Framework for the development and implementation of a cybercrime strategy in Africa

JC Jansen van Vuuren[1], L Leenen [2] and P Pieterse [3]

[1] Tshwane University of Technology
[2] Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[3] South African Police
jansenvanvuurenjc@tut.ac.za
lleenen@csir.co.za
pietersen@saps.gov.za

Keywords: Cybercrime, Cybercrime strategy

1. Abstract:

With the development of ICT and the Internet there was barely any inclination that it could transform itself into a pervading revolution which could be misused for criminal activities. Cybercrime is increasing more rapidly than expected. IBM estimated in 2016 that by 2019 the global cost of cybercrime will reach $2 trillion, a threefold increase from the 2015 estimate of $500 billion. Organised crime is using cyber platforms in a much more sophisticated way that requires a highly skilled and specialised law enforcement response. Cryptocurrencies creates the opportunity for criminals to hide proceeds and the use of cryptocurrency mining malware is resulting in cybercriminals believing they are cashing in on unprecedented successes of these currencies. Regulatory has to be updated to effectively respond to unlawful activities relating to cybercrime. A holistic approach must be used by governments to develop a strategy and implementation plan to address the phenomenon of cybercrime for law enforcement. Currently most African countries address cybercrime in an uncoordinated and fragmented way. This paper presents a framework for African countries to develop and implement a national cybercrime strategy.

2. Introduction

Crimes increasingly involve computer systems or electronic evidence on computers or storage devices. Cybercrimes revenues have reached $1.5 trillion in 2018 (McGuire, 2018). IBM already estimated the global cost of cybercrime will reach $2 trillion in 2019, a threefold increase from the 2015 estimate of $500 billion (Laberis, 2016). By 2021 it is expected to increase to $6 trillion (Morgan, 2017). With the increase in broadband internet connectivity in Africa, the issues relating to cybercrime are emerging and there is a need to ensure that citizens, governments and business are protected and therefore a strategy and cybersecurity frameworks based on a common approach and common understanding are needed among member states of the African Union (African Union, 2015).

Cybercrime has evolved into a distinctive and sophisticated crime phenomenon on the Organised Crime Platform, which needs a highly skilled and specialised law enforcement response. The use of cryptocurrencies will potentially increase cybercrime; cybercriminals using cryptocurrency mining malware is resulting in cybercriminals believing they are cashing in on unprecedented successes of these currencies. These currencies are also used to disguise cybercriminals' proceeds (Labunski, 2017; McGuire, 2018) .

It is internationally accepted that regulatory requirements will have to be imposed for law enforcement to effectively respond to unlawful activities relating to cybercrime. Governments are obliged to use a holistic law enforcement approach to develop a strategy and implementation plan to address the phenomenon of cybercrime (McGuire, 2018). Currently most African countries address cybercrime in an uncoordinated and fragmented way.

This paper presents a framework for African countries to develop and implement a national cybercrime. Sections 1 and 2 gives the background for drive to develop a cybercrime framework and implementation plan for Africa. Section 3 gives an overview of the increasing cyber threats globally and then at the growth in cybercrime in Africa. The authors also consider to what extent African countries have reacted by developments in legislation to deal with cybercrimes, and more generally by looking at the cyber capability and capacity of African countries. This leads to a discussion of the importance of a national cybercrime strategy and the implementation of such a strategy in Section 4 and 5. The paper is concluded in Section 5.

3. Cyber Attack Statistics

This section provides an overview of attack statistics derived from the Microsoft Security Intelligence reports Volume 7 (2009) , Volume 21 (2016), Volume 22 (2017) and Volume 23(2018). **Figure *1*** shows the significant increase in ransomware attacks in Africa from 2017 to 2018. Ransomware on android devices are increasing on a monthly basis. Approximately 30% of malware on Android devices is ransomware. (Labs, 2017). Approximately 80% of ransomware attacks in Africa is due to Ceber (80%), where Wannacry, the most used ransomware in the rest of the world, only represents 17% of the attacks in Africa (Moyo, 2017).

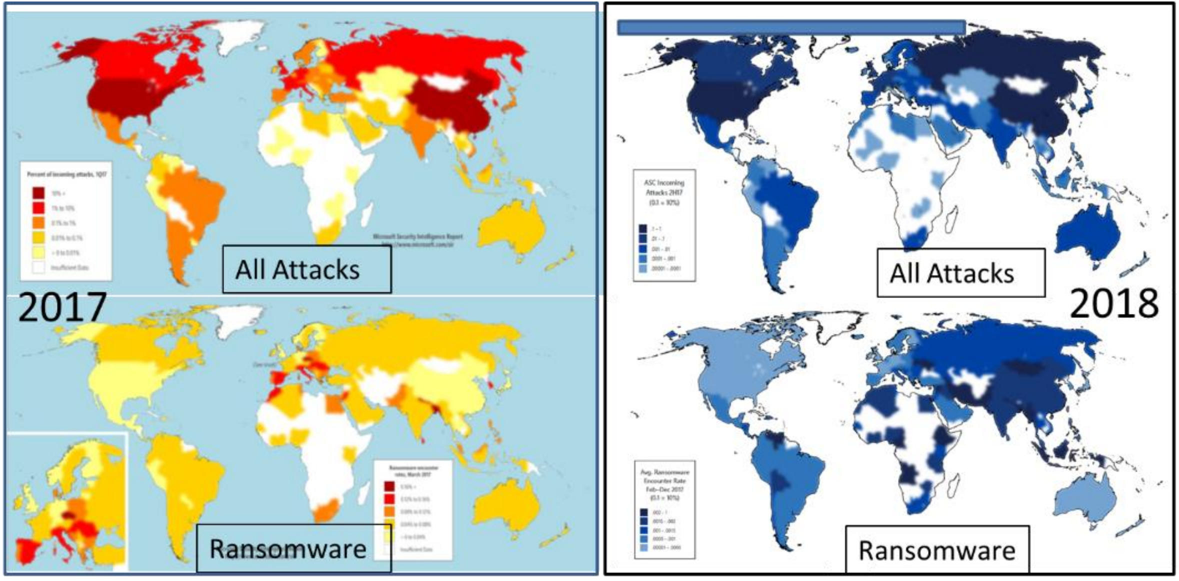


Figure 1: All Cyber Attacks 2017-2018

The maps shown in **Figure *2*** and **Figure *3*** illustrate the increase of malware threats over the past decade. **Figure *4*** shows that phishing is increasing rapidly in Africa with South Africa having the second highest concentration of phishing sites after Ukraine. Even in terms of phishing impressions South Africa is second after Iceland and Nigeria third. (A phishing impression is where a user clicks on a link in a phishing email that leads to a malicious website) (Microsoft, 2017). This weakness also contributes to the high levels of cybercrime in Africa. More than 75% of phishing mails include malicious URLs to phishing sites (Microsoft, 2018).

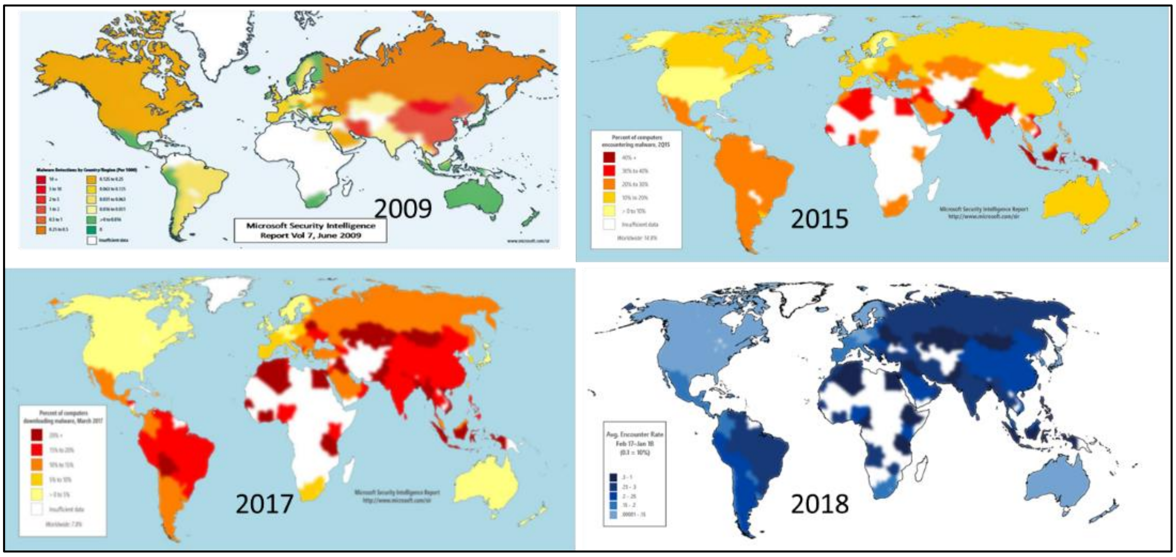

Microsoft Security Intelligence Report Vol 7, June 2009
2009
Percent of computers encountering malware, 2015
40% +
30% to 40%
20% to 30%
10% to 20%
> 0 to 10%
Insufficient data
Worldwide: 14.8%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
2015
Percent of computers downloading malware, March 2017
20% +
15% to 20%
10% to 15%
5% to 10%
> 0 to 5%
Insufficient data
Worldwide: 7.3%
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
2017
Avg. Encounter Rate
Feb 17–Jan 18
(0.1 = 10%)
2018

Figure 2: Malware Infection rates

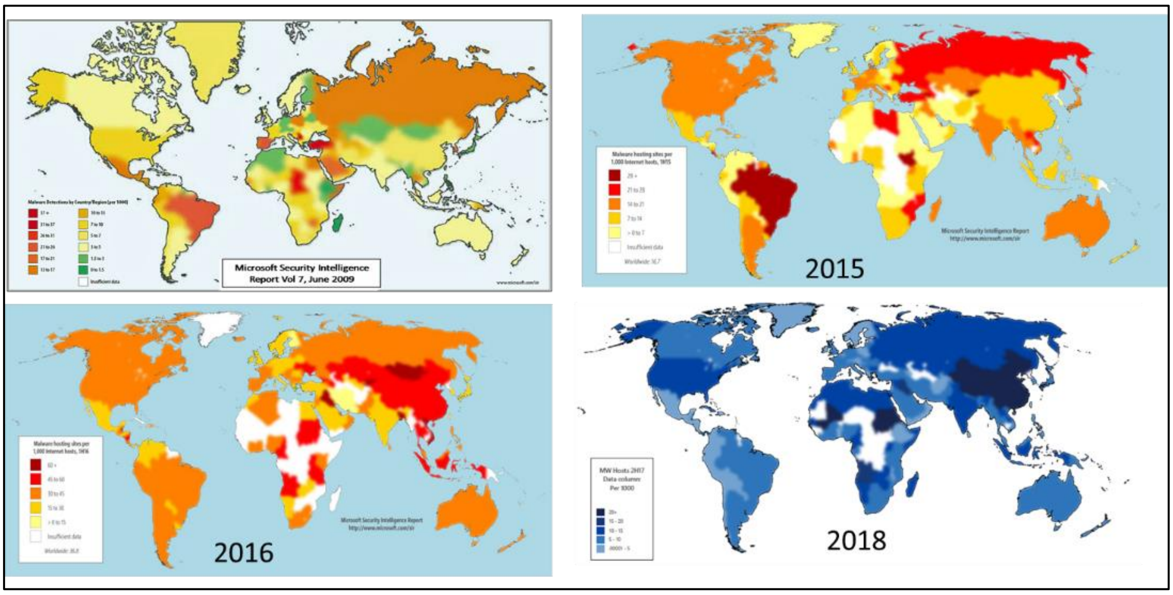

Microsoft Security Intelligence Report Vol 7, June 2009
Malware hosting sites per 1,000 Internet hosts
Insufficient data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
2015
Malware hosting sites per 1,000 Internet hosts
Insufficient data
Microsoft Security Intelligence Report
http://www.microsoft.com/sir
2016
MW Hosts 2H17
Data column
Per 1000
2018

Figure 3: Malware distribution rates (hosting sites)

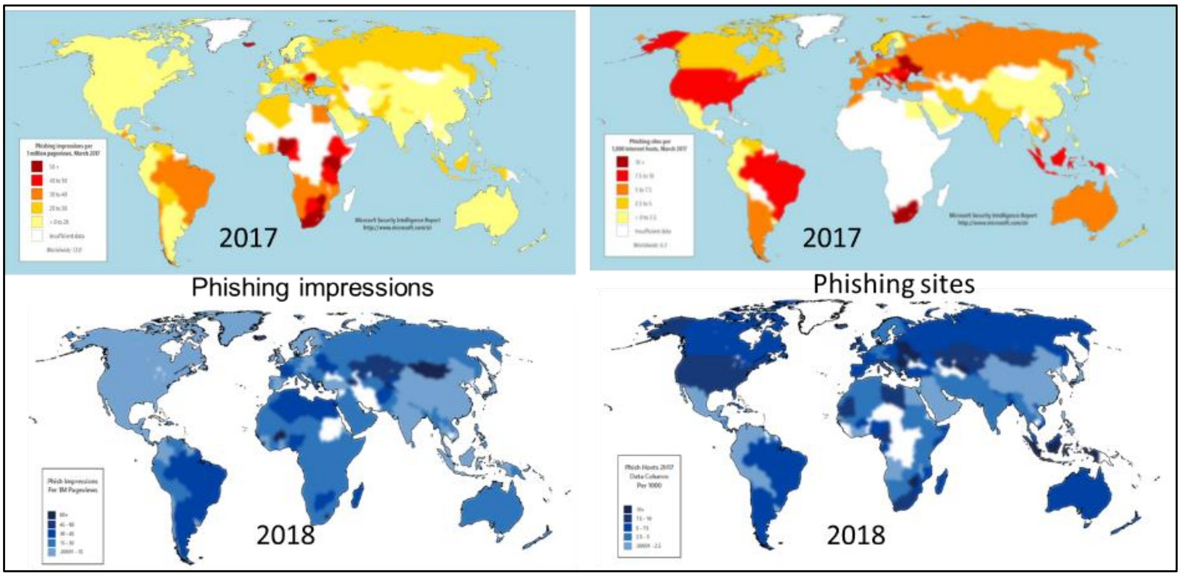


Figure 4: Phishing 2017-2018

3.1 Cybercrime Economy

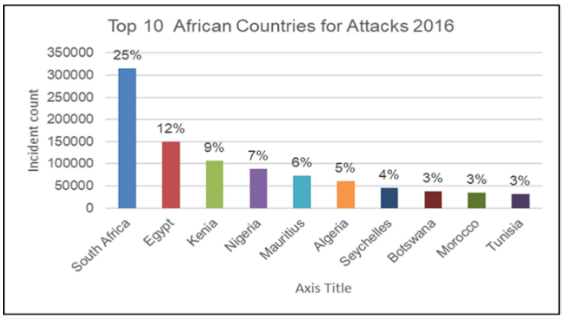
The cybercrime economy takes place at a variety of levels, from large “multinational” operations that can generate profits of over $1 billion to small scale operations, where profits of $30,000- $50,000 are more the norm. Criminals moved to cybercrime as it became must more lucrative. Individual earnings from cybercrime are now on average 10-15 percent higher than income derived from traditional crimes. The high-earning cybercriminals can make $166,000+ per month, middle-earners can make $75,000+ per month and and low-earners can make $3,500+ per month (McGuire, 2018). 91% of attacks by sophisticated cybercriminals start through spear phishing attacks (Morgan 2017).

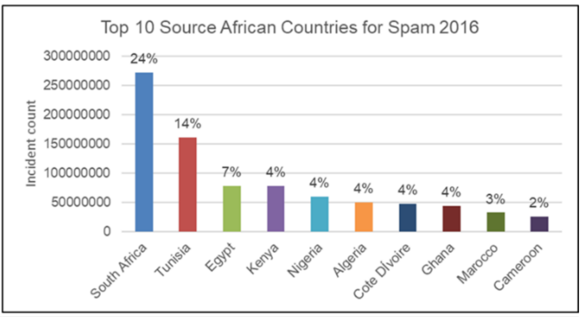
The use of crypto currencies and in addition the opportunities of the use of cryptocurrency mining malware, resulted in the increase of cybercrime. Cybercriminals believe they are cashing in on unprecedented successes as these currencies are also used to disguise their proceeds (Labunski, 2017). There is also a rapid increase in the use of cryptocurrencies for the payment of ransomware in Africa from approximately 10% in July 2015 to nearly 60% by the end of that year (Symantec, 2016).**Error! Reference source not found.**

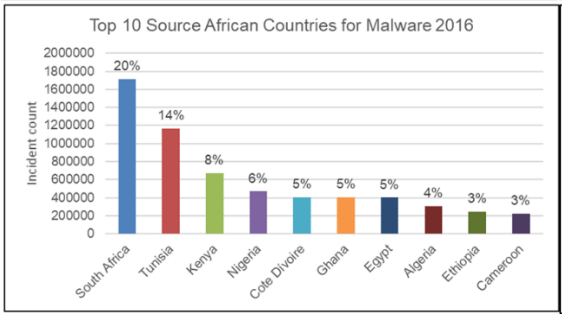
The revenues of cybercrime are now significant enough to attract the attention of those who are ready to use them to fund **more serious crime**, such as human trafficking, drug production or even terrorism (McGuire, 2018). McGuire founded in his study on the growth of the cybercrime economy that:

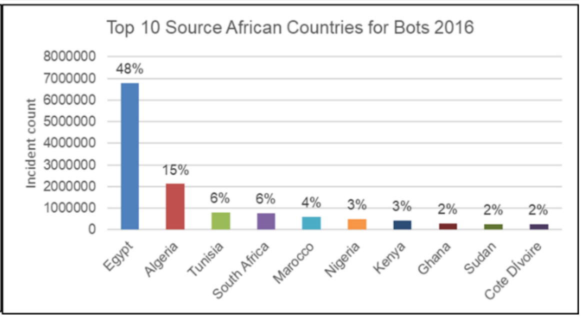
- At least 30 percent of the sample of cybercriminals included in his study said they had physically transferred cyber revenues or sent money via couriers on airlines to deposit in foreign banks.
- Digital payment systems were used as laundering tools in at least 20 percent of the cases with PayPal playing a part in at least 10 percent of cases.
- 95 percent of ransomware profits were cashed or laundered with the cryptocurrency trading platform.

3.2 Cybercrime in Africa


Top 10 African Countries for Attacks 2016


Top 10 Source African Countries for Spam 2016


Top 10 Source African Countries for Malware 2016


Top 10 Source African Countries for Bots 2016

Currently the capabilities of law enforcement agencies in Africa need to be improved to detect, handle and prosecute cybercriminals. In addition, the judiciaries must advance their knowledge on the cybercrime environment in terms understanding of the technicalities and complexities whenever cases are brought before courts. Most African countries also lack legislation on personal data protection (PDP) (African Union, 2015). African countries need to develop a coordinated approach in terms of a National Cybercrime Strategy that would cater to these needs (Usmani & Appayya, 2017). In a study done by Glace+ (Global Action on Cybercrime Extended) on Cybercrime legislation in Africa, the main challenges of the criminal justice systems in Africa are (Luchetti, 2018):

- Cybercrime investigation units are usually understaffed and not adequately trained/ skilled in the areas of:
  - The use of VPN or Tunneling and Proxy;
  - The use of darknets and virtual currencies;
  - Understanding of the Modus Operandi and the Evidence to collect; and
  - Investigations into possible forms of Organized Crime vs. Single criminal.
- There are limited technical capabilities to support a successful investigation due to:
  - Data/mobile forensics laboratories being outdated;
  - The capacity to do malware forensics and reverse engineering; and
  - Collaboration with local telecommunication service providers;
- The lack of international cooperation in:
  - Police force to Police force;
  - International Judicial Cooperation; and
  - Interactions with international large service providers (on social networks, etc.).

Cybercrime legal provisions in Africa is also a problem. By April 2016, out of the 54 countries in Africa only 11 countries seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) - although in one or more of the countries only the implementation of regulations may still have been lacking. A further 12 countries seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe). The majority of African countries (30) in 2016 did not have specific legal provisions on cybercrime and electronic evidence in force, but draft laws or amendments to existing legislation reportedly had been prepared in at least 15 countries (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). In some instances, bills had been presented to national parliaments, in others the fate of draft laws is uncertain(Symantec, 2016). The status in 2018 are depicted in **Figure *5***.

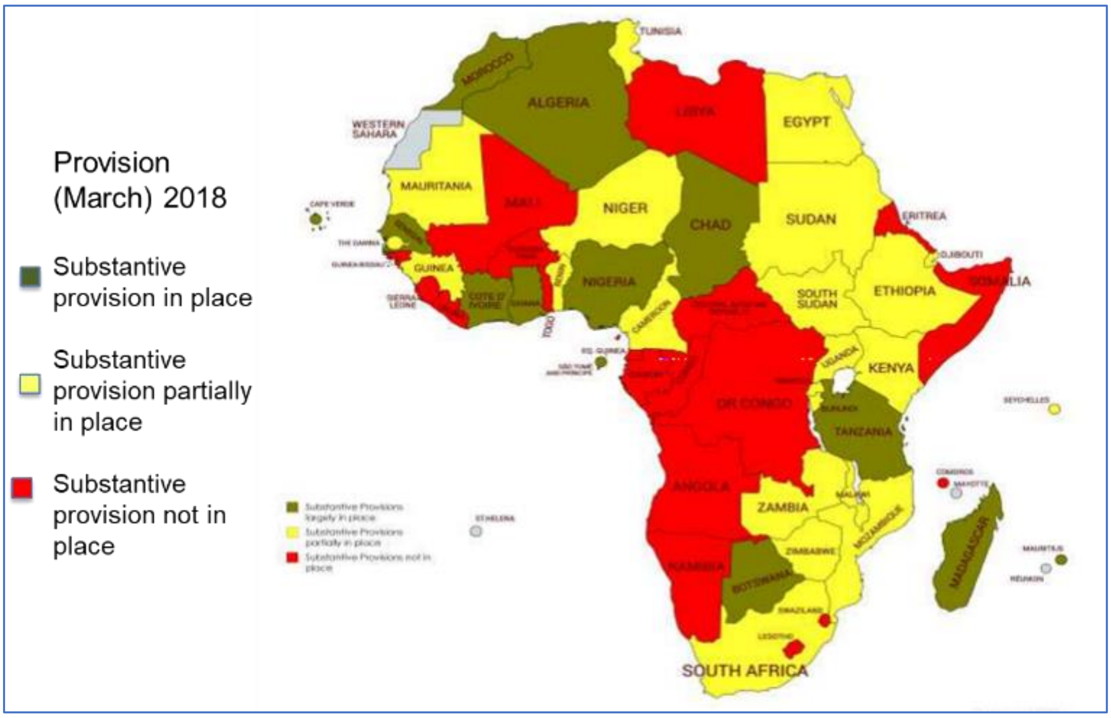
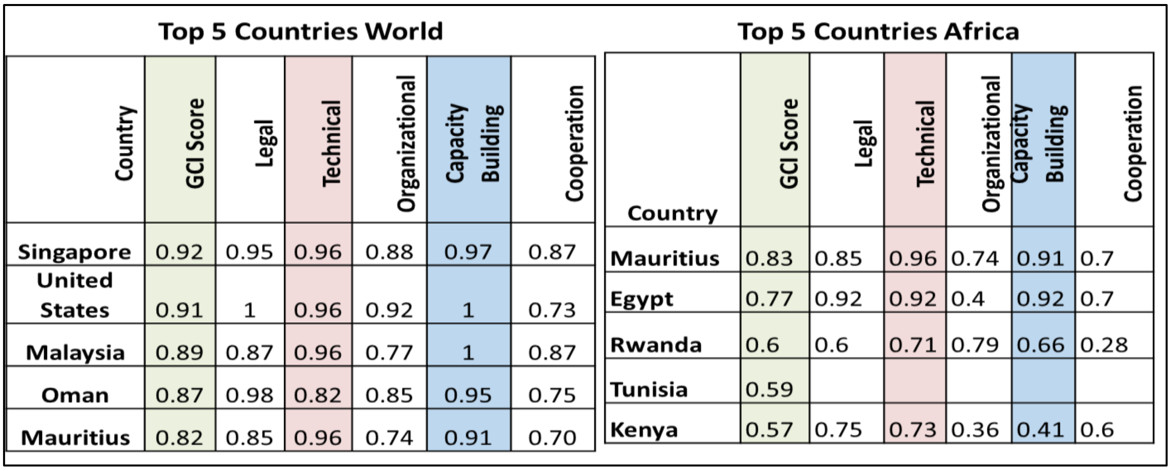


Figure 5: Cybercrime Legislation in Africa March 2018

The International Telecommunications Union (ITU) conducted a survey, the Global Cybersecurity Index (GCI), providing insight into the cybersecurity engagement of sovereign nation states and showing the commitment of countries towards cybersecurity. Their methodology uses a cyber maturity metric to assess the various facets of nations' cyber capabilities (ITU, 2017a, 2017b). Included in the matrix is the legal commitments and cooperation which is very important for cybercrime strategy implementation. According to the GCI, the five most advanced countries in Africa and in the World are listed in Figure 6. Detailed information on Tunisia is not provided in the report, and Egypt and Tunisia were included in the Arab region.



Top 5 Countries World

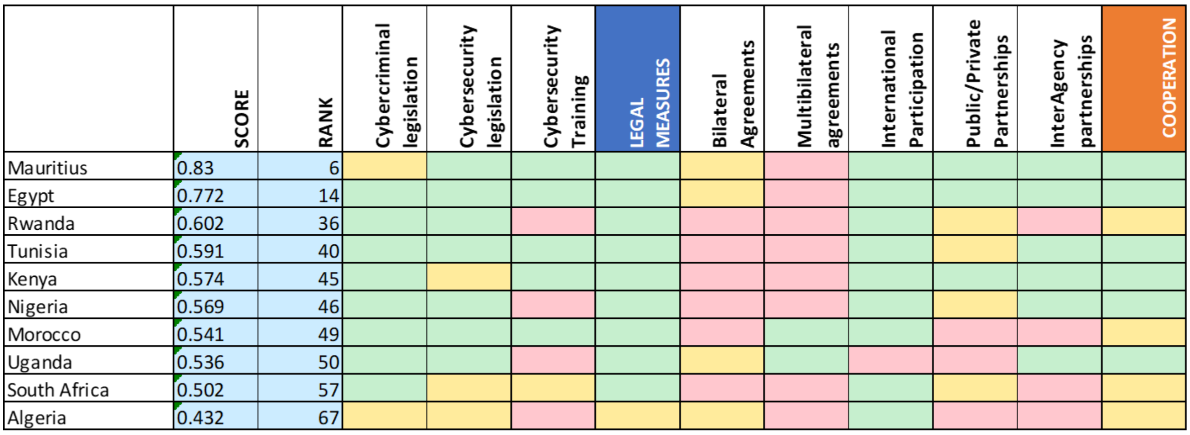
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70

Top 5 Countries Africa

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Mauritius	0.83	0.85	0.96	0.74	0.91	0.7
Egypt	0.77	0.92	0.92	0.4	0.92	0.7
Rwanda	0.6	0.6	0.71	0.79	0.66	0.28
Tunisia	0.59					
Kenya	0.57	0.75	0.73	0.36	0.41	0.6

Figure 6:Global Security Index 2017. Top five most committed countries in the world and Africa (ITU, 2017a)

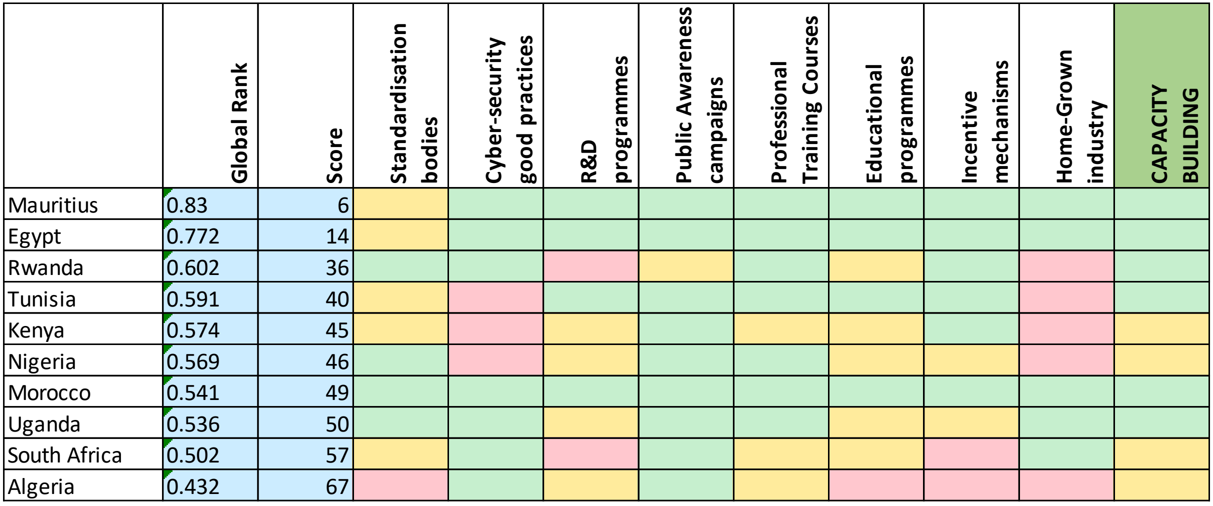
The legal measure in this index is based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime, and the cooperation measure is based on the existence of partnerships, cooperative frameworks and information sharing networks. These results are given in Figure 7 and Figure 8 - the level of commitment ranges from the highest (green), medium (yellow) and to the lowest (red).



	SCORE	RANK	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity Training	LEGAL MEASURES	Bilateral Agreements	Multibilateral agreements	International Participation	Public/Private Partnerships	InterAgency partnerships	COOPERATION
Mauritius	0.83	6	🟨	🟩	🟩	🟩	🟨	🟥	🟩	🟩	🟩	🟩
Egypt	0.772	14	🟩	🟩	🟩	🟩	🟨	🟥	🟩	🟩	🟩	🟩
Rwanda	0.602	36	🟩	🟩	🟥	🟩	🟥	🟥	🟩	🟨	🟥	🟨
Tunisia	0.591	40	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟨	🟩	🟩
Kenya	0.574	45	🟩	🟨	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩
Nigeria	0.569	46	🟩	🟩	🟥	🟩	🟥	🟥	🟩	🟨	🟩	🟩
Morocco	0.541	49	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟥	🟥	🟨
Uganda	0.536	50	🟩	🟩	🟥	🟩	🟨	🟩	🟥	🟥	🟩	🟩
South Africa	0.502	57	🟩	🟨	🟨	🟩	🟥	🟥	🟩	🟨	🟥	🟨
Algeria	0.432	67	🟨	🟨	🟥	🟨	🟨	🟥	🟩	🟥	🟥	🟨

Figure 7: Top ten countries in Africa - Global Cybersecurity Index for Legal and Cooperation ITU 2017a)

In the capacity building measurements, countries were evaluated on standardisation bodies, cybersecurity good practices, R&D programs, public awareness campaigns. professional training courses, national education programs and academic curricula, incentive mechanisms and the home grown cybersecurity industry (ITU, 2017a).



	Global Rank	Score	Standardisation bodies	Cyber-security good practices	R&D programmes	Public Awareness campaigns	Professional Training Courses	Educational programmes	Incentive mechanisms	Home-Grown industry	CAPACITY BUILDING
Mauritius	0.83	6	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Egypt	0.772	14	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Rwanda	0.602	36	🟩	🟩	🟥	🟨	🟩	🟨	🟩	🟥	🟩
Tunisia	0.591	40	🟨	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟩
Kenya	0.574	45	🟨	🟥	🟨	🟩	🟨	🟨	🟩	🟥	🟨
Nigeria	0.569	46	🟩	🟥	🟨	🟩	🟩	🟨	🟨	🟥	🟨
Morocco	0.541	49	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Uganda	0.536	50	🟩	🟩	🟨	🟩	🟩	🟨	🟨	🟩	🟩
South Africa	0.502	57	🟨	🟩	🟥	🟩	🟨	🟨	🟥	🟩	🟨
Algeria	0.432	67	🟥	🟩	🟨	🟩	🟨	🟥	🟥	🟥	🟨

Figure 8: Top ten countries in Africa - Global Cybersecurity Index for Capacity Building ITU 2017a)

4. Cybercrime and Cybersecurity strategies

Cybersecurity strategies are interdisciplinary and involve many stakeholders. The primary interest of a cybercrime strategy is to implement crime prevention in the criminal justice system and to ensure policing of ICT in the borderless online environment. It includes offences by means of ICT such as financial and other online fraud, sexual exploitation of children, terrorists' use of the Internet, infringements of intellectual property rights and other offences. Cybercrime strategies also need to address electronic evidence that impacts the capabilities of criminal justice. Cybersecurity and cybercrime strategies should complement and reinforce each other (Seger, 2012b). The comparison between the two types of strategies is demonstrated in **Figure *9***.

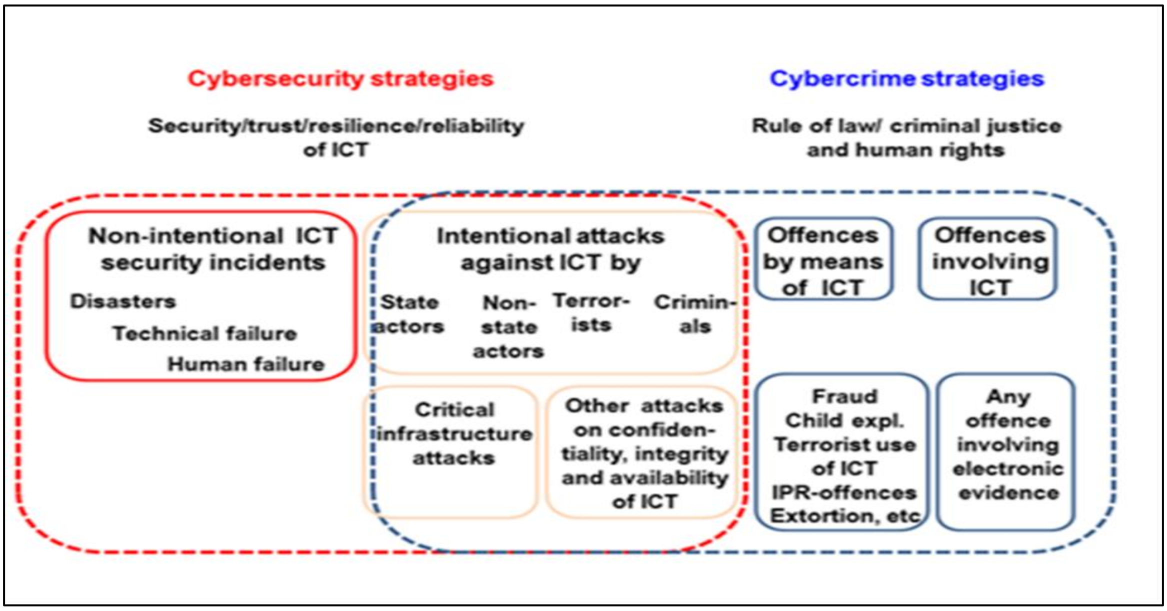

Cybersecurity strategies
Security/trust/resilience/reliability of ICT
Cybercrime strategies
Rule of law/ criminal justice and human rights
Non-intentional ICT security incidents
Disasters
Technical failure
Human failure
Intentional attacks against ICT by
State actors
Non-state actors
Terror-ists
Crimin-als
Critical infrastructure attacks
Other attacks on confiden-tiality, integrity and availability of ICT
Offences by means of ICT
Offences involving ICT
Fraud
Child expl.
Terrorist use of ICT
IPR-offences
Extortion, etc
Any offence involving electronic evidence

Figure 9: Comparison between Cybersecurity and Cybercrime strategies (Data Protection and Cybercrime Division, 2013)

5. Cybercrime Strategy Implementation

A successful implemented cybercrime strategy will ensure an effective criminal justice response to offences against the confidentiality, integrity and availability of computers and by means of computers, as well as to any offence involving electronic evidence (Data Protection and Cybercrime Division, 2013; Seger, 2012b). The strategy must also reflect the cultural values and beliefs of the African Nations

5.1 Governance

Governments need to develop, manage, implement and adopt coherent policies and strategies on cybercrime. They have to ensure that links and synergies are established between cybercrime strategies and cybersecurity policies and strategies. Decisionmakers must be engaged to understand the risks, agree on strategic priorities, provide political backing and allocate resources to measure cybercrime. The strategies and policies must contribute to human rights, the rule of law, democratic governance and human development as well as the security, confidence and trust in ICT (Data Protection and Cybercrime Division, 2013). The public and private sector must collaborate to ensure multi-stakeholder participation.

5.1.1 Strategies and Policies

The objective of a cybercrime strategy is to ensure that the rule of law applies in the ICT and online environment and that legitimate rights are protected. A cybercrime strategy will generally consist of legislation, including global harmonisation, operational law enforcement capacities through additional resources and powers, law enforcement and judicial training. interagency cooperation, industry/law enforcement cooperation and international cooperation (African Union, 2015; Seger, 2012b). Seger (2012) identified the elements for the implementation of the cybercrime strategy as cybercrime reporting and intelligence, prevention (education and awareness), legislation, high-tech crime and other specialised units, interagency cooperation, public/private (LEA/ISP) cooperation and effective international cooperation. The authors of this paper used the elements of the Seger Framework as well as the requirements of the African Union to develop a suitable framework for Africa. This framework for the implementation of cybercrime strategies in Africa is given in **Figure *10***. Cybercrime strategies in Africa must also reflect the cultural values and beliefs of the African Nations (African Union, 2015). Countries in Africa will need technical assistance to create the capacities necessary for the implementation of a cybercrime strategy that includes legislation, the creation of specialised units, training and other measures foreseen under the strategy. Public and private sector collaboration can also support the development of a strategy on cybercrime. Many donors require a policy to be in place before supporting law enforcement with technical assistance and capacity building programmes. A coherent strategy would also help the African countries to mobilise technical assistance from public and private sector as they will understand the purpose of their contributions. The cybercrime strategy must be operationalized, coordinated and monitored to determine progress, results and impact to allow for corrective measures and justify the allocation of resources. Human rights and rule of law requirements must be met and promoted. There must be a sufficient level of harmonization of domestic legislation with international standards to facilitate international cooperation (Data Protection and Cybercrime Division, 2013).

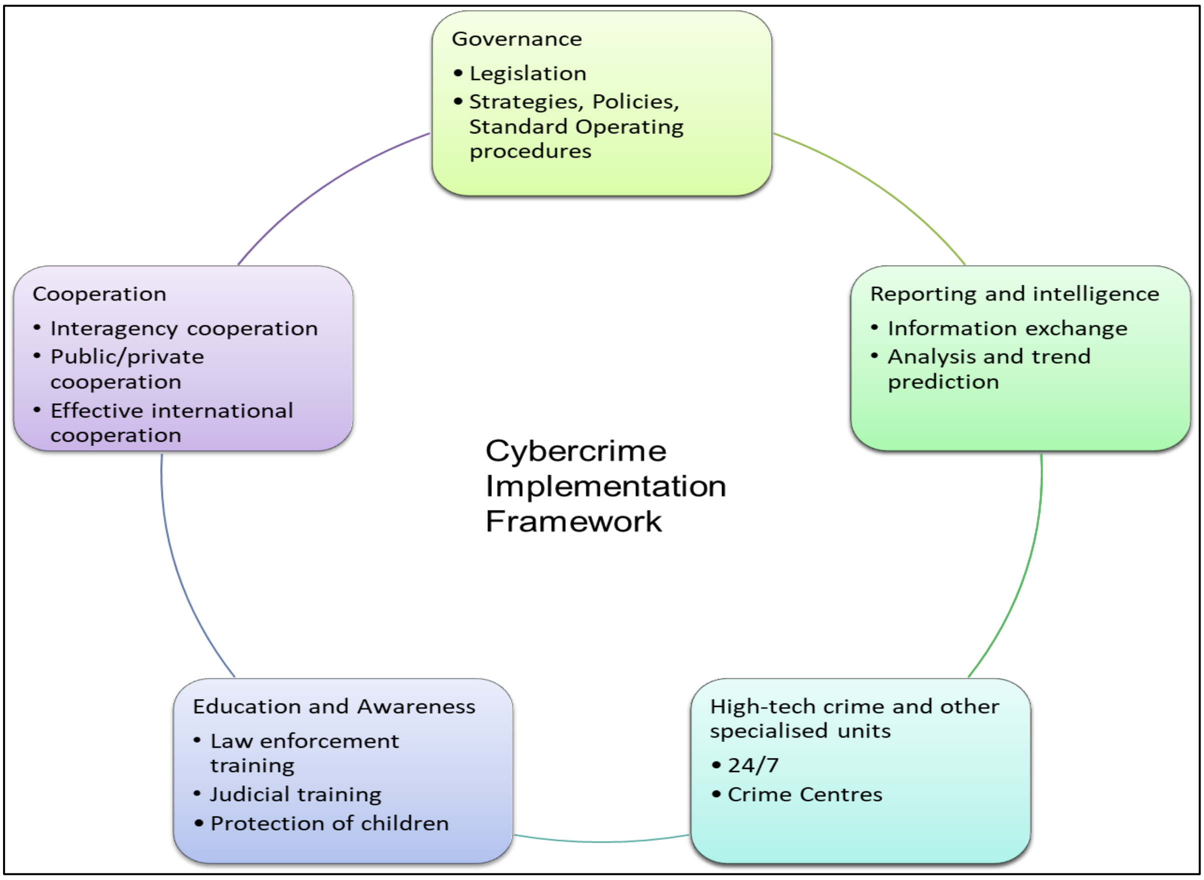

Governance
• Legislation
• Strategies, Policies, Standard Operating procedures
Reporting and intelligence
• Information exchange
• Analysis and trend prediction
High-tech crime and other specialised units
• 24/7
• Crime Centres
Education and Awareness
• Law enforcement training
• Judicial training
• Protection of children
Cooperation
• Interagency cooperation
• Public/private cooperation
• Effective international cooperation
Cybercrime Implementation Framework

Figure 10: Implementation Framework for Cybercrime in Africa

5.1.2 Legislation

Countries must development an effective legal framework to detect, handle and prosecute cybercrime. This will facilitate the enforcement of new laws for different types of cybercrimes and its prosecution. It would also provide legal practitioners and judicial officers with the capacity and expertise to deal with digital evidence (Usmani & Appayya, 2017). There must be substantive law measures to criminalise offences against computer data and systems (including as a minimum illegal access, illegal interception, data and system interference, misuse of devices) and by means of computers (including as a minimum computer-related forgery and fraud, child pornography and other forms of sexual violence against children, violations of intellectual property rights and related rights by means of computers if committed on a commercial scale) (Data Protection and Cybercrime Division, 2013). Provision must be made for the use of electronic evidence in criminal proceedings, the expedited preservation of data, production orders, search and seizure of stored computer data, real-time collection of traffic data and the interception of content data for specified investigations to ensure efficient investigations. However, it must be ensured that there is no abuse of these powers and personal data is protected (Data Protection and Cybercrime Division, 2013). The Budapest Convention (Council of Europe, 2001), does serve as a guideline and many countries have used it as a "model law" when preparing domestic legislation. This convention is a negotiated and formally adopted international agreement and thus also a legal framework for cooperation between state parties. This convention is also the basis for technical cooperation, not only by the Council of Europe, but also by major donors such as the European Union (Seger, 2012a). This convention and the African Union also indicate that legislation must be harmonized with international standards to provide law enforcement with procedural law tools for efficient investigations, to establish safeguards and conditions limiting investigative powers and adopting data protection regulations (African Union, 2015; Council of Europe, 2001). There are, however, also challenges in the setting up of legislation in

Africa. The Namibian minister of Justice has indicated that Namibia has come up with a draft bill on electronic transactions and cybercrime, but due to rapidly evolving technologies this legislation needs to flexible so that it takes into account the need for legal certainty and precision, while catering for the country's ability to cooperate with other states on matters of jurisdiction (Shanghala, 2018).

5.2 Cybercrime reporting and intelligence

It is important to gather and exchange intelligence from the public, businesses and government agencies. The value of collecting intelligence about (possible) cyberthreats cannot be under-estimated. (Usmani & Appayya, 2017). It is also necessary to establish reporting channels for citizens in the private and public sector. Intelligence is needed to analyse and predict trends. It is important for African countries to have access to data and knowledge on cybercrime as a shortage in this regard is a key obstacle to the prevention and control of cybercrime and results in difficulties to obtain political commitment and resources. It is thus necessary to establish convenient reporting channels for users, individuals, and public and private sector organisations. Information from these reporting channels may trigger law enforcement investigations, provide intelligence for a better understanding of scope, threats and trends of cybercrime, and allow for collating data to detect patters of organised criminality (Data Protection and Cybercrime Division, 2013; Seger, 2012b).

5.3 High-tech crime and other specialised units

Specific skills are required for the investigation of cybercrime and forensic analysis of electronic evidence and the prosecution of cybercrime. Currently there are limited units in police forces in African countries that deal with electronic evidence and cybercrime. Specialised units, such as high-tech crime units and prosecution services responsible for cybercrime and services for cyber-forensics must be created. Criminal justice authorities should thus be supported in the setting up or strengthening of high-tech units with strategic and operational responsibilities for prosecution and computer forensics. In the judiciary, special courts can be created compatible with the legal system of the country. In addition, a 24/7 contact point for cybercrime (must be established for urgent international cooperation and interagency cooperation with other police services (such as economic crime units, child protection units) for urgent international cooperation, especially for data preservation. Such collaboration enhances networking and training opportunities, international treaties and mutual legal assistance (Data Protection and Cybercrime Division, 2013). Some African countries are already advanced in this area as the Ivory Coast government who has set up a special forensic police unit which is composed of policemen, computer and telecommunication experts, and law practitioners to combat escalating cybercrime (Kobo, 2014).

5.4 Capacity Building and Awareness

The capacity and capability of legal professionals and the judiciary need to be enhanced to deal with the technical aspects of cybercrime such as the examination of the digital evidence. (Usmani & Appayya, 2017). Capacity building on different levels of the institutions dealing with cybercrime must be part of the cybercrime strategy because it responds to needs, produces immediate impact, favours multi-stakeholder cooperation and contributes to human development. (Usmani & Appayya, 2017). All law enforcement officers, prosecutors and judges will sooner or later need to deal with electronic evidence and need comprehensive training in this regard (Data Protection and Cybercrime Division, 2013)

5.4.1 Law enforcement training

Law enforcement officers needs to have the skills and competencies necessary to investigate cybercrime, secure electronic evidence, and carry out computer forensics analyses for criminal proceedings, assist other agencies, and contribute to network security. It is important to set up a training strategy with a training needs analysis (covering requirements from first responders to generic investigators, specialist investigators, internet crime investigators, covert internet crime investigators, network crime investigators, digital forensic investigators and managers) (Seger, 2012b). The establishment of a cyber academy responsible for cybercrime training in different African regions, is recommended.

Functions of police officers will determine the appropriate level of training, from first responder to forensic investigators. The training must be scalable, standardized and replicable. It is possible to use existing law enforcement training materials and initiatives (Data Protection and Cybercrime Division, 2013). These training materials must be adapted to include cybercrime reporting and investigation procedures. There must also be cooperation between law enforcement, academia and industry.

5.4.2 Judicial training

In addition to law enforcement officers, prosecutors and judges need to be able to deal with cybercrime. At the level of the police, specialised cybercrime units are often established that offer technical support to other police services, but the creation of specialised prosecution services is rare within the judiciary. The lack of knowledge and skills among prosecutors and in particular judges is a major concern in most countries and in all regions of the world (Data Protection and Cybercrime Division, 2013); Africa is not an exception. Judges and prosecutors must have at least a basic knowledge to deal with cybercrime and electronic evidence. In addition, it is also important to train lawyers, solicitors and advocates, especially in common law countries where they are officers of the court.

It is important that the training is coherent with other training, and therefore the training for judiciary must be integrated into the regular judicial training system of the country. This includes the preparation of training materials or the adaptation of existing materials to the needs of a jurisdiction, the training of trainers in the delivery of training, the mainstreaming or insertion of such training modules into the regular curricula of judicial training institutions to ensure sustainability.

.

5.4.3 Cybercrime Assessment Exercises

Cybercrime Assessment Exercises can be developed to evaluate the preparedness of law enforcement agencies and the other stakeholders dealing with cybercrime. This can be online exercises for individuals or in the form of cybersecurity drills (Usmani & Appayya, 2017) . Such an exercise is also an effective way to measure the level collaboration and information sharing between the different law enforcement units on national and international levels and will contribute to capacity building. These exercises in African countries will be essential to increase the level of cybercrime capability in Africa.

5.4.4 Awareness, and Educational Campaigns

In addition to technical, administrative and procedural measures to protect computer systems, public education and awareness are essential elements to prevent cybercrime. Educational campaigns targeting diverse groups in society must be organised to raise awareness on cybercrime issues and the measures required for cybercrime protection (Usmani & Appayya, 2017). Support for citizens can also include public websites with information on cybercrime prevention, educational materials and courses, recommendations for employees of public or private sector organisations, resources to prevent risks in a specific sector or organisation or assistance to victims of cybercrime (Data Protection and Cybercrime Division, 2013). Best Practices on Cybercrime must be developed to encourage businesses to adopt practices aimed at promoting secure online behaviour throughout the wider community, the distribution and development of low cost tools will help businesses to prevent and detect online threats (Usmani & Appayya, 2017). Special attention must be given to the empowerment of children. It is important for them to use the Internet in such a way that they will protect themselves, ensure their dignity, security and privacy to enhance the prevention and control of the sexual exploitation and abuse of children (Seger, 2012b)

5.5 Cooperation

5.5.1 Interagency cooperation

Public/private cooperation and information exchange have a strong impact on the prevention and control of cybercrime. This includes in particular cooperation between law enforcement authorities and Internet service providers (ISP), but also with CSIRTs (Computer Security Incident Response Teams) and financial sector RISK teams or (ISAACS), as well as non-governmental initiatives (such as for child protection) and others. Specific procedures must be developed to guide the collaboration (Council of Europe, 2001; Seger, 2012a).

5.5.2 Public/ Private collaboration

The cooperation between law enforcement and service providers is particularly essential and can take many forms – it will address awareness, training, technological improvements, vulnerability remediation and recovery operations (Usmani & Appayya, 2017). Collaboration can also be used for training and networking opportunities and by authorities for mutual legal assistance. Collaboration with institutions such as financial intelligence units are important for the exchange of information and intelligence of cybercriminals operations. A centralized cybercrime centre for law enforcement can be set up for specialized technical support for law enforcement officers in all units (Data Protection and Cybercrime Division, 2013). Formal agreements such as Memoranda of Understanding could be considered to provide a framework for this type of cooperation to define the expectations, responsibilities and authorities - but also limitations - and that it ensures that the rights of users are protected.

Financial institutions, public authorities and private sector organisations should pay attention to the prevention of fraud and money laundering. Measures must be put in place to search, seize and confiscate proceeds from cybercrime. These measures may include cybercrime reporting systems; prevention and public awareness; regulation licensing and supervision; risk management and due diligence, harmonisation of legislation, interagency cooperation, public/private cooperation and information exchange and other measures (Seger, 2012b)

5.5.3 Effective international cooperation

Cybercrime is an international problem which requires a coordinated and cooperative international response. Cybercrime involves multiple jurisdictions as it is a transnational crime. Efficient cooperation is necessary between police forces of different countries to preserve volatile electronic evidence. This also includes direct cooperation between high-tech crime units and between prosecutors of different countries and 24/7 points of contact (Seger, 2012b). Chapter III of the Budapest Convention on Cybercrime provides a legal framework for international cooperation with the measures and obligations of countries to cooperate to the widest extent possible as well as the measures to preserve data and efficient mutual legal assistance (Council of Europe, 2001). To strengthen partnerships it is important to sign multilateral agreements to ensure information exchange. (Usmani & Appayya, 2017). In the European Union, ENISA and Europol signed a strategic cooperation agreement to facilitate closer cooperation and exchange of expertise in the fight against cybercrime (ENISA, 2014).

The African Union promotes the exchange of information and communication between countries at foreign policy level (not only technical) and developing cyber diplomacy capabilities and holding consultations in order to reduce the risks of criminal use of ICTs. A continental and harmonized approach must be followed to enhance regional, continental and international cooperation that are necessary in cross-border investigating and prosecuting of cybercrime (African Union, 2015). This approach shall provide the African Countries with a clear understanding for the future risks and vulnerabilities in smart technology and the Internet of Things (IoT) and support the countries to create a secure and resilient cyber environment. The African Union will also develop regional mechanisms and work with member states on the harmonization of the cybercrime laws at regional and continental level and strengthen law enforcement cooperation both at regional and continental levels. They will support inter-governmental organizations and private companies to achieve norms and standards for exchanging of information during the investigation and prosecution of transnational cybercrimes and encourage African Union Member States in developing cyber diplomacy capabilities to participate in discussions carried out at international level such the UN Group of Governmental Experts (African Union, 2015).

6. Conclusion

The rapid growth of technologies and an increasing reliance on the cyber domain has led to an alarming increase in cyber-attacks and cybercrime globally. The focus of this paper is on African countries and how they well they have responded to this looming crisis in terms of building cyber capabilities and capacity. Governments have a responsibility to ensure national security and this includes cybersecurity. One important driver towards a cyber secure nation is to have a cybersecurity and a cybercrime strategy, and to implement these strategies.

This paper presents a framework for the implementation of a cybercrime strategy in the African context by analysing five different components: Governance, Cybercrime reporting and intelligence, specialised cybercrime units, Capacity building and awareness, and Cooperation.

7. References

African Union. (2015). A global approach on Cybersecurity and Cybercrime in Africa. Retrieved from https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf

Budapest Convention on Cybercrime, ETS No185, Treaty Series 185, Council of Europe, Pub. L. No. 01/07/2004, Budapest Stat. (Council of Europe 2001 01/07/2004).

Data Protection and Cybercrime Division. (2013). Capacity building on cybercrime. Retrieved from http://www.combattingcybercrime.org/files/virtual-library/capacity-building/capacity-building-on-cybercrime.pdf

ENISA. (2014). Fighting cybercrime: Strategic cooperation agreement signed between ENISA and Europol. Retrieved from https://www.enisa.europa.eu/media/press-releases/fighting-cybercrime-strategic-cooperation-agreement-signed-between-enisa-and-europol

ITU. (2017a). Global Cybersecurity Index (GCI) 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2017b). INDEX OF CYBERSECURITY INDICES 2017. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf

Kobo, K. (2014, August 28 2014). Cracking down on cybercrime in Ivory Coast,. Retrieved from http://www.aljazeera.com/news/africa/2014/08/cracking-down-cybercrime-ivory-coast-20148279503515697.html

Laberis, B. (2016). 20 Eye-Opening Cybercrime Statistics. Retrieved from https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

Labs, S. (2017). SophosLabs 2018 Malware Forecast. Retrieved from https://www.sophos.com/en-us/en-us/medialibrary/PDFs/technical-papers/malware-forecast-2018.pdf?la=en

Labunski, B. (2017, December 17, 2017). Rise of "Bitcoin Will Result in Increased Cybercrime in 2018. Retrieved from https://www.business2community.com/cybersecurity/rise-bitcoin-will-result-increased-cybercrime-2018-01973924

Luchetti. (2018). Cybercrime legislation in Africa - Regional and International standards. *GLACY+*. Retrieved from file:///C:/Users/JoeyCSIR/OneDrive/ICCWS2019/34122-wd-05.pres_cybercrime_legislation_in_africa_12apr2018_matteo_l.pdf

McGuire, M. (2018). *Into the Web of Profit: Understanding the growth of the Cybercrime Economy: An in-depth study of cybercrime, criminals and money.*. Retrieved from https://learn.bromium.com/rprt-web-of-profit-thank-you.html?aliId=4744500

Microsoft. (2009). *Microsoft Security Intelligence Report Volume 7*. Retrieved from http://www.microsoft.com/security/portal/Threat/SIR.aspx

Microsoft. (2016). *Microsoft Security Intelligence Report. Volume 21*. Retrieved from https://www.microsoft.com/security/sir/default.aspx

Microsoft. (2017). *Microsoft Security Intelligence Report. Volume 22*. Retrieved from https://www.microsoft.com/security/sir/default.aspx

Microsoft. (2018). *Microsoft Security Intelligence Report. Volume 23*. Retrieved from http://info.microsoft.com/rs/157-GQE-382/images/EN-AU-CNTNT-eBook-Security-GDPR-Microsoft-SIR-Volume-23%5B1%5D.pdf

Morgan, S. (2017). 2017 Cybercrime report.

Moyo, A. (2017). Africa's top ransomware families revealed. Retrieved from https://www.itweb.co.za/content/VKA3Ww7djeRqrydZ

Seger, A. (2012a). The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web. Retrieved from file:///C:/Users/JoeyCSIR/OneDrive/Cybercrime%20ICCWS2019/The%20Budapest%20Convention%20on%20Cybercrime%2010%20years%20on.pdf

Seger, A. (2012b). *Cybercrime strategies*. Retrieved from https://rm.coe.int/16802fa3e1

Shanghala, S. (2018). *Namibia: Cybercrime a Threat to National Security - Shanghala*. Paper presented at the 27th Session of the Commission on Crime Prevention and Criminal Justice, Vienna, 14-18 May 2018. https://allafrica.com/stories/201805150356.html

Symantec. (2016). *Cyber Crime & Cyber Security Trends In Africa*. Retrieved from https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa/documents/publications/2017/03/10/report-cyber-trends-in-africa

Usmani, K. A., & Appayya, J. A. (2017). Capacity Building is the Key to Fight Against Cybercrime: The Mauritian Perspective. *Global Cyber Expertise Magazine, 4, November 2017*.