of RD as an important extra tool to detect vulnerabilities before they can be exploited. One of the perceived risks of having an RD policy, however, is the possibility of extra scrutiny among the hacker community. According to Jeroen, "In our experience, this is only true for the initial phase when the RD announcement is shared among the community of ethical hackers. We therefore advise companies to first invest in pen tests and the overall maturity of their infrastructure and response mechanism before employing RD.".

Rules of the game

Hackers, white or black-hat, can do serious damage. It is there-

Jeroen van der Ham is Security Researcher at the Dutch National Cybersecurity Centre

Victor Gevers, known as an ethical hacker under his pseudonym @0xDUDE

fore crucial that governments and organizations set clear and transparent procedures for RD. Victor Gevers, known as an ethical hacker under his pseudonym @0xDUDE, explains: "Ethical hackers, not seldom teenagers, have to be made aware of how far they can go. There should be clear and basic rules, such as no use of 'brute force', social engineering, DDOS-attacks or malware". On the other hand, organizations should also rethink what RD means for their internal processes. Jeroen cautions organizations against the lack of communication with ethical hackers: "A classic mistake is that organizations stop communicating after an RD. The ethical hacker might become frustrated with the response and might decide to go public. We therefore recommend establishing clear timelines for response to an RD. For software vulnerabilities, this is usually 2-3 months, and for hardware up to 6."

Via the GFCE Initiative on Responsible Disclosure, the Dutch Government, together with Hungary, Romania and Hewlett Packard, exchange best practices and try to get more governments and organizations to adopt this practice. An important recommendation for governments is to find a balance between encouraging organizations to disclose and fix vulnerabilities and punishing organizations for being aware of these vulnerabilities and failing to implement available corrective measures.

But hacking is illegal!

Yes, some forms of hacking can be harmful and illegal, while sometimes it takes place in a grey area of the law. Surprisingly, as an ethical

Manifesto on Coordinated Vulnerability Disclosure

During the EU High Level Meeting on Cyber Security on 12 May 2016 in Amsterdam, 29 organizations signed the Coordinated Vulnerability Disclosure Manifesto. In this manifesto, they announce public reporting mechanisms on vulnerabilities in their ICT systems and call upon other organizations to do the same. The Manifesto was initiated by Rabobank and CIO Platform Nederland, in coordination with the Dutch National Cybersecurity Centre in the context of the Dutch chairmanship of the EU. The Manifesto is signed by major organizations in the field of transport, healthcare, energy and has been embraced by the GFCE initiative on Responsible Disclosure as global best practice. Contact the GFCE secretariat if you want to co-sign the manifesto

Signing ceremony of the Manifesto during EU High Level Meeting

hacker, @0xDUDE is no proponent of increasing legal protection for ethical hackers. : "You have to understand that it is in the DNA of hackers to always find ways around; also, legislation is too slow to keep up with technical developments," explains @0xDUDE. "That is why I am more in favor of the publication of clear and transparent guidelines by governments and organizations. We should create a culture where ethical hackers can simply contact an organization in case of doubt about employing a certain hacking technique".

Likewise, Jeroen is not in favor of a legislative route to RD. "In the Netherlands we involve the Public Prosecutor in setting up our guidelines. They also published a report by themselves, which is currently used by Courts to develop jurisdiction on this matter. RD should be judged case-by-case, following guidelines and based on the intentions of the ethical hacker, proportionality of means and possible harm caused."

Do's

- → Have national guidelines on RD and prosecution of ethical hackers
- → Have transparent and clear rules on RD procedure including:
  - Forbidden hacking techniques
  - Response time (including sending of RD report confirmation of receipt and action taken)
- → Give credit to ethical hackers, not necessarily with financial incentives

Dont's

- → Don't start RD policy before ICT infrastructure and incident response is in order (including Pen-test)
- → Don't stop communicating with ethical hacker after RD report
- → Don't be too risk averse in rigid punishment of organizations for vulnerability disclosures and failure to act

Rewarding hackers

Given the looming threat of legal action, what drives ethical hackers to cooperate on RD? According to @0xDUDE, it is not necessarily the money: "Some organizations have bounty programs to encourage RDs, but for most organizations this is not necessary to employ." There are other ways to reward ethical hackers for constructive cooperation: giving public credits, support in CV building or issuing an official certificate for rendered services. With a worldwide demand for IT professionals, it is also especially interesting to recruit a pool of young talents. With irony in his voice, @0xDUDE warns about the cultural gap: "Hackers are not necessarily impressed by your suits and university degrees."

More information:

The GFCE Responsible Disclosure Initiative

Best Practice Guide Responsible Disclosure – Experiences from the Netherlands, Global Conference on CyberSpace 2015

ISO standard 29147 on Information technology, Security techniques & Vulnerability disclosure

Manifesto on Coordinated Vulnerability Disclosure

Volume 1, June 2016
Global Cyber Expertise Magazine

Colophon

Editorial board	Anne Blanksma Çeta (GFCE) Belisario Contreras (OAS) Frida Orring (EU) Souhila Amazouz (AU)
Guest editors	Amirudin Abdul Wahab Alfred Schandlbauer Barbara Marchiori de Assis Heli Tiirmaa-Klaar Kerry-Ann Barrett Panagiota-Nayia Barmpaliou Thiam Ndèye Fatou Coundoul William Wright
Artwork & design	Ivonne Vivanco (OAS)
Chief editor (rotating)	Anne Blanksma Çeta (GFCE)

Publishers

African Union, www.africa-union.org,
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 2:
31 August 2016