Report Expert Meeting on Cybersecurity in West Africa

12-13 April 2016, Dakar Senegal

Overview

The Dakar Expert Meeting on Cybersecurity in West-Africa was well attended with around 200 participants, a lot of media coverage and a wide variety of participants from the government, the private sector, research institutes and the technical community. These included representatives from the Netherlands, Senegal, United States, India, European Union, African Union, UNODC and most ECOWAS countries. The focus of the panels and discussions during the two days was the need for countries in West-Africa to prioritize cybersecurity.

It is important to discuss cybersecurity issues in Africa for several reasons: the rapidly growing ICT sector, high-quality ICT products and services it provides and the construction of ICT Hubs of Africa. Besides that, Senegal is clearly committed to the GFCE and the subject of cybersecurity and therefore a good place to start the discussion about cybersecurity in Africa. The GFCE can support these countries in their efforts to strengthen their cybersecurity by giving them access to knowledge and means to achieve this.

The concrete result of the expert meeting is the ‘Dakar Declaration on Cybersecurity’. With this Declaration an agenda will be set for cyber capacity building with the following components: a) national cybersecurity strategies; b) Computer Security Incident Response Teams (CSIRTs); c) legal frameworks for cybersecurity; d) cybersecurity awareness and e) cybersecurity education. We call for the African Union and ECOWAS to support this Declaration and stimulate the follow-up process of this Declaration.

Summary

Opening
H.E. Theo Peters, Ambassador of the Kingdom of the Netherlands in Senegal, welcomed all participants. He explained how the GFCE was created during the Global Conference on Cyberspace in 2015 in The Hague as a permanent forum in which member countries, international organizations and private companies work together on cyber capacity building. The GFCE is supported by a Secretariat which is currently financially supported by the Dutch Government. He further elaborated on the important GFCE initiatives currently taking shape:

- Analysis of cybersecurity and cybercrime trends in Africa (Symantec, the African Union, United States).
- Stimulating responsible disclosure and dialogue with ethical hackers for improving cybersecurity (Hungary, Romania, HP, the Netherlands).
- Cybersecurity Awareness Raising in West-Africa including this expert meeting (Senegal, UNODC, Netherlands).

His speech was followed by Mr. Pierre Lapaque, regional representative on West- and Central Africa from the UNODC, who emphasized the need to put proper legal frameworks in place to unlock the opportunities of cyberspace. He further explained what the UNODC is doing in the area of capacity building, which includes promoting the establishment of legal frameworks, offering technical assistance, supporting the gathering of electronic evidence and improving the cooperation between law enforcement agencies.

The third speaker was H.E. Dr. Yaya Abdoul Kane, Ministry of Post and Telecommunications of the Republic of Senegal and represent of the Senegalese Prime Minister. He spoke about the importance of sharing best practices in cyberspace and raising awareness about the challenges we all face in cyberspace. Besides that, he repeated that Senegal just signed the Cybersecurity Convention of the African Union and already signed the Budapest Convention on cybercrime. Furthermore, Senegal is working together with the Netherlands and the ITU to further improve its cybersecurity. As part of this cooperation in January, a Cybersecurity Maturity Review was conducted by researchers of the Global Cybersecurity Capacity Centre. Based on the outcomes, Senegal will create a national cybersecurity strategy.

The opening session was concluded by Prof. Abdallah Cissé, trainer, Cybersecurity and lawer consultant, who stated that cybersecurity should be a central concern in all technical developments. According to Cissé, the African continent is not yet taking full benefits of ICT (Information communication technology) and is mugged by security breaches. Africa is trying to find its way in the digital way, what is reflected in the negotiation of a lot of African countries on the Malibu Convention on cybersecurity. For the coming years, management of cybersecurity risks is key. In order to achieve this, a coherent, efficient and controllable cyber strategy is needed and the proper structures should be put in place. To overcome the digital divide it is important that African countries are being supported, especially to ensure the proper technological structures.

Opportunities and threats in Cyberspace

Over the last 60 years the development of ICT created numerous opportunities. This development continues at high speed and is likely to continue. Alongside the complex and dynamic development of ICT, the amount and size of cyber threats is increasing. In this session, participants got an overview of the most recent attacks and different challenges were discovered. Within these challenges a priority for governments is to have a national cybersecurity strategy.

The scenario exercise was led by Prof. Marco Gercke from the Cybercrime Research Institute in Germany. He introduced different cybersecurity incidents through a scenario based movie about the fictional country Salama. These scenarios included: cyberattacks by activists, ransomware, suspicious emails, DDOS-attacks, online defacements, disclosure of confidential documents, Twitter-account takeover and critical infrastructure attacks. The scenario exercise triggered an interactive discussion wherein participants became aware of the urgency and challenges we have to respond to in cyberspace. The discussion was based on a fictional but realistic scenario that clearly confronted everyone with the dilemmas we have to deal with in cyberspace. The panelists were asked to come up with concrete solutions for the challenges presented in the short movie clips.

National Cybersecurity Strategies

This session focused on one of the main recommendations of the Cyber Security Assessment of Oxford in Senegal this year: the need to develop a national cybersecurity strategy. As a result, Senegal decided to follow this recommendation and has started with developing a national cybersecurity strategy. The Netherlands will support Senegal in this process. Furthermore, this session underlined the importance of developing national cybersecurity strategies and was moderated by M. Amine RACHED (Tunesia).

Highlights of panelists:

Mrs. Ndeye Fatou Coundoul Thiam Technical Advisor from the ICT Ministry of Senegal, started with a presentation of some of the outcomes of the Cybersecurity Maturity Review of Senegal which was conducted in January 2016 in collaboration with a large number of national stakeholders on two days in January, by the Oxford University experts, under GFCE initiative.

Secondly, Mr. Sona Michel from Burkina Faso stressed that cybersecurity is an issue that is in the forefront of mind in Burkina Faso. He told that the following issues are at stake in Burkina Faso: access to services and information, education and economic opportunities. Burkina Faso has already created a cyberstrategy, which includes sub-strategies focusing on 5 different sectors. A national strategy on cybersecurity is under development, the same in a lot of African countries and for Burkina Faso, multistakholder cooperation in cybersecurity and open data initiatives are central for its approach to cyber.

Thirdly, Prof. Paul Cornish from the Global Cyber Security Capacity Centre at Oxford University gave an overview of their work, in particular the Maturity Model. The Maturity Model is an independent self-assessment tool of the state of cybersecurity in a country on 5 dimensions. The essence of the recommendation of the Senegal Review is to develop and implement a national cybersecurity strategy.

Finally, the session was concluded by Mr. Eric Luiijf from TNO in the Netherlands. He explained how national cyber strategies should look like and went through the different elements of cyber strategies. The aim of a national cyber strategy should be to coordinate actions of governments internally, but also to coordinate with private- and public organizations (multistakeholder approach).

Legal and Programmatic Frameworks

In the next session the issue of cybercrime was discussed. Rapidly developing cybercrime possibilities require effective control in order to maintain the high trust of the digital society. In order to do so, criminal justice organizations tasked with combating cybercrime should have sufficient specialists. The Budapest Convention was explained and the importance of this document was widely acknowledged. In the Budapest Convention the legislation and approach to combat cybercrime globally is described in order to make the detection and punishment of cybercrime simpler. Besides that, the importance of the following elements was emphasized: the need to have specialists to combat cybercrime; the Budapest convention; and the concept of coordinated vulnerability disclosure. Coordinated vulnerability disclosure is about the situation where an ethical hacker or independent researcher who discovers vulnerabilities in a system, notifies the company or government before going public. The panel was moderated by Prof Abdoullah Cisse.

Highlights of the panelists:

Dr. Raphael Koffi of ECOWAS explained the involvement of ECOWAS in the area of cybersecurity. ECOWAS has a mandate to promote economic integration, but part of that is the harmonization of IT's in ECOWAS countries, which concerns mainly harmonization of policy and regulatory frameworks. ECOWAS secured three Acts about cybersecurity and is also involved in regional capacity building workshops, supported by the US and UN. The main challenge ECOWAS is confronted with is the implementation of these ideas is derivate of the staffing shortages. This makes it impossible to properly implement and follow up on agreed frameworks. Besides that, more awareness raising is needed to sensitize stakeholders on cybersecurity and cyber law. The way forwards should be to develop a regional cybersecurity strategy along national ones. Also CSIRTs should be set up and stakeholders have to be made aware of the issues at stake.

Mr. Neil Walsh of UNODC further illustrated how cybercriminals operate by using a real example of hacking into the software used by ports and distribution centers in order to control international shipping of illegal drugs. Furthermore, Mrs. Mancebo explained how UNODC uses information technologies in forensic investigations.

This was followed by the judge Mr. Papa Assane Touré, who stressed the need to involve a lot of players in ensuring cybersecurity. Senegal has a legal framework on cybercrime since 2008. The judge has a central role in cybercrime and is responsible for different legal notions related to cybercrime, such as defining information systems. Senegal already has developed extensive jurisprudence on this. Mr. Touré, addressed the need for judges to specialize in cybercrime, because of the complicated nature of this domain and this should be supported by international legal cooperation given the global nature of cyberspace. At the moment, in his opinion, this cooperation is still too weak, for example in extradition of cyber criminals (so far none) and cooperation with large technological companies. The Malibu convention and ECOWAS regulation on cybercrime are instrumental to improve this. Furthermore, the Budapest Convention is the strongest instrument which Senegal can use to improve its legal international cooperation in cyber.

The session was concluded by Mr. Vincent Toms from GDI Foundation. He argued that ethical hackers should be more involved in improving cybersecurity. This is in line with the idea of coordinated vulnerability disclosure, which is about the situation where an ethical hacker or independent researcher who discovers vulnerabilities in a system, notifies the company or government before going public.
The Netherlands has a legal framework in place to facilitate coordinated vulnerability disclosure. This idea was illustrated by the practical insights of an ethical hacker from GDI Foundation, Mr. Victor Gevers. He translated this idea in concrete examples and explained what his work as ethical hackers entails and how ethical hackers can help to lower the emergency response time.

Computer Security Incident Response Teams (CSIRTs)

In order to be able to adequately respond to different threats and to return to a stable situation after a disruption or cyberattack, countries need to have access to different response measures. ICT incidents that lead to an infringement of availability, integrity or exclusivity of the network- and information infrastructure should be solved in the first place by the concerned organization itself. In situations where this is not possible and incidents lead to a disruption of society or damage is done to the critical infrastructure, the government should adequately intervene. The importance of creating and strengthening CSIRTs was widely supported. The session was moderated by Dr Mouhamadou Lo.

Highlights panelists:

The session started with some remarks of Mr. Haythem El Mir from Tunisia, who talked about what CSIRTs are and how they operate, especially in the African context.

Mr. Serge Valery Zongo**,** from the International Telecommunication Union, followed with giving an overview of the kind of cybersecurity incidents which can occur and the different challenges that accompany it. These challenges have to do with critical communication infrastructure protection, establishing cybersecurity standards, awareness raising, etc. Besides that, he elaborated on the active support of ITU for setting up CSIRTs in countries. This is important because only 16 African countries have currently a CSIRT in place.

Furthermore, Mr. Ahmad Sa'ad Abubakar from Computer Emergency Response Team (CERT also known as CSIRT) Nigeria, explained how most government institutions and businesses in Nigeria migrated to an online environment. In 2015 CERT Nigeria was established to manage risks of cyber threats and effectively coordinate incident response and mitigation strategies to proactively deal with cyber attacks. Also a Situation Awareness Platform was established to coordinate information sharing on national level and support National Cyber Security Strategy. Nigeria CERT serves as a model to help others to establish international response teams. Nigeria CERT works closely with FIRST and international CERTs, for example in the area of training and knowledge sharing.

This was followed by the operational director of the Africa CERT: Mr. Marcus Adomey. He discussed the different understandings of the work of CSIRTs. A narrow understanding of the tasks of a CSIRTs would make it difficult to convince other stakeholders to create a CSIRT and to find right resources to manage it. He further presented different models of cooperation between and within CSIRTS and how they can cooperate.

Lastly, Mr. Martijn de Hamer, an expert from the National Cybersecurity Centre in the Netherlands, elaborated on his activities in supporting CSIRTs worldwide in reaching full maturity. The Dutch CSIRT is cooperating via different international fora, such as ENISA, FIRST, Cybergreen (Japan) and off course the GFCE. He further gave more detailed information about the CSIRT Maturity initiative of the GFCE, which supports countries in setting up CSIRTs. This initiative is a collaboration between ITU, Microsoft, OAS and the Netherlands.

Education and Expertise on Cybercrime

The focus of this session was on the importance of cybersecurity education. Good education on all levels is necessary in order to be able to continue making trustworthy ICT and be able to offer resistance to cyber threats. A professional group is a perquisite for the growth of the digital economy. The importance of good education on all levels in order to achieve trustworthy ICT was broadly supported. Regional experts discussed different initiatives in the field of education. The session was moderated by Dr. Wangue David Brice from Cameroun.

Highlights of panelists:

Prof. Pierre Parrend from ECAM started the session with stressing the need of cybersecurity education in order to be able to deal with malware, site destruction, defacement etc. There is a need to intensify cybersecurity awareness raising. He further told about the work of ECAM, which involves pen-test trainings, cybersecurity audits and (Master) trainings for operational security managers.

Mr. Ali El Azzouzi**,** Director of Maroc Data Protect, is also involved in pen-testing, intrusion tests and ethical hacking in Morocco. He emphasized the need for national structures to deal with cybersecurity, discussed which skills are necessary for cybersecurity professionals and stated that recruitment should not be primarily knowledge based, but competence based.

Furthermore, Mr. Alex Corenthin from University of Dakar – UCAD and represent of ISOC/SENEGAL, made a connection between cyber education and awareness raising. He argued that cybersecurity trainings should be implemented in all levels of society and more resources should be given to educational institutions for proper trainings. Besides that, he sees E-learning as a way to dematerialize education and training and insisted on the creation of special schools to address cybersecurity.

Lastly, Mr. Idrissa Coullibaly from Sonatel Senegal outlined the mission of his company which is to provide technical solutions to 4 countries in the West-African region (such as cloud computing, hosting, internet access). He also talked about the support they provide to SMEs in launching cyber related businesses. Cybersecurity is a threat to West Africa because of the low costs and low bar to conduct cyber attacks in the West African region. Sonatel sees a role for itself to provide secure internet infrastructure and advisory support to parties who use this infrastructure.

Cyber Culture and Awareness

In the last panel, the focus was on the importance of cybersecurity awareness raising. We are all more often and longer online with our phones, tablets or computers. Luckily we are also becoming increasingly aware which risks this entails. However, it is also important to know what to do to prevent the risks. International and regional experts exchanged knowledge and expertise in the area of cybersecurity awareness raising. Different awareness campaigns were presented which strive to increase the development of knowledge about online security and stimulate acting in the same way. These campaigns are a joint initiative of the government, private companies and knowledge institutes. A good example is the US' Stop Think Connect Campaign. The session was moderated by Mr. Ibrahima Nour Eddine Diagne.

Highlights of the panelists:

Ms. Cari MacCachren, US Department of State, started the session with sharing her experiences as initiator of the GFCE initiative: A Global Campaign to Raise Cybersecurity Awareness (together with Canada, OAS, US). Aim of this initiative is to increase overall understanding of cyber threats worldwide and to empower citizens to be safer and more secure online. She explained the definition of cybersecurity awareness in a multistakeholder model and suggested the following approach based on the US campaign Stop, Think, Connect: identify stakeholders, get their attention, inform them of the risks, identify a path of protection and focus on specific tasks. Besides that, she elaborated on the OAS awareness campaign toolkit which aims to provide guidance and resources for developing cybersecurity awareness campaigns.

Secondly, Mme. Shona Sanni, GSMA, elaborated on children and mobile technologies. SMA represents 800 mobile operators worldwide. She further talked about the GSMA youth program, which aims at: promoting safe and responsible use of mobile technology in the Mobile Alliance Against Child Sexual abuse content. Africa has the greatest potential for growth and has a young population (70% <30) internet access will explode in Africa so the time to act is now. Therefore, she highlighted the importance of ITU/UNICEF guidelines on child online protection in this regard.

Furthermore, Mrs. Maimouna Dia Dione (Director of SENTRUST, Senegalese private sector) started with stating that Senegal has a high penetration rate of mobile phone in Senegal and other digital tools and that there is a big growth of e-economy in Senegal and thereby a growing exposure to cyber risks. Therefore, it would be good to start developing standards, install a commission on data protection and create a CSIRT. Another important issue is cyber awareness, according to Dione, the government should take an active role in this regard, but also private companies should take responsibility.

Commissionaire Pape Gueye from the Senegal Police further highlighted the digital revolution that has started in Senegal and positively impacts the economic situation in the region. However, he also identified two major questions as a consequence of this development in the area of awareness raising: What? And who? According to Gueye the general population should be educated on the risks in cyberspace and this awareness raising should be done by all of us.

The session was ended by Nenna Nwakanma from World Wide Web in Ivory Coast, she told the story of Susan Blankart, a Dutch Ambassador to Sudan who swam across the Nile. This story illustrated that those things that are sometimes perceived as a threat (dangerous water, women who are not supposed to be swimming) are actually opportunities (being able to swim). This also counts for cyberspace. Cyberspace most of all provides a huge opportunity for Africa. Therefore, we have to nurture a cyberculture and acknowledge that cultural freedom/openness and security are both sides of the same coin.

Closing ceremony

The expert meeting was wrapped up by Mrs. Frantzen, Acting Ambassador of the Netherlands in Senegal and Mr. Malick Diaye, Director du Cabinet of the Senegalese Ministry of Post and Telecommunications. They gave a brief summary of the discussions during the meeting and announced that on the base of this meeting the '**Dakar Declaration on Cybersecurity'** will be formulated. With this Declaration an agenda will be set for cyber capacity building with the following components: a) national cybersecurity strategies; b) Computer Security Incident Response Teams (CSIRTs); c) legal frameworks for cybersecurity; d) cybersecurity awareness and e) cybersecurity education. We call for the African Union and ECOWAS to support this Declaration and stimulate the follow-up process of this Declaration.