In the study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

Summary Of Findings

International cooperation as one of its strategic objectives.

In Morocco, its National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) considers the promotion of national and reciprocal legislation and/or international legal instruments under Article 50 of Law No. 2016/007 on cybercrime.

Mauritania is required to co-operate with any international country in the investigation / prosecution of cyber-criminal offences in terms of national their implementation within the Republic of Guinea.

Economy sets out certain functions on this Ministry to participate in international cooperation efforts (including treaties, conventions etc) and overseeing personal data, whilst Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital assistance between the Republic of Congo and foreign judicial authorities.

In Guinea, international cooperation on combatting cybercrime is mandated under Article 106 of Law 2016/037 on cybersecurity and the protection of the fight against cybercrime shall be determined by regulation”, whilst Articles 105 and 106 of the same Draft Law details the procedures for mutual legal cooperation agreements on cybersecurity and

In Chad, Article 104 of its Draft Law on Fighting Cybercrime states that “the procedures for establishing cooperation agreements on cybersecurity and

In Benin, international cooperation for cybersecurity, three main areas: (1) electronic transactions, (2) personal data protection, (3) cybersecurity and cybercrime. The Convention will enter into force thirty (30) days after the 15th instrument of ratification or accession is deposited. The current status is five (5) ratifications out of fifty-five (55) AU

The African Union Convention on Cyber Security and Personal Data Protection (AUCC/ Convention) was drafted in 2011 to establish a credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and legislative challenges on the African Continent in a compatible and harmonised manner. As such, the Convention promotes, in the main, for African states

For the purposes of the Report, we considered whether the selected African Union member states have in place legislative/regulatory, policy and institutional measures in the areas of data protection, cybersecurity and cybercrime and electronic transactions called for by the AUCC. In particular, high-level interventions for implementation of the AUCC in the selected African Union member states. In turn, the study aimed to contribute to the advancement of frameworks; (ii) implementing institutional frameworks provided for in legislative and regulatory frameworks; and (iii) balancing interests in cybersecurity

The 2019 NEPAD Cybersecurity Policy and Regulation Assessment Report (“the Report”) analysed the policy and regulation in ten (10) African Union member States (Ghana, Guinea, Mauritius, Namibia and Senegal), while fourteen (14) more Member States have signed the Convention.

What are the electronic transactions policy developments?

What are the electronic transactions legislative measures?

What are the cybercrime and cybersecurity legislative measures?

What are the data protection institutional measures?

What are the data protection policy developments?
Foreword

The emergence of a global and borderless information society brings new opportunities to all countries worldwide as technologies play an even more important role in social and economic development. Services in the health, educational, business, finance and public administration sectors are possible thanks to ICT applications.

ICTs also bring new challenges which must be addressed if we are to securely conduct e-health transactions, enable citizens to access e-government services, provide the necessary trust for online commercial and business transactions and maintain the integrity of our information technology systems and resources. Despite the low level of ICT development and the low Internet penetration, Africa is experiencing rapid growth of cybercrime; cybercriminals have found ways to take advantage of the weak ICT infrastructure and turn Africa into a haven for operating illegally with impunity. Cybersecurity is still considered a luxury rather than a necessity in many African economies and its importance has not yet been sufficiently appreciated or recognized. Cybersecurity budgets in many organizations are reported to be less than 1% and many organizations have no budget allocated to Cybersecurity.

Cybersecurity has become even more important with the emergence of the COVID 19 pandemic, which has imposed the use of ICTs for all aspects of daily life. Computer attacks and digital scams have increased alarmingly during these times of uncertainty. It is therefore becoming crucial for countries and organisations to have frameworks in place to govern data protection and the security of electronics transactions. Putting in place adequate security and trust solutions is therefore one of the main challenges that must be addressed.

This Cybersecurity Assessment Report provides an overview of the various legislative and legal measures taken by African governments in selected countries to ensure the protection of personal data, the security of electronic transactions and the fight against cybercrime. It compares these measures to those defined by the African Union Convention on Cybersecurity and Personal Data Protection (AUCC), a credible framework for Cybersecurity in Africa. The study reveals that institutional measures relating to cybercrime and cybersecurity, as well as policy measures and institutional strategies relating to electronic transactions, are the areas lagging the furthest behind in the implementation activities of the member states studied.

The report has been developed to contribute to the advancement of cybersecurity in Africa and to strengthen the legal framework within which electronic transactions and the transfer of personal information take place on the continent. Building on the findings and recommendations of this report, AUDA-NEPAD will work to support member states in the development of policies and laws and in the implementation of institutional measures as required by the African Union Convention on Cybersecurity and Personal Data Protection.

Ibrahim Assane Mayaki

AUDANEPAD CEO
EXECUTIVE SUMMARY

Cybersecurity is of rising significance on the African continent, whether in response to opportunities in the digital economy or rising incidents of cybercrime.

The African Union Convention on Cyber Security and Personal Data Protection (AUCC/Convention) was drafted in 2011 to establish a credible framework for cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating of cybercrime. Working documents prefacing the AUCC note that the objective of such a Convention was to address the cybercrime related legislative challenges on the African Continent in a compatible and harmonised manner. As such, the Convention promotes, in the main, for African states to establish policy, strategic, institutional and legal frameworks for cybersecurity in the context of a credible digital environment. The AUCC encompasses in cybersecurity, three main areas: (1) electronic transactions, (2) personal data protection, (3) cybersecurity and cybercrime. The Convention will enter into force thirty (30) days after the 15th instrument of ratification or accession is deposited. The current status is five (5) ratifications out of fifty-five (55) AU member States (Ghana, Guinea, Mauritius, Namibia and Senegal), while fourteen (14) more Member States have signed the Convention.

The 2019 NEPAD Cybersecurity Policy and Regulation Assessment Report ("the Report") analysed the policy and regulation in ten (10) African Union member states - Benin, Chad, Republic of Congo, Democratic Republic of Congo, Guinea, Kenya, Mauritania, Morocco, Senegal and Tunisia. This Executive Brief provides an overview of the Report and the study constituting the Report.

At the national level, the Report recommended African Union member states to consider: (i) drafting or reviewing of outdated legislative and regulatory frameworks; (ii) implementing institutional frameworks provided for in legislative and regulatory frameworks; and (iii) balancing interests in cybersecurity and human rights. At the continental level the Report recommended: (i) harmonising definitions of cybersecurity; (ii) gathering baseline and annual statistics; (iii) promoting dialogues with national and regional stakeholders on the significance of the Convention and concerns pertaining to the ratification of the Convention; (iv) comparing the AUCC with global models and conventions and moving towards compatibility with these models and conventions; (v) promoting cybersecurity in the context of cyber stability; and (vi) broadening co-operation with African Union member states.

“the AUCC “aims at defining the objectives and broad orientations of the Information Society in Africa and strengthening existing legislations on Information and Communication Technologies (ICTs) of Member States and the Regional Economic Communities (RECs)” (AUCC, 2014) and considers that “the goal of [the] Convention is to address the need for harmonized legislation in the area of [cybersecurity] in Member States of the African Union…” (AUCC, 2014).

INTRODUCTION

Objective And Scope Of The Study

The objective of the study was to assess the laws, policies and regulations of selected African Union member states in order to develop guidelines and interventions for implementation of the AUCC in the selected African Union member states. In turn, the study aimed to contribute to the advancement of Africa’s cybersecurity posture, and the strengthening of the legal framework within which electronic transactions and the transfer of personal information take place on the continent.

To date, a number of African Union member states have developed and published policies, legislation and established institutions meeting the requirements in the provisions of the AUCC. Of the ten (10) African Union member states under study, Benin, Chad, Mauritania and Tunisia have signed the AUCC, Guinea and Senegal have ratified the AUCC and DRC, Kenya and Morocco have neither ratified nor signed the AUCC.

The Report, albeit only considering a sample of African countries, fills a gap in available information on whether measures that African states (through the sample) have established or are in the process of establishing (policy, regulation and institutions), align with the requirements of the AUCC.
Country Selection

The ten (10) African Union member states studied were selected based on several factors including:

- Countries that have signed and/or ratified the AU Convention.
- Countries with representatives in the PAP Committee on Transport, Industry, Telecommunications, Energy, Science and Technology which are collaborating with AUDA-NEPAD on the Cybersecurity project.
- Countries that are recognised ICT leaders within their respective regions (for benchmarking); and
- Regional and geographic balancing.

Assessment Criteria And Data Sources

For the purposes of the Report, we considered whether the selected African Union member states have in place legislative/regulatory, policy and institutional measures in the areas of data protection, cybersecurity and cybercrime and electronic transactions called for by the AUCC. In particular, high-level considerations were:

- What are the data protection legislative measures?
- What are the data protection policy developments?
- What are the data protection institutional measures?
- What are the cybercrime and cybersecurity legislative measures?
- What are the cybercrime and cybersecurity policy developments?
- What are the cybercrime and cybersecurity institutional measures?
- What are the electronic transactions legislative measures?
- What are the electronic transactions policy developments?
- What are the electronic transactions institutional measures?

Information gathering in accordance with the methodology, including the distribution of a questionnaire to the select African Union member states (government, private sector and academic representatives), including the exchange of information on national legislation, was conducted between July 2019 and January 2020.

FINDINGS

Cybersecurity Policy And Strategic Objectives

- Stakeholders consulted suggest differences in the governing motivation or stimulus for cybersecurity measures implemented. African Union member states may be motivated by economics, national security, or military defence. Another major difference is the scope of cyber security measures: whilst the majority of countries prioritised policy and legislation, strategies to implement policies and institutions to support implementation of policies and strategies are not as widespread.
- Guinea, Kenya, Mauritania, Morocco and Tunisia have a Cybersecurity Policy that recognises Critical Information Infrastructure, identifies the national security interests in cyberspace and recognises the need for mitigation measures. Kenya, Morocco and Tunisia have a national Cybersecurity Strategy to implement the Policy.

Laws And Regulations

<table>
<thead>
<tr>
<th>Benin</th>
<th>Chad</th>
<th>Congo</th>
<th>DRC</th>
<th>Guinea</th>
<th>Kenya</th>
<th>Mauritania</th>
<th>Morocco</th>
<th>Senegal</th>
<th>Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Data Protection Laws

| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓ |

Electronic Transactions Laws

| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓ |

Cybercrime Laws

| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓| ✓ |

* Partial Implementation / Draft Law or Regulation

The majority of member states under study have prioritised the introduction of laws and regulations in the areas of data protection, cybercrime and electronic transactions. However, of the African Union member states that have laws and regulations in place, three member states have data protection, cybercrime and cybersecurity, and electronic transaction laws that are all outdated (dating from 2000 - 2008).

Morocco:
- Law 09/08 relating to the protection of individuals with respect to the processing of personal data.
- Law 53/05 relating to the electronic exchange of legal data.
- Law No. 07/03 supplementing the Penal Code with respect to offenses relating to automated data processing systems.

Senegal:
- Law No 2008/12 on the protection of personal data.
- Law No. 2008-08 on Electronic Transactions.
- Law No. 2008/11 on Cybercrime for the substantive and procedural aspects of cybercrime.

Tunisia:
- Law 2000/63 regarding electronic commerce.
- Law No. 2004/5 relating to electronic security and on the organisation of the field of computer security and setting the general rules for the protection of computer systems and networks.
### Summary Of Findings

#### Concerning data protection

- Of the African Union member states that have laws, policies & strategies in place, the analysis pointed to three (3) member states whose data protection, cybercrime and cybersecurity, and electronic transaction laws are all outdated (dating from 2000 - 2008) and require revision. Additionally, of the African Union member states that have laws, policies & strategies in place, the study indicated that seven (7) of the member states have laws, policies and/or strategies that are in draft.

- Concerning cybercrime and cybersecurity, five of ten (5/10) member states have a policy or strategy concerning cybercrime and cybersecurity (Benin; Kenya; Mauritania; Morocco; Senegal; and Tunisia), and have either operational CERTs/CIRTs or adopted another institutional measure.

#### International Cooperation

- In Chad, Article 104 of its Draft Law on Fighting Cybercrime states that “the procedures for establishing cooperation agreements on cybersecurity and the fight against cybercrime shall be determined by regulation”, whilst Articles 105 and 106 of the same Draft Law details the procedures for mutual legal assistance between the Republic of Congo and foreign judicial authorities.

#### Emergency Response Measures

- The Member states under study have had both successes and failures in the area of CERTs/CIRTs. Sub-Saharan African countries were slower to join the progression. South Africa, Nigeria and Kenya are further examples of success. A measure of success is the ability of the newly created CERT to be accepted as a full member at the Forum for Incidence Response Teams (FIRST). The process has rigour. In addition to an application, the country applying requires two sponsors and to go through a review process to prove a certain level of competence. Tunisia was the first country in Africa to receive FIRST membership followed by Egypt, Morocco and three CERTs (associated with financial institutions) in South Africa. In 2015, Nigeria and Kenya became official members. Out of the 326 teams belonging to FIRST, so far, Africa has eight.

- In the study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

### Table: Institutional Measures

<table>
<thead>
<tr>
<th>Benin</th>
<th>Chad</th>
<th>Congo</th>
<th>DRC</th>
<th>Guinea</th>
<th>Kenya</th>
<th>Mauritania</th>
<th>Morocco</th>
<th>Senegal</th>
<th>Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Partial Implementation / Draft Law or Regulation

### Table: Emergency Response Measures

- The Member states under study have had both successes and failures in the area of CERTs/CIRTs. Sub-Saharan African countries were slower to join the progression. South Africa, Nigeria and Kenya are further examples of success. A measure of success is the ability of the newly created CERT to be accepted as a full member at the Forum for Incidence Response Teams (FIRST). The process has rigour. In addition to an application, the country applying requires two sponsors and to go through a review process to prove a certain level of competence. Tunisia was the first country in Africa to receive FIRST membership followed by Egypt, Morocco and three CERTs (associated with financial institutions) in South Africa. In 2015, Nigeria and Kenya became official members. Out of the 326 teams belonging to FIRST, so far, Africa has eight.

- In the study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

### Table: International Cooperation

- In 2009 the Beninese government drafted a Decree No. 200/MISP/DC/SGM/DGPZ/SRCT/DER/SA related to the creation of a division responsible for the fight against cybercrime. The decree stipulates that the victims of internet crime can approach Interpol or the local authorities regarding the incidence of cybercrime. Further, Article 624 within Book Six of Benin’s Digital Code sets out mechanisms of international cooperation.

- In Chad, Article 104 of its Draft Law on Fighting Cybercrime states that “the procedures for establishing cooperation agreements on cybersecurity and the fight against cybercrime shall be determined by regulation”, whilst Articles 105 and 106 of the same Draft Law details the procedures for mutual legal assistance between the Republic of Congo and foreign judicial authorities.

- In Guinea, international cooperation on combating cybercrime is mandated under Article 106 of Law 2016/037 on cybersecurity and the protection of personal data, whilst Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital Economy sets out certain functions on this Ministry to participate in international cooperation efforts (including treaties, conventions etc) and overseeing their implementation within the Republic of Guinea.

- In Kenya, provision for international cooperation in tackling cybercrimes is made under Part V of the Computer Misuse and Cybercrimes Act of 2018.

- Mauritania is required to co-operate with any international organization in the investigation / prosecution of cyber-criminal offences in terms of national reciprocal legislation and/or international legal instruments under Article 50 of Law No. 2016/007 on cybercrime.

- In Morocco, its National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) considers the promotion of national and international cooperation as one of its strategic objectives.
In the study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

In Morocco, its National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d’Information) considers the promotion of national and personal data, whilst Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital the fight against cybercrime shall be determined by regulation”, whilst Articles 105 and 106 of the same Draft Law details the procedures for mutual legal

In Chad, Article 104 of its Draft Law on Fighting Cybercrime states that “the procedures for establishing cooperation agreements on cybersecurity and of cybercrime. Further, Article 624 within Book Six of Benin’s Digital Code sets out mechanisms of international cooperation.

The decree stipulates that the victims of internet crime can approach Interpol or the local authorities regarding the incidence

In 2009 the Beninese government drafted a Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division responsible for

International Cooperation

institutions) in South Africa. In 2015, Nigeria and Kenya became official members. Out of the 326 teams belonging to FIRST, so far, Africa has eight

Emergency Response Measures

Continental Level

Regional Level

Support legislative harmonisation at member state level

At the regional level, several initiatives have focussed on developing regional model legislation in the three focus areas of the AUCC, related to data protection, electronic transactions and cybercrime. These include the ECOVAS Cybersecurity guidelines\(^1\), the ECCAS Model Law/CAMC Directives on Cybersecurity\(^2\) and the SADC Model Law on data protection, e-transactions and cybercrime\(^3\). Regional support for national implementation of legislation including the drafting of legislation and regulation that give effect to legislation, and capacity building for institutions that have oversight of the legislation, are needed.

Continental Level

Harmonised definitions of cybersecurity

Global studies show that in developed and developing worlds, harmonised definitions of cybersecurity is a transversal issue. France for instance defines cybersecurity as “an information system allowing to resist likely events resulting from cyber space which may compromise the availability, the integrity or confidentiality of data stored, processed or transmitted and of the related services that Information and Communication (ICT) systems offer” (Luijif, Besseling & Spoelstra et al., 2013), whilst the UK views cybersecurity as “embracing” both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers” (Luijif, Besseling & Spoelstra et al., 2013). The above comparison shows a distinction in where cybersecurity is located, a priority at the information system level or a priority at the national security level. Harmonised definitions of cybersecurity are needed at the continental level.

Baseline and Annual Statistics

Both baseline data on cybersecurity legislative, policy and institutional measures and annual updates will be valuable in assessing successes and challenges and targeted support (at the continental level) for advancing such cybersecurity measures in Africa. The AUCC refers to monitoring and evaluation mechanisms to assess implementation – such mechanisms may provide the baseline and annual research needed.

Promote dialogues with national and regional stakeholders on the significance of the Convention and concerns pertaining to the ratification of the Convention.

There must broader engagement with Member states on reservations concerning the Convention. The Pan-African Parliament and the African Internet Governance Forum may be used to broaden engagement with national stakeholders. Drawing on a lesson from the EU, the AU could consider creating a body similar to the European Network and Information Security Agency (ENISA) at the continental level. African states and the AU should consider applying the World Economic Forum’s A Call for Agile Governance Principles\(^4\) in future legislation on technology.

Compatibility and Comparison with Other Models and Conventions

Over the course of the study, African Union Member States raised concerns relating to the compatibility of the provisions of the AUCC with the provisions of the Budapest Convention on Cybercrime, as well as compatibility with regional model laws and treaties.

In total, seven member countries have signed and ratified the Budapest Convention (Benin, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria and Senegal). The Budapest convention was the first international effort to provide guidelines for countries to develop their national legislation and establish a framework for international cooperation. Regional models include the ECOVAS Cybersecurity guidelines, the ECCAS Model Law/CAMC Directives on Cybersecurity and the SADC Model Law on data protection, e-transactions and cybercrime.

It is recommended that at the continental level, guidance is provided to African Union member states on how to deal with conflicting requirements from the various regional, continental and instruments, particularly where such requirements may be in conflict with one another.

Promote cybersecurity in the context of cyber stability

Cyber stability has been defined as “a geo-strategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels” (Orijii, U.J., 2012). Continental bodies must promote cybersecurity in the context of its geostrategic character encompassing the many facets of benefits and harms permeating the various areas of life.

Broaden co-operation with Countries

Member states raised the need for in-country support for countries implementing cybersecurity measures. Facilities to support countries drafting policies, legislation and establishing the institutions called for by the Convention may be considered at a continental level.

\(^{1}\) ECOVAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary session of the ECOVAS Council of Ministers at Abuja, Nigeria (August 2011).


About Knowledge Partner

This report was prepared independently by EndCode.

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.

Disclaimer

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AU-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AU-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AU-NEPAD.
In the study and sample, five (5) of the ten (10) countries (Benin, Chad, Kenya, Morocco and Tunisia) have operational CERTs/CIRTs.

Summary Of Findings

International Cooperation

In Morocco, its National Cybersecurity Strategy (Stratégie nationale en Sécurité des Systèmes d'Information) considers the promotion of national and international cooperation as one of its strategic objectives.

In Mauritania, there is no explicit mention of international cooperation in the context of cybercrimes. However, in terms of national security, the country mandates the co-operation with any international country in the investigation/prosecution of cyber-criminal offences in terms of national defence and security interests in cyberspace and recognises the need for mitigation measures. Kenya, Morocco and Tunisia have a national Cybersecurity Strategy.

In Kenya, provision for international cooperation in tackling cybercrimes is made under Part V of the Computer Misuse and Cybercrimes Act of 2018.

In Guinea, international cooperation on combatting cybercrime is mandated under Article 106 of Law 2016/037 on cybersecurity and the protection of personal data, whilst Article 1 of Decree D/2018/175/PRG/SGG on the Powers and Functions of the Ministry of Posts Telecommunications and Digital Economy of GUINEA-BISSAU makes provision for international cooperation.

In Tunisia, there is no explicit mention of international cooperation in the context of cybercrimes. However, in terms of national defence and security interests, the country mandates the co-operation with any international country in the investigation/prosecution of cyber-criminal offences in terms of national defence and security interests in cyberspace and recognises the need for mitigation measures.

In 2009 the Beninese government drafted a Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division responsible for international cooperation in the fight against cybercrime. Further, Article 624 within Book Six of Benin’s Digital Code sets out mechanisms of international cooperation.

International Cooperation

In 2009 the Beninese government drafted a Decree No. 200/MISP/DC/SGM/DGPN/SERCT/DER/SA related to the creation of a division responsible for international cooperation in the fight against cybercrime. Further, Article 624 within Book Six of Benin’s Digital Code sets out mechanisms of international cooperation.

In South Africa, the FIRST Cyber Security fragility of success is the ability of the newly created CERT to be accepted as a full member at the Forum for Incidence Response Teams (FIRST)³. The process has rigour. In addition to an application, the country applying requires two sponsors and to go through a review process to prove a certain level of competence. Tunisia was the first country in Africa to receive FIRST membership followed by Egypt, Morocco and three CERTs (associated with financial institutions) in South Africa. In 2015, Nigeria and Kenya became official members. Out of the 326 teams belonging to FIRST, so far, Africa has eight member CERTs/CIRTs.

Emergency Response Measures

Institutions

Institutional Measures

Institutional Measures

Objective And Scope Of The Study

INTRODUCTION

The Member states under study have had both successes and failures in the area of CERTs/CIRTs². Tunisia, Egypt and Morocco have built effective emergency response measures. In contrast, the Emergency Centre for the Prevention and Management of Cyberspace Incidents (CEEIC) in Kenya has had limited success so far due to a lack of operational experience, limited resources and low awareness.

Institutional Measures

Institutional Measures

RECOMMENDATIONS

At the national level, the Report recommended African Union member states to consider: (i) drafting or reviewing of outdated legislative and regulatory measures in the areas of data protection, cybersecurity and cybercrime and electronic transactions called for by the AUCC. In particular, high-level policy development is recommended to ensure that national and regional ICT and cybersecurity strategies are not as widespread.

What are the electronic transactions policy developments?

What are the electronic transactions legislative measures?

What are the cybercrime and cybersecurity institutional measures?

What are the cybercrime and cybersecurity legislative measures?

What are the data protection institutional measures?

What are the data protection policy developments?

What are the data protection legislative measures?