International Cyber Security Diplomatic Negotiations: Role of Africa in Inter-Regional Cooperation for a Global Approach on the Security and Stability of Cyberspace

Ms Souhila Amazouz

A dissertation presented to the Faculty of Arts in the University of Malta for the degree of Master in Contemporary Diplomacy, Specialization in Internet Governance

March 2019

Declaration of Intention

I hereby declare that this dissertation is my own original work

Souhila Amazouz

31 March, 2019

Addis Ababa, Ethiopia

Acknowledgements

I wish to thank my advisors Prof. Jovan Kurbalija and Vladimir Radunovic for their careful supervision of this dissertation and their valuable comments.

I also wish to thank Patrick Borg of DiploFoundation for all his help, understanding and patience during the entire process of this Master's Degree.

I would also like to thank my friends and colleagues Nabila, Dorothy, Awa and Lamia for their support.

Dedication

To my dear mother Djedjiga Berkane, this dissertation is dedicated to you.

Abstract

This research paper examines African countries cybersecurity readiness and how Africa can play a role in shaping international negotiations and discussions on global cybersecurity governance.

A review and analysis of the existing national and regional cybersecurity policies and strategies as well as the Internet Governance frameworks in African countries will give us a complete picture on how Africa, as a region, deals with the changes and challenges related to the new digital environment.

In addition to an analysis of existing platforms, laws and instruments related to peace & security and fighting against organised crime and terrorism, both at regional and continental levels, to see how it would be possible to use them or adapt them to the reality of cyberspace. This research paper will present mechanisms and processes to facilitate coordinating views and positions of African actors on international cybersecurity policy. This will allow African decision makers and diplomats to debate on international cyber security policy and politics at the level of the African Union, sensitize African leaders on strategic importance of cyber space and the geopolitics surrounding cyber dialogues to enable Africa to develop its common position in line with its economic and political interests.

The dissertation will highlight the need for Africa as a region to play an active role in regulating this new digital world which is already marked by cyber dominations as cyber technologies impact the global economy, human rights and international peace and security.

Table of Contents

Introduction Chapter

Background

Today the world is marked by globalization and digitalization, with more than half of the world's population online which means that 3.9 billion people (51.2% of world population) have integrated the global network (Cyberspace) by using Internet to either communicate, entertain or to perform critical daily activities (International Telecommunication Union [ITU] (2018a).

The US' Homeland Security defines Cyber space as "the interdependent network of information technology infrastructure that includes Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries" (Government of the USA, 2008).

The transformative power of cyber technologies as an enabler for social progress and economic growth as well as the huge impact of ICTs on empowering and changing lives of people have been proven and recognized all over the world (United Nations Conference on Trade and Development [UNCTAD], (2017).

Furthermore, according to Ebert and Maurer (2013), cyberspace has become a space of great strategic, economic and political stakes. Today, we cannot imagine the world without the use of cyber technologies: we rely more and more on interconnected and

inter-dependent global networks and infrastructure to perform critical activities, including states actions, such as security and delivery of government services.

However, the increasing number of cyber incidents constitutes a major concern across the world. Protection and prevention against sophisticated and large scale cyber-attacks is a real challenge. The security of the cyber environment represents the new planetary emergency that threatens national and international security and amplifies traditional security risks, such as cross-border organized crime and terrorism.

In this regard, cybersecurity is described by the International Telecommunication Union as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets". Cybersecurity strives to ensure the general security objectives of cyber domain that includes availability, integrity and confidentiality (International Telecommunication Union [ITU], (2008a)).

Moreover, the ITU Global Cyber Security Agenda (GCA) defines cyber Security as actions and safeguards aiming at enhancing security and building trust in the use of ICT applications (International Telecommunication Union [ITU], (2007).

Nonetheless, states across the world do not use the same terminology when it comes to the regulation and security of cyberspace as they view cybersecurity concepts differently. For instance, Western countries see cybersecurity as the protection of cyber domain, including networks, infrastructure and information systems against cyber threats and cyber-attacks, while China, Russia and their allies use the term information security instead of cybersecurity to refer to strategic control of information and content to protect their societal- political and economic-social systems against cyber threats that may affect their national sovereignty (Radunovic, 2017a).

Therefore, the security of global cyberspace requires cyber security frameworks, as well as regional and international cooperation to ensure peaceful use of cyber space by states and non-state actors. Most digital advanced states see cyberspace as a source of cyber domination and economic power. According to reports recorded in the Digital Watch map, there is a growing number of states developing their cyber offence and cyber defense capabilities. Even though there are very few documented cyber-attacks officially attributed to governments, the international community worries about the militarization of cyberspace and calls for adopting multilateral approaches and enhancing international cooperation to avoid misperceptions and escalation of tensions in cyber domain.

Several international and regional cyber dialogues and diplomatic initiatives are underway, seeking to regulate state and non-state operations in cyberspace, at the United Nations (UN) level and also at regional intergovernmental organizations, such as the

European Union (EU), the Organization of American States (OAS) and the Association of Southeast Asian Nations (ASEAN), as well as at a bilateral level, with a growing number of cyber agreements and cyber partnerships among states.

For all states and regions around the world, maintaining security and stability in cyber space, protecting the global digital economy, as well as promoting human and people rights in the digital environment are among the key priorities of the 21st century. However, it is worth noting that ongoing debates and discussions on establishing global cybersecurity frameworks or treaties, as well as defining norms of responsible behavior in cyberspace are led by the most powerful states which, most of the time, follow their national interests without real involvement of developing countries and regions, such as Africa.

For Africa, the majority of countries is not aware of the strategic importance of cyberspace and is yet to develop their national cyber capacities or to participate in international cybersecurity policy debates, as they are still in the process of deploying their ICT infrastructures and providing access to digital services to their populations.

While substantial progress has been noticed at a national level in some African countries, a lot remains to be done at sub regional and continental levels to build the digital trust, guarantying respect of online rights of African citizens, through enhancing cooperation across the Continent and coordinating Africa position on international cybersecurity

policy and ensuring active participation of African nations in shaping the governance of the digital world.

Purpose of the research:

This dissertation aims to help African policy makers and diplomats to better understand the cybersecurity landscape in Africa, the international dimension and complexity of cybersecurity policymaking and its implications on inter states diplomatic relations and international security.

The objective of this research is to make an analysis of the international discussions and diplomatic initiatives related to the security and stability of global cyberspace, identify the reasons why developing countries, and particularly African countries, are not fully involved in international cyber dialogues, either in multilateral or bilateral settings.

This research paper aims also at identifying the social, economic and political drivers for raising awareness on cyber issues and building cyber capacities of African states. It proposes solutions to enhance intra-Africa cybersecurity cooperation, put cyber security high on the political agenda of African leaders and prepare the Continent to play an active role and speak with one voice in international cybersecurity policy discussions.

Research Objectives:

The dissertation shall explore and discuss the following research questions. These questions will also guide the research and literature review:

- Why ongoing international bilateral and multilateral discussions and diplomatic initiatives related to the security and stability of the global cyberspace are led and dominated by powerful states;
- Why developing countries and regions, such as African states are not fully involved in the international cybersecurity policy dialogues;
- Have African countries reached a cybersecurity maturity level that allows them to participate and play an active role in international fora;
- What are the driving forces for the development of national and regional cybersecurity frameworks in Africa – what mechanisms are needed to address cybersecurity in Africa both at legal, institutional technical, operational and political levels;
- How to bring cybersecurity on the top of the political agenda of African nations;
- How the African Union, through its existing policy organs, platforms and structures can take the lead to organize and facilitate comprehensive and structured cyber cybersecurity dialogues within the region to define Africa cyber principals, Africa Cyber norms, CBMs and Africa International cyber security policy to guide Africa participation and negotiations at an international level.

Research Methodology

This research paper is being based on desk research, in addition to getting information and views of African policy makers and experts from national, regional and continental organizations dealing or required to deal with cybersecurity issues.

This paper aims at integrating the literature review and analysis of a wide range of resources, namely relevant publications and journals, critical Government policy documents, UN resolutions, AU Summit decisions, official statements, as well as secondary sources.

For the design of my research, I have used mainly written sources as a tool for a descriptive analysis of findings in the literature gathered in this area of study. The qualitative methods have been employed to conduct this research to gather data related to international cybersecurity policy initiatives and Africa cybersecurity landscape, as well as information related to African Union Peace and Security Mechanisms and Structures.

To address the research questions and explore ways to sensitize African policy makers on the political and economic implications of the international cybersecurity policy discussions, I have examined current cyber security diplomatic initiatives and measures taken at an international level to counter malicious use of ICTs, both the formal discussions held at the UN and inter-governmental organisations and the informal discussions taking place in forums and conferences, with special focus on Africa state and non-sate actors participation and Africa representation in International Fora.

To assess the cybersecurity readiness of African countries and address the information gap with regard to African states cyber diplomacy initiatives and partnerships, I rely on available African government's policy documents and official statements, and I shall,

then, focus on the analysis of three relevant aspects (policy and governance, cyber legislations and Incidence response mechanisms such as Computer Emergency Response Team (CERT) or Computer Incident Response Team (CIRT).

As African countries are mainstreaming digitalization in their economies and societies, I have conducted a research to show the relationship between Africa digital agenda and cybersecurity and I also will try, with some examples and statistics, to show major cybercrime activities affecting the security, economy and social wellbeing of African people.

To enable African countries to debate on cybersecurity policy and politics, in the context of international security, and after an analysis of the African Union components, I propose a structure that enables the use/reuse of the exiting decision-making organs and structures, as well as the peace and security platforms to address cyber issues by adapting them to the reality of the digital environment.

As the dissertation is related to Africa Participation in International Cyber security policy debates, through my research, I highlight the importance for AU Member States to develop cyber diplomacy capabilities and involve Ministries of Foreign Affairs (MFAs) in formulating national and continental cybersecurity policies and focus more on international cooperation and cybersecurity politics to guide Africa participation, as a region, in International cybersecurity initiatives, and help African governments to engage

more in bilateral and/or multilateral cyber dialogues and agreements with other states and regions to safeguard the political and economic interests of the African nations.

Chapters review:

The dissertation is organized into four chapters:

Chapter1 examines the international cybersecurity discussions and negotiations, both the formal and informal processes, with focus on Africa participation.

Chapter 2 reflects the cyber security readiness of the Continent with an analysis on existing policy, legal, regulatory, organizational and institutional frameworks within Member States of the African Union.

Chapter 3 is dedicated to the driving forces that may stimulate and push cybersecurity high on the Agenda of African leaders, along with the Africa digital transformation agenda and Africa security policy that may have implication, on the stability of the Continent.

Chapter 4 highlights the role the African Union, as well as its policy organs, mechanisms and platforms in organizing cybersecurity conversations to identify basic principles and norms of conduct in African Cyber space, develop Confidence Building Measures (CBMs) adapted to the African context, develop comprehensive cyber capacity programs,

coordinate Africa participation in international fora, notably at the United Nations level, and work with African States towards developing an Africa cyber engagement strategy to guide Africa cyber dialogues and partnerships.

Literature Overview

This part summarizes the pre-existing Literature from the perspective of what other authors' research suggests, with regard to Africa cybersecurity trends and participation in international cybersecurity policy discussions and initiatives.

The aim is to highlight the major accomplishments in relation to Africa cybersecurity agenda and to examine the cyber maturity of African states to see how a coordinated continental approach will enable African nations to play an active role in shaping the governance of global cyberspace in a way that preserves Africa interests as a region.

This part focuses on papers and publications that analyzed the process and initiatives undertaken at the international level to address the challenges of regulating cyberspace as common space and shared responsibility. It aims at stressing on understanding Literature and underlying reasons for success and failures, while demonstrating the lack of information in most policy documents on African countries positions and involvement in international cyber dialogues.

I will briefly analyze a number of works that have been studied for the elaboration of this dissertation and will organize this review as it was conducted during my research, from

the most relevant to the most specific information in relation to the topic of this dissertation.

To understand the international cyber security policy, I have consulted the major writings in this arena, major policy papers, UN resolutions and reports, statements related to formal discussions and processes within the framework of the United Nations and its agencies, as well as regional inter-governmental organizations, such as the African Union (AU), EU, OAS, ASEAN and papers related to the informal initiatives which are becoming alternative platforms for open and inclusive discussions on cybersecurity policy and governance, such as the Global Commission on the Stability of Cyberspace (GCSC), Global Conference on Cyberspace (GCCS), the Global Forum on Cyber Expertise (GFCE) and the Internet Governance Forum (IGF), in addition to some relevant publications. The Literature review suggests that most authors do not reflect on developing countries participation.

For instance, Maurer (2011) provides an analysis of the UN's activities on cybersecurity where he outlined definitions and concepts related to international cybersecurity policymaking at the United Nations, with focus on cyber-warfare and cybercrime which are addressed at UN with different organizational platforms and approaches. Maurer emphasized on cyber norms emergence process and cybersecurity negotiations that are marked by geopolitics and the relationship between actors, as well as the divergent views and positions between western states and Russia and its allies. However, Maurer did not

show developing states perceptions on cybersecurity discussions under the umbrella of the United Nations.

Radunovic (2017a) provides an overview of the international dialogue on establishing the norms of state behaviour and confidence-building measures (CBMs) aiming at maintaining peace and security in cyberspace. In his analysis, he reviewed major international and regional diplomatic initiatives and instruments, with a focus on the efforts of the United Nations, the Organization for Security and Co-operation in Europe (OSCE), ASEAN Regional Forum, OAS, and Shanghai Cooperation Organisation (SCO), the G20 and NATO. The paper did show real analysis on Africa efforts and commitment to build cybersecurity frameworks and does not reflect Africa perception and/or involvement in International cybersecurity policy dialogues.

The United Nations Institute for Disarmament Research [UNIDIR] (2011), while assessing cybersecurity and cyberwarfare in courtiers across the world, the number of African countries cited in the document is limited and the information provided in the report most of the time does not help to get a real picture on African countries investing in cyber security and cyberwarfare capabilities. Moreover, the assessment on the work and role of international and regional organizations in regulating cyberspace did not mention the African Union or any African regional organisation.

To assess the maturity level and identify the common priorities of African countries with regards to cybersecurity, I gathered information on the national cybersecurity frameworks (policy, legal, technical and institutional) of all African countries, using- mainly- Government websites and official publications. Although not all African countries publish their legal and policy documents.

Symantec's 2016 report provides information on cyber security readiness of only 32 countries over 55 and it does not cover international cooperation as it does report on cyber engagements or partnerships established by African countries to strengthen their cyber capacities (Symantec, 2016).

Regarding the regional and continental initiatives, legal instruments and mechanisms that aim to reinforce cooperation for the security of the African cyberspace, I consulted, particularly, available publications in addition to some publications of African authors.

Orji (2015) gave an overview on cybersecurity law and regulations in Africa. But when he developed the response of African countries to cyber security challenges, he just stressed on 23 countries over 55, while he provided an analysis on the lack of mutual legal assistance (MLA) agreement among Africa sub regions that may be extended to facilitate cooperation in cybercrime investigations.

To show the importance for Africa to build trust in its cyberspace, I highlighted the engagement of the Continent for the digitalization and need to cultivate trust and confidence in the use of cyber technologies. I tried to show how African countries are affected by cyber-attacks, either generated inside the Continent or coming from other regions like WannaCry that affected several African organisations. In this chapter, I referred mainly to AU Summit policy documents, AU Ministerial declarations and to some African Websites to give examples on criminal activities targeting national economies.

To highlight the role of the African Union, in working with African States towards enhancing cooperation to combat malicious use of digital technologies, developing Africa cybersecurity policy to guide Africa cyber engagements and partnerships, in line with Africa policy and vision for an integrated, prosperous and peaceful Africa, I consulted and analyzed AU policy documents, available publications of African authors and official statements and meetings reports. As a result, the literature review shows a lack of consideration of cyber issues in most AU policy documents and security treaties.

For instance, Bedzigui (2018) stressed the need to harmonise AU response to conflicts prevention, governance structures and post conflict solutions, but did not highlight cyber issues as an important aspect of maintaining peace and security in Africa.

Tamarkin (2015), in his report on AU's Cybercrime response, focused on analyzing legal instruments, such as the Malabo Convention and the sub regional model laws, but did not emphasize on intra-Africa cooperation to fight cybercrime and how to create dialogues and consolidate efforts towards common African policy to deal with international initiatives in cyberspace.

In conclusion, there is a lack of a comprehensive work and analysis of Africa cybersecurity landscape, including trends and cyber threats targeting the region. In addition to the lack of reports and statements on Africa participation in international cybersecurity policy discussions, both in formal and informal meetings, as well as information gap regarding Africa cyber engagements and positions on international cyber politics.

Chapter 1

1.1. Africa Involvement in International Formal and Informal Cyber policy debates

For today modern societies, cyberspace or digital space is about interconnected transnational and borderless networks or telecommunication systems (Maurer, 2011) which are directly linked to social development and economic growth as well as to national security and prosperity of states.

Due to global nature of networks, Information Communication Technologies (ICTs) have added a complex dimension to inter-state relations. Moreover, cybersecurity threats are considered among the main concerns of the 21st century that can affect the international security and stability notably with the yearly increase number and degree of sophistication of Cyber-incidents.

Nevertheless, the motivations of cyber-attacks may vary from using ICTs or Internet by individuals to perpetrate criminal activities to a state sponsored cyber operations that may target critical national infrastructure or information systems of other countries to disrupt their social, economic or political environments.

In recent years, cybersecurity has come to the forefront of diplomatic and political agenda of important bilateral and multilateral meetings, particularly due to the reported large scale cyber-attacks and data breaches that affected several states and infected hundreds of thousands of computers across the world these last years. For instance, WannaCry

(Volz, 2017), and NotPetya (BBC News, 2018a) two malicious cyber-attacks attributed respectively to North Korea and Russia, as well as other major data breaches, such as the Facebook case where up to 87 million users were affected by Cambridge Analytica's improper collection and using of personal information of internet users for political and commercial purposes (Metcalf, 2018), in addition to cyber conflicts activities, such the attack on Sony servers in 2014, officially attributed by the US government to North Korea and the alleged Russian attack against the Democratic National Committee and US elections in 2016 (Radunovic, 2017b).

In a blog post, Beaver (2016) reflects on the emergence of cyberwarfare capabilities among lead powers, like the United States, Russia and China, which have announced publically the existence of cyberwarfare units among their militaries. Also as revealed by Clapper *et al* (2017) in the joint statement for the record to the U.S Senate Armed Services Committee, as of late 2016 more than 30 nations developed offensive cyber-attack capabilities .This contributes in making security of cyber space more challenging for less digital advanced countries.

While the proliferation of offensive cyber capabilities is increasing at an alarming rate, the search for cybersecurity governance mechanisms is underway, both in formal and informal consultations, with regional and international diplomatic initiatives.

According to Kurbalija (2018), to ensure legitimacy of the cyber dialogues and facilitate the implementation of any international agreed outcomes or recommendations, the world needs more inclusive and transparent cybersecurity processes and negotiations.

The search for global Cybersecurity mechanisms and treaties to address the emerging cyber threats are conducted in formal negotiations both at bilateral and/or multilateral levels and also in informal fora with participation of state and non-states actors in shaping digital policies.

1.2. Formal cybersecurity diplomatic initiatives

1.2.1. The United Nations

As a global governing body with large states participation and outreach, the United Nations has been trying to maintain a meaningful conversation on cybersecurity for the last 15 years, mainly through the establishment of the Group of Government Experts (GGE), to discuss international cyber policies. The UN General Assembly (UNGA) has approved a number of resolutions related to information security and state use ICTs.

In fact, Cyber security became an agenda item of the United Nations General Assembly (UNGA) since 1998, with the adoption of the Resolution 53/70 (UNGA, 1998) entitled "*Developments in the field of information and telecommunication in the context of international security*" that recognized the benefits of ICTs and acknowledged the risks related to its misuse.

In 2000 and 2001, UNGA adopted resolutions 55/63 (UNGA, 2000) and 56/121 (UNGA, 2001) on establishing legal basis for combating criminal misuse of Information technologies. The call for more awareness on the implications related to the use of ICTs and the need for creation of global culture of cybersecurity came with Resolution 57/239 (UNGA, 2002), while resolution 58/199 (UNGA, 2003a) calls for the protection of critical information infrastructure and cooperation among states through sharing information and best practices. The resolution proposed elements for protecting critical information infrastructures that should be implemented and invited states that developed national cybersecurity frameworks to assist other UN nation members to develop cyber capacities.

Moreover, the UNGA resolution 58/32 (UNGA, 2003b) requested the UN Secretary General to consider existing and potential threats in cyberspace, as well as possible cooperative measures to address them. Through this resolution, UN members requested the Secretary General to conduct a study on the use of ICTs for civilian and military applications, with the assistance of a group of governmental experts to be appointed by him on the basis of equitable geographical distribution, and to submit a report on the outcome of the study to the General Assembly.

The resolution 58/32 (UNGA, 2003b) paved the way for the creation of the first Group of Government Expert under the UN auspices in 2004. This group was composed of 15

members and was marked by the participation of two African countries i.e. Mali and South Africa. The group published a procedural matters document A/60/202 (UNGA, 2005) but, unfortunately, did not agree on any substantive report to submit to the UN Secretary General.

According to the UN Office for Disarmament Affairs (UNODA), the disagreement among GGE members was related to two policy issues. The first issue was related to identifying the impact of ICT development on national security and military affairs, as well as dealing with the emerging threats related to the exploitation by states of vulnerabilities to build cyber capabilities. And the second issue was about controlling the trans-border information content that divided the GGE members, while the United States and its allies emphasize the protection of digital networks and critical information infrastructures, Russia, China and their partners emphasize the information security and controlling content and communications that may threaten the state stability (Segal and Waxman 2011).

The second GGE was created in 2009 and came up with a consensus report A/65/201 (UNGA, 2010) which was submitted to the UNGA for adoption in 2010. Among its recommendations, the need for dialogues on state responsibility in the use of ICTs, confidence building and risks mitigation, information exchange on national ICT security strategies and ICT legislations, as well as recommendation on capacity building for

developing countries. This GGE was made of 15 members, with participation of South Africa as the only representative of Africa.

The third GGE, made of 20 members, came up with a substantial consensus report A/68/98 that was adopted by the UNGA in 2013. The report clearly outlined the applicability of International laws, in particular the UN charter, to cyberspace, as well as the role the UN may play in promoting dialogues among states on cyber issues. The report recognized state sovereignty over its cyberspace, as well as its jurisdiction over ICT infrastructures located within its territory. The GGE report introduced the norms, rules and principals of state behavior in cyberspace and emphasized on capacity building in a global effort where advanced states and UN agencies are requested to assist less developed countries in securing ICTs and their use. African countries were represented in this group by Egypt.

The fourth GGE, established in 2014, also agreed on a consensus report A/70/174 with substantive recommendations adopted by the UNGA in June 2015. The findings of the report were notably related to codification of voluntary and non-binding norms for sates use of ICTs. With focus on the respect of human rights and fundamental freedoms in cyberspace, Confidence Building Measures (CBMs) and peaceful settlement of disputes, international cooperation to increase stability and security in the use of ICTs, in addition to highlighting the role of UN in promoting dialogues among sates for developing a common understanding on how international laws and norms apply to cyberspace. The

number of GGE members increased from 15 to 20 and it was marked by the participation of three African countries, namely Egypt, Kenya and Ghana.

The 2016/2017 group was established in accordance with Resolution 70/237 (UNGA, 2015b). The GGE was expanded to 25 members with participation of four African countries Kenya, Egypt, Botswana and Senegal. The group was unable to reach consensus and the report was not submitted to the UNGA consideration. The fundamental disagreement among the members was related to the application of UN charter principles in cyberspace, notably the state right to self-defense or retaliation to international cyber-attacks as per the article 51 of the UN Charter which was outlined in the draft GGE report as the right of states to respond to internationally cyber-attacks committed through the use of ICTs (Tikk and Kurten, 2017).

In an official statement Michele Markoff, the US representative attributed the lack of consensus on the final report to "the reluctance of a few participants to seriously engage on the mandate on international legal issues" (Government of the USA, 2017). While Cuba's representative expressed his opposition along with other states to the application of humanitarian law in cyber space and argued that this may legitimize armed conflicts and military actions in the context of state use of ICTs (Government of Cuba, 2017).

The divisive views on state behaviour in cyberspace between the super powers led to the adoption of two different resolutions in relation to cybersecurity in December 2018. The

Resolution A/RES/73/27 (UNGA, 2018a) sponsored by the Russian Federation calling for establishing regular institutional dialogues under the auspices of the United Nations in form of an Open-Ended Working Group (OEWG) and a second Resolution A/RES/73/266 (UNGA, 2018b) sponsored by the United States calling for the continuation of the GGE process and emphasise more on cooperation and coordination among states and respect of human rights and freedoms in cyberspace. (Brown, 2019).

The vote on the two resolutions shows a split among African countries, while almost all African states voted in favour of the Russian resolution, seven (07) abstained (Somalia, Chad, Cameroon, Benin, Senegal and Gabon). On the other hand 18 countries supported the American resolution and 15 abstained while Egypt and Zimbabwe voted against, this shows that Africa position was not coordinated as a region and most countries followed their own military and political alliances. Furthermore, it is worth noting that 18 African countries voted in favour of both resolutions which reflects the lack of awareness of African states on the political stakes and nuances between the two blocks on international cybersecurity policy.

The creation of the OEWG offers a space for African states to participate in the global discussions on international information security. However, the lack of capacity of African diplomats based in New York on cyber diplomacy and also in the absence of structured discussions at the African Union to shape and coordinate Africa cyber policy positions, it will be a real challenge for African delegates to defend common interests.

Since 2004, discussions and exchange of views of the different Governmental Experts Groups on the development of ICTs in the context of international security were dominated by the five Permanent Representatives of the UN Security Council and other emerging digital powers such as India, Brazil, Germany and Israel. The deliberations of the different GGEs revealed deeply diverging views among these states on their approaches to the global cybersecurity. Moreover, as discussions are undertaken in the first UNGA Committee (disarmament and International Security), The GGEs outcomes and recommendations are relatively influenced by global geopolitics.

According to experts (Segal and Waxman, 2011), different interests among powerful states stemming from their strategic priorities, internal politics, and public private relationships, continue to impact the vision on how global cyberspace should be used, regulated and secured. So far, two poles have been created, namely with the United States and their allies at one and China and Russia at another, with different views on information security and Cybersecurity. Many growing Internet powers and developing states lie in between and did not take position such as African countries.

The political motivations of major GGE powers are clearly reflected in some recommendations, such as the right to self-defense included in 2017 report that aim to give advantage to the states that have developed offensive cyber capabilities in adopting countermeasures to react to wrongful international cyber operations.

Although the previous recommendations of the GGE reports remain not legally binding as they do not reflect a participation of the majority of countries across the world, they represent a great achievements in shaping international cyber relations as they are developed under the auspices of the United Nations.

However, it is worth noting that African countries are not fully participating in this process and most of them are not aware about the challenges and stakes of these discussions and their impact on their national and international security and stability. For instance, the outcomes of the 2013 and 2015 GGE reports that, among other concerns, include states obligations to secure their critical infrastructure from ICT threats and also states responsibility in case of severe cyber incidents committed in their cyberspace or attributed to them. This may put some African countries in weak positions as they do not have yet the required capacity to monitor and protect their digital networks against the very sophisticated cyber-attacks and infiltrations (Symantec, 2016).

Moreover, the participation of Africa as a region in this important cyber policy multilateral debates is limited to individual representation of countries but not coordinate and not framed to speak on the name of the entire Continent and, even though African countries joined the GGEs since 2004, no official statements or reports were publically released by African delegates to express a common African position on the outcomes of the GGEs.

Furthermore, most African countries did not react to the Resolution 64/211 (UNGA, 2009) and Resolution 70/237 (UNGA, 2015b) calling for a voluntary self-assessment of national efforts to protect critical information infrastructures. Only three countries, namely Mozambique, Togo and Madagascar (UNODA) replied and were reflected in the UN Secretary-General reports. The African states responses, if provided in majority, may serve African diplomats to show the challenges of Africa with regard to cyber security, highlight the inequalities in cyberspace between developed and developing states and also to advocate for the same states' rights in the digital environment.

1.2.2. The European Union &Council of Europe (CoE)

The Council of Europe (CoE) convention on cybercrime, known as Budapest convention, entered into force in 2001. As of August 2017, and according to the CoE website, this convention is ratified by 61 states across the world, including non-CoE members. Budapest convention is considered by western countries and their allies as the only binding international instrument for cooperation between states to fight against cybercrime.

Many countries worldwide were inspired by Budapest provisions in drafting their domestic cybercrime legislations. Moreover, the CoE in cooperation with the European Union developed a number of projects that aim to promote a large ratification and implementation of the Budapest convention by states parties across the world, including the Global Action on Cybercrime Extended (GLACY+), Cybercrime@Octopus and a

joint project of the Council of Europe and the European Union for the Middle East and North Africa region (MENA) region called Cybersouth (CoE, 2019a; 2019b; 2019c; 2019d). Furthermore, EU considers cyber capacity as part of its foreign and development policy and provide assistance to all states across the world aiming at closing the cybersecurity gap between developing and developed states.

In this regard, many African countries and regional organizations benefited from these programmes to build up their law enforcement and cybercrime capacities namely: Mauritius, Ghana, Nigeria, Senegal, Morocco, Burkina Faso, Uganda, Gambia, Tunisia and Cape Verde, in addition to the Regional Economic Community for West Africa (ECOWAS) (CoE, ECOWAS, 2017). Among the aforementioned African countries, four countries have already ratified the Budapest Convention (Mauritius, Senegal, Morocco and Cape Verde).

While the adoption of the African Union Convention on Cybersecurity and Personal Data Protection by the AU summit in 2014 shows the political commitment of African leaders to secure their cyberspace. The pace of ratification is very slow with only four countries ratified (Senegal, Mauritius, Namibia and Guinea), this is due to lack of assistance and support from the African Union to Member States, the lengthy processes within the countries, lack of awareness of decision makers and parliaments on the importance of cybersecurity and its relation to national security and prosperity. While, on the other hand five countries benefitted from CoE support and ratified the Budapest Convention (Ghana,

Senegal, Mauritius, Cape Verde and Morocco) which shows the willingness of African countries to strengthening their legislations and criminal justice capacities and also their engagement for international cooperation to fight cybercrime, as stated by René Bagoro, Minister of Justice of Burkina Faso in his speech in 2018: "it must be recognized at once that these texts have proved insufficient to repress the abuses and other violations of the fundamental rights of which cyberspace constitutes the field of action" (CoE, 2019e).

To address the growing cyber security challenges, African countries may favour bilateral cyber partnerships to build their cyber capacities. As indicated by experts (Segal and Waxman, 2011) in a blog, in the absence of International cyber treaty, powerful states may rely on technical partnerships and joint policy statements for shaping international cyber policy where the lack of cybersecurity expertise of less developed countries may encourage these governments to turn to whoever can provide it, and this can influence their positions on international cybersecurity politics.

1.2.3. The International Telecommunication Union (ITU)

For Africa, the organization, in 2005 in Tunis, of the World Summit on Information Society (WSIS) played an important role in raising awareness of African policy makers and experts on Internet Governance and cybersecurity issues. The same Summit gave the International Telecommunication Union (ITU) a mandate to follow up on the line C5 of the Tunis Agenda on matters related to building confidence and security in the use of ICTs (ITU, 2005). In this regard, the ITU created the High Level Expert Group on Cybersecurity and launched the Global Cybersecurity Agenda (GCA) in 2007, as a

framework for international cooperation where all stakeholders can coordinate an international response to the growing cybersecurity challenges (Touré, 2011).

However, despite the great progress made by the ITU on cybersecurity, the latter could not get an official recognition in its role in shaping the global Internet and cybersecurity policy. The attempt to amend the International Telecommunication Regulations (ITR) during the World Conference on International Telecommunication (WCIT) in 2012 did not reach consensus among ITU members, due to the divergent views on the Internet governance model, notably the role of governments and inter-governmental organizations in Internet policy and Internet development (ITU, 2012).

Yet, ITU remains the most active organization dealing with cybersecurity at international level (Kurbalija, 2016), it has developed several security frameworks and standards, in addition to conducting a range of activities related to cybersecurity awareness, cyber capacity development and deploying cybersecurity solutions and policies.

It is worth noting that ITU has given significant support in many African countries to build appropriate technical and operational cybersecurity frameworks.

1.2.3.1. *Programme Computer Incident Response Teams (CIRT)*

Thanks to the ITU programme on Computer Incident Response Teams (CIRT) that encourages the creation of national computer incident response teams to identify and manage cyber threats and vulnerabilities, 28 African countries have benefited from the

assessment to define their readiness to implement national CIRT, seven (07) African countries established their National CIRT namely: Burkina Faso, Côte d'Ivoire, Ghana, Kenya, Tanzania, Uganda, and Zambia , while the implementation is in progress to set up national CIRT in Burundi, Zimbabwe and Gambia.

1.2.3.2. Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)

The project HIPSSA was initiated by ITU and the European Union to provide technical assistance for harmonizing ICT policies and legislations in sub-Saharan Africa. The project rapidly became an important building block in developing Pan-African harmonized policies and frameworks in the region, including on cybersecurity matters. Within the project a number of legislative frameworks and model laws have been developed by Africa sub regions (ITU, 2008b).

1.3. Informal cybersecurity initiatives

1.3.1. Global Conference on Cyber Space (GCCS)

The GCCS is a relevant and contemporary event that has established since 2011 an informal, inclusive and multi stakeholder international dialogues on cyber policy and principals. The first Conference took place in London in 2011- defined as the London process- and initiated a broad dialogue on the opportunities and challenges in cyberspace , among its outcomes the development of a set of rules to govern the behavior in Cyberspace (Government of the UK, 2011).

The second GCCS was held in Budapest in 2012 and focused on identifying the relationship between Internet freedom and Internet Security. The Seoul GCCS of 2013 outlined the commitment of international community for an open and secured cyberspace (Access Now, 2017).

The 2015 GCCS was hosted by the government of Netherlands and was marked by the Chair's Statement (2015), announcing the creation of the Global Forum on Cybersecurity Expertise (GFCE).

The fifth edition of GCCS conference was hosted by India. It came up with Delhi Communique (2017) for GFCE members. Among its recommendations, it highlighted the need to identify gaps related to knowledge, technology and expertise between nations and called for more international cooperation to narrow these gaps and build cyber capacities of both governments and individuals for an inclusive cyberspace.

While the GCCS represents a multi stakeholder platform for discussions with real opportunities for International exposure and cooperation, Africa participation in the GCCs is limited to few countries such as Senegal, Kenya, Morroco and Tunisia which are members of the GFCE which generally nominate delegates from the ministry of ICT to attend the conferences without internal coordination with other Ministries.

1.3.2. The Global Forum on Cyber Expertise (GFCE)

The Global Forum on Cyber Expertise (GFCE) is a key initiative for fostering solidarity in cyberspace, the forum aims at providing political, technical and financial support to strengthen international cooperation among all stakeholders in the global cyber domain (GFCE, no date).

The GFCE is a global coordinating platform for cyber capacity building for states and international organizations, as well as private companies to exchange best practices, knowledge and expertise on cyber policies and capacity building experiences (GFCE, date).

Africa participation remains modest and limited to some governments (Ivory Coast, Kenya, Mauritius, Morocco, Nigeria, Rwanda, Senegal, Tanzania and Tunisia) and some intergovernmental organisations such as the African Union Commission and the Regional Economic Community for West Africa (ECOWAS) without representation of the private sector and civil Society, to support the creation of multi stakeholder cyber security mechanisms in Africa.

1.3.3. Global Forum on Internet Governance, AfIGF, Regional IGFs

The global Internet Governance Forum (IGF) was created as per the Tunis Agenda recommendations (ITU, 2005). According to Maurer (2011), the establishment of the IGF is considered as a compromise between the supporters of UN institutions in governing

the global internet, from one side, and the US allies, in the other side, which are reluctant to this kind of approach.

Even though the IGF outcomes are not legally binding, the previous IGFs helped in maintaining open and inclusive debates on Internet governance, Internet policy and cybersecurity, with participation of representatives of governments, Civil society, technical community, private sector and all interested parties in IG issues. The IGF 2017 held in Geneva in the premises of the UN was marked by several sessions dedicated to cyber issues. Whereas, the IGF 2018 held in France came up with "Paris call for trust and security in cyberspace", the declaration reinforces the recommendations of previous UNGGE Report's notably the applicability of international laws in cyberspace and the need for cyber norms to regulate cyberspace. It is worth noting the strong support for Paris Call from several governments and tech companies. While the USA, Russia and China did not sign the declaration it is reported that four African countries namely Gabon, Morocco, Congo and Senegal have signed the declaration (Radunovic, 2018)

The Internet Governance space in Africa has been very active during the WSIS process, with regional meetings held from 2002 to 2005 in Bamako, Accra, Addis Ababa, Cairo, Johannesburg, Douala and Tunis. Moreover, within the IGF global initiative, Africa has hosted IGF two times in Egypt (2009) and in Kenya (2011).

Even though, Africa Internet community expressed a strong need for the creation of the African Internet Governance Forum (AfIGF) since 2006 and launched the first AfIGF five years later in Kenya, it was officially recognized by ICT Ministers as a necessary continental platform to facilitate multi-stakeholder discussions on issues related to Internet development in Africa with particular focus on Internet Governance issues.

The Secretariat of the AfIGF is hosted by the AUC in its Headquarters, in Ethiopia (AfIGF website). The AfIGF is organised every year and ensures that Africa concerns are taken into account in the global IGF process. Furthermore, the AfIGF is supported by sub regional IGFs in all the five regions of Africa that manage to bring together the existing national IGFs at the level of the region, to promote local policy dialogues on Internet Governance and other emerging digital policy issues, including cybersecurity . As per the UN Internet Governance Website there are 23 African countries that established their national IGF **(Benin, Cameroon, Chad, Democratic Republic of the Congo, Gambia, Ghana, Kenya, Malawi, Mauritius, Mozambique, Namibia, Nigeria, Rwanda, Senegal, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zimbabwe).** If we compare with other regions such as Latin American and Caribbean that counts 19 national IGFs and Asia pacific with only ten IGFs (10) we can consider establishing IGFs in Africa as a successful model, especially in recent years with the increasing participation and involvement of government representatives.

The Internet Governance debate in Africa has made a slow and steady progress since 2012. However, despite the annual organisation of the AfIGF, African regional IGFs and National IGFs in the aforementioned countries, Africa participation in the Global IGF remains modest and most of the time limited to individual experts and representatives of Africa civil society movements.

1.4. Conclusion

Cybersecurity became of strategic importance for governments, as well as for regional and international organisations. Therefore, discussions and negotiations on the political, economic, social and military implication of the use of ICTs by states and non-state actors are underway at different levels, both in formal and informal ways.

In the absence of global consensus on the way to regulate cyberspace, many states and regions have defined their international cybersecurity policy according to their strategic priorities and political agenda. Whereas the United States and the European Union members are increasingly engaging in bilateral and regional cyber partnerships and even started exploring how existing international law applies to cyberspace through simulating legal, technical, strategic and operational cyber scenarios with the aim to prepare for sever cyber-attacks as per Tallinn Manual guiding principles. Others, such as Russia, China and other states emphasize a central role of the United Nations in formulating global cybersecurity norms and advocate for an international agreement to consolidate cyber peace. For instance, six members of the Shanghai Cooperation Organization (SCO) leaded by Russia and China submitted, in 2015 an official letter to the UN's Secretary-

General seeking the identification of rights and responsibilities of states in the information space.

While multilateral cyber policy debates are dominated by the powerful states that advanced concepts aiming at shaping, regulating and securing the digital space, such as the norms of responsible behavior in cyberspace and confidence building measures to mitigate cyber conflicts. African countries are yet to develop a common understanding on cybersecurity matters and Africa participation in these debates is not coordinated across African states and/or stakeholders and remains limited to some states represented by governmental experts at the GGEs and by the technical community and civil society in the global IGF.

Chapter 2

Is Cyber Security on the high Agenda of African Countries - Why should it be?

2.1. Cyber Security is not high on the agenda of African States.

Internet penetration in Africa is growing faster than other regions. According to Internet World Stats Website, the percentage of connected people reached 36.1 %, in June 2018, and GSMA report (2017) revealed that Africa expects a penetration rate of 60% on mobile broadband connections, by 2020, which accounts for more than 90% of Internet subscriptions, as Internet users rely more on Mobile Broadband access.

Though, the ITU report on Measuring the Information Society for 2018 (ITU, 2018c) shows that Africa still lags behind the other regions, as it records the lowest average values far from the global average, it has been noticed that almost all countries have experienced growth in Internet penetration and a significant expansion in the use of ICTs, as source of economic and social growth.

This progress is also reflected in the 2018 Broadband Commission report with 45 African countries among 55 having adopted their National Broadband or ICT Policy, while a number of countries have even undertaken a review of their policies and refocused their strategies towards the development of digital services to enable the modernization of strategic sectors, such as education, health, agriculture and the delivery of government services to populations (ITU, 2018b).

However, more African countries are increasing access to and using ICTs, they become more connected to the global network which expose them to the very sophisticated and large scale associated cyber-attacks.

Considering the strategic importance of ICTs & Internet for modern economies and societies as well as the multidisciplinary and borderless nature of cyberspace, it becomes critical for African countries to effectively adapt to the new realities of the digital environment. For Africa, developing an inclusive and sustainable African digital economy and smart society will depend on building trust and confidence in the use of cyber technologies.

2.2. Africa Cybersecurity landscape

With the rapid adoption of digital technologies and the shift of vital activities to the virtual world, it becomes challenging to secure, protect and defend cyber operations carried out at societal, economic and individual levels.

For Africa, in general, the lack of cybersecurity culture and awareness among Internet users and policy makers on the risks related to the extensive use of digital technologies to perform either private, personal and professional applications have significantly raised the level of vulnerability and exposure of African states and individuals to cyber threats.

Moreover, in the absence of detailed and reliable information regarding cybercrime and cyber-threats affecting African countries, it is difficult to evaluate the origin and

implications of cyber-attacks targeting individuals, business and governmental institutions.

2.2.1. At continental level

In Africa, discussions on the security of ICT networks and electronic communications began in 2009 when the Ministers in charge of communication and information technologies of Member States of the African Union adopted a declaration [EXT/CITMC/MIN/Decl. (I)] (known as the Olivier Tambo Declaration) in which they requested the African Union Commission to develop jointly with the United Nations Economic Commission for Africa, a convention on cyber legislations to address the legal and regulatory requirements on electronic transactions, cyber security and personal data protection (Amazouz, 2018).

The same declaration was endorsed by the 14th AU Summit of Heads of States and Governments in 2010 [Assembly/AU/11(XIV)] where African Leaders also recognized ICT as a sector of top priority in Africa development programs and called all countries to consider ICT infrastructure and services, as a basic public utility infrastructure.

The third ordinary conference of Ministers in charge of ICT and communication of the African Union held in Abuja, in 2010, in their declaration [AU/CITMC/MIN/Decl.(III)] the ICT Ministers reiterated the call for developing a convention on cybersecurity that responds to Africa needs and support its implementation in the African Union Member States by 2012.

The African Union Commission led the process of developing the convention by facilitating consultations and discussions among all concerned stakeholders. The first draft of the convention was available and open for input in 2011, then it was submitted for adoption by the Ministers of ICT and Communication as well as Ministers in charge of Justice and Legal Affairs in their respective conferences.

The convention was finally adopted by Heads of States and Governments during the 23rd Assembly held in Malabo, Equatorial Guinea in June 2014. The African Union Convention on Cyber security and Personal Data Protection, also known as “the Malabo Convention" aims to set up essential rules for establishing a modern information society and secure digital environment (cyber space) in Africa by addressing the need for harmonized cyber legislations to facilitate cooperation in the Member States of the African Union.

This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the AU Commission of the fifteenth (15th) instrument of ratification. However, as of February 2019, only four (04) countries have ratified the Convention (Senegal, Guinea, Namibia and Mauritius), while eleven (11) have expressed their willingness to ratify by signing the Convention (Benin, Chad, Comoros, Congo, Ghana, Guinée Bissau, Mauritania, Mozambique, Sierra Leone, Sao Tome & Principe and Zambia) (AUC, no date). The ratification pace remains slow due to the low level of

awareness at the executive level on the need for a continental instrument to address the transnational organised crime carried out through ICT networks.

In an effort to support African countries in the implementation of the Malabo convention, and in partnership with Internet Society (ISOC), the AU Commission developed Guidelines on Internet Infrastructure Security (ISOC, 2017) and Guidelines on Personnel Data Protection in Africa (ISOC, 2018) where explanations and guidance on domestication of the Malabo Convention provisions are given.

Moreover, as per Malabo convention provisions and as indicated in the Addis Ababa declaration of 2017 [AU/CCICT-2/MIN/Decl. (2) Rev], the Ministers of ICT and Communication agreed that AU vision, with regard to cybersecurity of African countries, is having each country to adopt its national cybersecurity strategy, each country to establish a national Computer Emergency Response Team (CERT) and each African country to enact the necessary cyber laws. In addition to establishing regional and continental mechanisms and frameworks to facilitate cooperation among African states and sub regions.

During the Assembly of Heads of States and Governments held in Addis Ababa, Ethiopia, in January 2018, the African leaders adopted a declaration on Internet Governance and Development of Africa's Digital Economy that identifies some guiding principles for

regulating Africa cyber space, in addition to elevating cybersecurity to the top priorities of the African Union agenda (AUC, 2019).

In an effort to raise awareness and support Member States in developing their cyber capacities, the AU Commission in collaboration with partners, organized several capacity building workshops and meetings aiming at assisting African countries to develop their national cybersecurity frameworks (AUC, 2018b).

2.2.2. At regional level

The Regional Economic Communities (RECS) are part of the African Union and have the regional mandate of developing Cyber security policies, as well as coordinating cyber initiatives, within the five Sub Regions of the African Union, to ensure safe cyberspace for their Member States. In addition to undertaking cyber capacity building activities, so far a number of programs and legislative frameworks have been adopted by the Sub Regions notably: ECOWAS cybersecurity guidelines, ECCAS Model Law / CEMAC Directives on Cybersecurity (Data protection, e-transactions, cybercrime); SADC model law on data protection; SADC model law on e-transactions; SADC Model Law on Computer Crime and Cybercrime and Common Market for Eastern and Southern Africa (COMESA); model Law on electronic transactions and Model Cybercrime Bill adopted in 2011 (Orji, 2015).

2.2.3. At national level:

The increasing reliance on digital technologies in Africa and the growing number of reported cyber-incidents demand from governments to come up with strategic responses to counter cyber-threats and prevent any misuse of ICTs within the region. In fact, understanding and adequately managing national cyber risks require a coordinated national approach as well as the establishment of an appropriate organizational structure for securing digital infrastructure and services upon which a country's digital economy depends, represent the new challenge facing all African states.

In today digital world, cybersecurity is increasingly considered as horizontal and a strategic national issue, a high level and top down approach, affecting all levels of society, where a national cybersecurity strategy establishes national objectives and priorities to ensure the resilience of national critical infrastructures and services (ENISA, 2012).

In Africa, the majority of countries are at early stage of developing national cybersecurity frameworks. There are only few countries within the Continent that reached an acceptable level of cyber maturity and adopted their national policy & strategy and countermeasures to tackle online criminality (Symantec, 2016).

2.2.3.1. Cybersecurity policy and governance frameworks

African countries are at different levels of developing policy instruments and legislative frameworks to fight against cybersecurity threats. So far, only thirteen (13) countries have published their national cybersecurity strategy in Africa namely: Kenya, Rwanda, Egypt,

Nigeria, Mauritius, Ghana, Senegal, Mauritania, Tunisia, South Africa, Uganda, Cape Verde and Morocco.

2.2.3.1.1. South Africa

To ensure the security of South Africa's cyberspace and effectively combat emerging threats, The State Security Agency has published, in 2015, the National Cybersecurity Policy Framework (NCPF) that was approved by the cabinet since 2012 (Government of South Africa, 2015b).

This Framework outlines broad policy guidelines and strategic priorities on cybersecurity for the nation, notably promoting a culture of cybersecurity, building cyber capacities and promoting international cooperation in cyberspace. The NCPF aims to foster cooperation and coordination between government, private sector and civil society, by stimulating a strong interplay between policies, legislations and technical aspects (Vuuren *et al.*, 2013).

In South Africa, cybersecurity initiatives are led by the Cyber Response Committee (CRC) which, under the oversight and supervision of the State Security Agency, it involves key departments, including the department of telecommunications and postal services, the department of justice , the department of science and technology, as well as the department of international relations and cooperation who is responsible for the formulation, coordination, and managing of South Africa's foreign policy and international relations specific to cybersecurity (Symantec, 2016).

South Africa is among the rare African countries that officially recognized investing in developing cyber capabilities to secure South Africa against external cyber-attacks. The Ministry of Defense has already announced the development of Cyber Warfare Strategy and the establishment of a Cyber Command Centre Headquarters in 2018/19 (Government of South Africa, 2015a).

Furthermore, in 2015, the Department (Ministry) of Telecommunication and Postal Services (DTPS) officially established The South Africa National Computer Security Incident Response Team (CSIRT), known as the National Cybersecurity Hub, that has for objective to serve as a national point of contact for coordinating cybersecurity incidents between all cyber actors (South African National Cybersecurity Hub, 2015).

As stated by the South Africa parliament report (Government of South Africa, 2017), National Cybersecurity Hub is a platform that receives and analyses all cybersecurity incidents, trends and vulnerabilities, as well as facilitating the establishment of sector, regional and continental CSIRT's, to effectively contribute in dissemination of alerts and early warnings on major cyber incidents, in addition to initiating national Cybersecurity awareness campaigns.

2.2.3.1.2. Kenya

In Kenya, the Information Communication Telecommunication plays a significant role in the development of national economy. The rapid uptake and transformative power of ICT

has contributed to considering it as a priority sector by the government. According to Kenya Economic Survey, the ICT sector in Kenya was worth Sh138 billion (1.37 Billion USD) in 2014 (Ogutu, 2015).

To secure the online environment, the country has adopted a National Cyber Security Master Plan and Strategy in 2014 which demonstrates the commitment of the government to ensure security in the digital space. The National Cyber Security Strategy is in line with Kenya's Vision 2030 national priorities, addresses the emerging risks and challenges that may affect the cyber domain and defines the nation cybersecurity goals, namely: enhancing the nation's cybersecurity posture by increasing security and resilience of critical Information infrastructures, as well as digital applications and services; raising awareness and developing Kenya's cybersecurity workforce; cultivating a culture of information sharing and collaboration cross-sector and cross organizations, as well as promoting a balance between information security, online privacy and Kenya's economic priorities (Government of Kenya, 2014).

In Kenya, there is a strong political commitment towards cyber security; it is handled by the National Security Advisory Council (NSAC) that reports directly to the National Security Council (NSC) which is chaired by the President of the Republic of Kenya. The NSAC is seconded by the National Cyber Security Committee (NCSC) which provides policy advice on cybersecurity issues and facilitates national responses to cyber incidents,

through the operation of the National Kenya Computer Incident Response Team, known as Coordination Centre (KE-CIRT/CC) (Privacy International, 2017).

2.2.3.1.3. Egypt

The institution which oversights on cyber security issues in Egypt is the Supreme Council for Cybersecurity (ESCC), established in 2015. The ESCC is chaired by the ministry of Communication and Information Technology and reports to the Cabinet of Ministers. The ESCC is mandated to further develop a national comprehensive strategy to ensure a safe and secure environment that would enable various sectors to deliver integrated e-services (Government of Egypt, no date).

A national cyber security strategy was adopted in 2018 with a detailed five years' action plan (2017-2021).The strategy emphasizes on the distribution of roles among government agencies, private sector, business institutions and civil society, as well as the measures to be established by the State to tackle significant cyber threats, such as cyber-attacks targeting ICT infrastructure and information systems and databases, cyber terrorism and cyberwarfare, as well as the theft and misuse of digital identity and personnel data (Government of Egypt, no date).

The strategic pillars are related to executive political and institutional support, legislative framework, regulatory and executive framework, cybersecurity industry development, cybersecurity taskforce, awareness raising on cybersecurity matters, as well as

cooperating with friendly countries and relevant international and regional organizations (Government of Egypt, no date).

2.2.3.1.4. Ghana

Ghana's intention of becoming an information hub of West Africa has led the government to enhance its cybersecurity practices and enact cyber laws (Lewis, 2013).

A National Cybersecurity Policy and Strategy (NCSPS) was approved by Cabinet in 2016. Its objective is to secure the Critical National Information infrastructure (CNII) of critical sectors. The strategy is made of nine (9) pillars: effective governance, legislative and regulatory framework, research and development towards self-reliance in protecting Ghana cyber domain, cyber security emergency readiness, cyber security technology framework, culture of security and capacity building, child online protection, compliance and enforcement, as well as international cooperation (CERT-GH, 2016).

The strategy highlights Government role in centralizing the coordination of national cyber security initiatives and promoting effective cooperation at national level. The strategy also outlines the need for the government to put in place policy measures that encourage active participation of Ghana in relevant international cyber security meetings and ensure an international cyber engagement, through compliance with international/regional treaties (Government of Ghana, 2017).

The national cybersecurity governance in Ghana relies on solid governance structure and institutions that embody a National Cybersecurity Inter-Ministerial Advisory Council (NCSIAC), a National Cyber Security Center (NCSC) and a National Cyber Security Technical Working Group (NCSTWG) (Yankson, 2018).

2.2.3.1.5. Rwanda.

The government of Rwanda is among the African countries that have invested in developing ICT infrastructures and applications. In addition to the adoption of national ICT policy, the government approved in 2017 the ICT Sector Strategic Plan (2018-2024) that focus on developing digital enabled economy (Government of Rwanda, 2017a).

To overcome the potential impact of cyber-attacks on national security and economy, the government adopted the national cybersecurity policy, as well as the national cybersecurity strategic plan in 2015, under the leadership of the ministry of ICT (Government of Rwanda, 2015a).

The scope of cyber security policy in Rwanda is to ensure that cyberspace is secure and resilient. Its strategic objectives are: increase the level of cyber security awareness in all sectors and protect key ICT and information assets against Cyber-attack; build local capabilities to respond to cyber-attacks; create legal and regulatory environment to mitigate cyber vulnerabilities, establish an institutional framework to enable good governance and cross sector coordination of cybersecurity initiatives, as well as promote international cooperation on cyber security (Government of Rwanda, 2015a).

As indicated in the National Cybersecurity Strategic Plan, the governance of cybersecurity and information security in Rwanda is led by the National Cyber Security Advisory Board (NCSAB) which has an advisory role. It works with national security organs and reports to the Office of the President. The NCSAB is supported by the National Cybersecurity Agency that have a coordinating responsibility between public and private sector for an effective implementation of the National Cybersecurity policy and strategy (Government of Rwanda, 2015b).

2.2.3.1.6. Mauritius

Mauritius vision with regards to cybersecurity is enhancing the capacity of the country to counter cyber threats and manage disturbance that may be caused by cyberattcks. The national cybersecurity strategy (2014-2017) highlights the government approach and strategy to protect the national information systems and networks whose strategic objectives are : secure Mauritius cyberspace and defend against cybercrime; enhance resilience to cyberattcks; establish a coordination and collaborative model between government institutions and business community to effectively ensure cyber security and cyber defense, as well as enhancing awareness and national expertise to mitigate cyber risks. In Mauritius the National Cybersecurity Committee (NCSC), as a decision-making body that reports to the ministry of ICT, has oversight over cybersecurity related issues within the country (Government of Mauritius, 2014).

2.2.3.1.7. Senegal

After adopting the Digital Senegal Strategy 2025, where digital confidence is among its three pillars, the government adopted a National Cybersecurity strategy (SNC2022) in 2017 which outlines some key elements, such as an assessment of current and future cybersecurity threats and vulnerabilities in Senegal, as well as identifying roles and responsibilities.

The strategic objectives of SNC are: strengthening legal and institutional framework, protection of CII and information systems, promotion of cybersecurity culture, development of cyber skills and having Senegal involved in regional and international work on Cybersecurity (Government of Senegal, 2017).

2.2.3.1.8. Nigeria

Nigeria National Cybersecurity Strategy (NCSS) addresses the nation's cyber risks exposure and readiness to provide strategic responses towards assuring security and protection of Nigeria in the global cyberspace, safeguarding critical information infrastructure (CII), building and nurturing trust within Nigeria cyber-community.

The NCSS set mitigation strategies to tackle cyber threats, such as Cybercrime, cyber-terrorism, cyber conflict, cyber espionage and Child online abuse, through proposing strategies on incident response, legal framework reforms, CII protection, cyber capacities development, Child online security and Public-Private partnership. The NCSS addresses also the impact of cyber threats on national security and economy, as it is considered as part of the national security strategy (NgCERT, 2014).

2.2.3.1.9. Morocco

In an effort to strengthen the Moroccan national capacity to secure information systems of administrations, public bodies and operators responsible for the management of critical infrastructure, the government created the Strategic Committee for the Security of Information Systems (CSSSI) and the General Directorate of Information Systems Security (DGSSI) that report to the National Defense Administration. The government adopted in 2012 the National Cyber Security Strategy that aims to evaluate the cyber risks affecting networks and Information systems of government institutions and critical infrastructures, protecting and defending the information systems, as well as strengthening the foundations of security, notably: Legal framework, Awareness raising, Training and Research & Development, in addition to promoting national and international cooperation (Government of Morocco, 2012).

2.2.3.1.10. Tunisia

Tunisia vision on cybersecurity is to protect public and private property against cyber threats and ensure trust in the use of information technology. The National Cyber Security Strategy Guidelines emphasize on the security of national information systems, building local cyber security expertise, developing legal and regulatory frameworks, as well as raising awareness on cyber risks and educating citizens (Loghmari, 2016).

The oversight of cybersecurity in Tunisia is led by the National Agency for Computer Security (NACS) since 2005. The agency carries out a general control of the information

systems and the networks belonging to the various public and private organizations (Government of Tunisia, 2002).

2.2.3.1.11. Uganda

The government considers information security as an enabler for the delivery of public services, part of national security goals, as well as a critical asset to the operation of important national sectors. In this regard, a National Information Security Framework (NISF) was adopted in 2014 to impose a minimum set of security measures to all public and private organisations.

As indicated in the NISF, the security of national cyber space can be seen under 4 headings, namely security governance, information security, personal security and physical security (Government of Uganda, 2014).

The Republic of Uganda performed a Cybersecurity Capacity Review, with support from Commonwealth Telecommunications Organisation (CTO) and Global Cyber Security Capacity Centre in 2016 (Government of Uganda, 2016).

2.2.3.1.12. Mauritania

The National Strategy on Cybersecurity (2017-2022) of Mauritania highlights the country vision with regards to digital trust as an enabler for the development of national digital economy. The pillars of the strategy are: protection of national information systems and government systems, protection of critical infrastructure, development of cyber security

and promotion of awareness, development of the legal and regulatory frameworks, encouraging public-private partnership and international cooperation (Government of Mauritania, 2018).

2.2.3.1.13. Cape Verde

Cape Verde adopted a four-year action plan on cybersecurity as the National Strategy in 2016. The strategy identifies priorities and objectives to be achieved by 2020, notably the development of cyber legislations and mechanisms to facilitate and coordinate adequate responses to cyber-attacks (Government of Cabo Verde, 2016).

The government aims at establishing a National Center on Cybersecurity to support the implementation of the National Strategy on Cybersecurity as well as a Commission on cybercrime composed of stakeholders from different sectors responsible for the development of a strategic plan for the implementation of the National Strategy on Cybersecurity by 2020 (UNIDIR, no date).

2.2.3.1.14. In summary

Although the number of African States that adopted cybersecurity policies and strategies remain low (24%), there are several countries which are developing their national strategies and are far in the process. Among the existing strategies, there are some similarities, such as defining the governance framework, outlining engagement in international cooperation and setting the strategic priorities like fighting criminal use of ICTs, protection of critical infrastructures and protecting national economy.

On the governance aspect, for most African countries, the Ministry of ICT has a central role in developing the strategy and coordinating cyber operations internally. Nevertheless, in some countries, such as Kenya, Egypt, Rwanda and Ghana, the cybersecurity governance is either under the Presidency or the Cabinet of Ministers which demonstrates strong commitment to cyber security.

Table 1

Country	**Name / Reference of the National Cyber Security strategy /policy**
Cabo Verde	National Strategy on Cybersecurity "a Estratégia Nacional para a Cibersegurança", approved on 11 February 2016
Egypt	National Cyber Security Strategy 2017-2021
Ghana	Ghana National Cybersecurity Policy &Strategy (NCSPS), approved 2016
Kenya	National Cyber Security Master Plan and Strategy in 2014
Mauritania	National Strategy on Cybersecurity (2017-2022) approved in 2018
Mauritius	National Cyber Security Strategy 2014 – 2019
Morroco	National Cybersecurity Strategy, approved in 2012
Nigeria	National Cybersecurity Strategy Adopted in 2014
Rwanda	National Cybersecurity Policy and Strategy (2014 – 2019). Approved 2015
Senegal	National Cybersecurity Strategy of Senegal (SNC2022) approved 2017
South Africa	National Cybersecurity Policy Framework (NCPF), approved 2012
Tunisia	National Cyber Security Strategy Guidelines approved in 2002

Uganda	National Information Security Framework (NISF) approved in 2014

Existing National Cyber strategies in Africa

2.2.3.2. National Computer Emergency/ Incident Response Team (CERT/CIRT)

A National CERT/CIRT is an important platform to effectively identify risks and vulnerabilities, prevent and respond to cyber-attacks, assist criminal justice with investigations and disseminate information to public.

In many countries, the national CERT manages cybersecurity threats and cyber-attacks and acts as a focal point to facilitate the coordination, both at national and international levels.

As of February 2019, and according to ITU website, nineteen (19) African countries have established their National CERT/ CIRT, notably: Algeria, Kenya, Rwanda, Cameroon, Sudan, Mauritius, Ghana, Burkina Faso, Tunisia, Cote D'Ivoire, South Africa, Zambia, Egypt, Libya, Tanzania, Ethiopia, Uganda, Morocco, Zimbabwe.

As a continental initiative, AfricaCERT is an association of African Computer Security Incident Response Teams. It provides a platform for collaboration and coordination among African CERTs from government, commercial, and educational organizations and it aims to foster cooperation and promote information sharing among members, as well as providing trainings and technical support. At present, eleven (11) countries are

members of AfricaCERT, namely: Burkina Faso, Cameroon, Cote d'Ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, South Africa, Sudan and Tunisia (AfricaCERT, no date).

It is worth noting that many African countries cooperate at a technical level to mitigate cyber risks, through their national CERTs. Currently, thirteen (13) countries (Cote D'Ivoire, Mauritius, Egypt, Ethiopia, Kenya, Morocco, Nigeria, South Africa, Sudan, Tanzania, Tunisia, Uganda, and Zambia) are members of the Global Forum of Incident Response and Security Teams (FIRST) and Seven (7) countries (Cote D'Ivoire, Egypt, Libya, Sudan, Morocco, Nigeria, Tunisia) are members of Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT). While several African experts participate regularly in the FIRST-ITU Regional Symposium & Cyber Drill for Africa and Arab Region, Africa hosted the event in 2016 and 2017 (EG CERT, 2017).

Table 2

Country	**Name and/or reference of the National Computer Emergency Response Team (CERT)**
Algeria	Algerian Computer Emergency Response Team (DZ-CERT) was created in 2015 and it is hosted by Research Centre for Scientific and Technical Information [CERIST]. (DZ-CERT, 2015)
Angola	A CIRT readiness assessment was conducted for Angola by the ITU in 2014 (ITU, 2019)
Benin	No CERT in place
Botswana	Botswana Computer Incidence Response Team (bw CIRT)

	Is being established by the government as per the National Cybersecurity Strategy recommendation. After the readiness assessment in 2014, the ITU is supporting Botswana to establish National CIRT. (bw CIRT, 2014)
Burkina Faso	Computer Incident Response Team Burkina Faso (CIRT-bf) was established in 2012 with support from ITU /IMPACT and it is hosted by the Regulatory Authority for Electronic Communications and Posts (ARCEP). (CIRT-bf, 2012). CIRT-bf is member of AfricaCERT
Burundi	National CIRT is being developed with support of ITU after the readiness assessment made in 2013. (ITU, 2019)
Cameroon	Computer Incident Response Team [cmCIRT] established in 2012 (cmCIRT, 2012) Member of AfricaCERT
Cabo Verde	CERT establishment in progress
Centre Africa Republic (CAR)	A CIRT readiness assessment was conducted for CAR by the ITU (ITU, 2019)
Chad	A CIRT readiness assessment was conducted for chad by the ITU (ITU, 2019)
Comoros	No CERT in place
Congo	A CIRT readiness assessment was conducted for Republic of Congo by the ITU (ITU, 2019)
Cote 'Ivoire	Cote d'Ivoire Computer Emergency Response Team (CI CERT) is the national CSIRT of the government of Cote D'Ivoire and was established in 2009 (CI CERT, 2009) Member of FIRST since 2016 Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Member of AfricaCERT
DRC	A CIRT readiness assessment was conducted in 2014 for DRC by the ITU. (ITU, 2019)
Djibouti	No CERT in place

Egypt	Egyptian National Computer Emergency Response Team (EG-CERT), hosted by National Telecom Regulatory Authority (NTRA) and established in 2009. (EG-CERT, 2009). Member of FIRST since 2012 Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Member of AfricaCERT
Equatorial Guinea	No CERT in place
Eritrea	No CERT in place
Ethiopia	Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CERT) hosted by Information Network Security Agency (INSA) and was created in 2012. (Ethio-CERT, 2012) Member of FIRST since June 2016
Gabon	A CIRT readiness assessment was conducted for Gabon by the ITU (ITU, 2019), A national CIRT is being developed
The Gambia	National CIRT is being established with support from ITU. (ITU, 2019)
Ghana	Ghana Computer Emergency Response Team (ghCERT). (ghCERT, 2014) Member of AfricaCERT
Guinea	No CERT in place
Guinea Bissau	No CERT in place
Kenya	National Kenya Computer Incident Response Team / Coordination Centre (National KE-CIRT/CC) Established in 2012 and hosted by the Communications Authority of Kenya (CA) as per the Kenya Information and Communications Act, 1998. (KE-CIRT/CC, 2012) KE-CIRT/CC is member of Forum of Incident Response and Security Teams (FIRST) since July 2015 Member of AfricaCERT
Lesotho	A CIRT readiness assessment was conducted in 2014 for Lesotho by the ITU. (ITU, 2019)
Liberia	A CIRT readiness assessment was conducted in 2014 for Liberia by the ITU. (ITU, 2019)

Libya	Libyan Computer Emergency Response Team (LibyaCERT) hosted by National Information Security Agency and Safety (NISSA), it was established in 2013. (LibyaCERT, 2013) Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)
Madagascar	A CIRT readiness assessment is underway (ITU, 2019)
Malawi	Malawi CIRT is being designed (SADC, 2018)
Mali	A CIRT readiness assessment was conducted for Mali by the ITU. (ITU, 2019)
Mauritania	No CERT in place
Mauritius	Mauritian National Computer Security Incident Response Centre (CERT-MU), established in 2008 and hosted by National Computer Board (NCB), Republic of Mauritius (CERT-MU, 2008) CERT-MU is member of FIRST Since 2012 AfricaCERT European TF-CSIRT European Government CERTs (EGC) group APCERT
Morocco	Moroccan National Computer Emergency Response Team (maCERT), established in 2011 and hosted by General Direction of Information System Security under Moroccan National Defense. (maCERT, 2011) Member of FIRST since 2013. Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Member of AfricaCERT
Mozambique	A CIRT readiness assessment was conducted in 2014 for Mozambique by the ITU. (ITU, 2019)
Namibia	A CIRT readiness assessment was conducted in 2014 for Namibia by the ITU. (ITU, 2019)
Niger	

	A CIRT readiness assessment was conducted for Niger by the ITU. (ITU, 2019)
Nigeria	Nigerian Computer Emergency Response Team (ngCERT) is the national CERT, established in February 2015 and it is hosted by the office of National Security Adviser (ONSA) (ngCERT, 2015) Member of First since July 2015 Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)
Rwanda	Rwanda National Computer Security and Incident Response Team (Rw-CSIRT), established in 2014 (Rw-CSIRT, 2014)
Saharawi	No CERT in place
Sao Tome &Principe	No CERT in place
Senegal	A CIRT readiness assessment was conducted for Niger by the ITU. (ITU, 2019)
Seychelles	A CIRT readiness assessment is underway (SADC, 2018)
Sierra Leone	A CIRT readiness assessment was conducted for Sierra Leone by the ITU. (ITU, 2019)
Somalia	No CERT in place
South Africa	South African Computer Security Incident Response Team (ECS-CSIRT), established in 2003 and hosted by State Security Agency. (ECS-CSIRT, 2003) ECS-CSIRT is Member of FIRST since 2009 Member of AfricaCERT Computer Security Incident Response Team First National Bank (CSIRT-FNB) is hosted by Standard Bank of South Africa (CSIRTFNB, 2009) CSIRTFNB is also Member of FIRST.
South Sudan	No CERT in place
Sudan	Sudan Computer Emergency Response Team (CERT Sudan) established and hosted by National Telecommunication Corporation in 2010 (CERT Sudan, 2010). Member of FIRST since April 2017

	Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) Member of AfricaCERT
Swaziland (Eswatini)	A CIRT readiness assessment was conducted for Eswatini in 2014 by the ITU. (SADC, 2018)
Tanzania	Tanzania Computer Emergence Response Team (TZ-CERT) hosted by Tanzania Communications Regulatory Authority TZ-CERT, it was established in 2010 under the law related to Electronic and Postal Act (EPOCA) no 3/2010 / section 124. (TZ-CERT, 2010) TZ-CERT is Member of FIRST since 2015
Togo	In the process
Tunisia	Tunisian Computer Emergency Response Team (tunCert) is the national CERT and hosted National Agency for Computer Security (ANSI) and was established in 2004. (tunCert, 2004) tunCert is Member of FIRST since 2007 Member of the Organisation of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) and Member of AfricaCERT in Tunisia sectorial CERTs are operating (Finance, Social, Health, Military) (Homri, 2018)
Uganda	Uganda Computer Emergency Response Team(ugCERT) Established in 2011. (ugCERT, 2011) Member of FIRST since 2017
Zambia	Zambia Computer Incident Response Team (zmCIRT) was established in 2012 with support from ITU/IMPACT It is hosted by Zambia Information and Communication Technology Authority (ZICTA). (zmCIRT, 2012) zmCIRT is Member of FIRST since August 2017
Zimbabwe	A CIRT readiness assessment was conducted for Zimbabwe in 2014 by the ITU. (ZmCIRT) is being developed with ITU support (SADC, 2018)

CERTs/ CIRTs in Africa

2.2.3.3. Regulatory response to cybersecurity in Africa (Cyber Laws)

Over the last years, governments, business, and citizens have become critically dependent on Internet and Information Communications Technologies (ICTs) Hathaway (2018). Furthermore, globalization and growing interconnection of critical digital infrastructures have introduced new possibilities for conducting malicious activities with large impact and significant scale.

To combat the disruptive or criminal use of ICTs, there is a need for adopting and implementing specific cyber legislations provisions at a national level, through identifying structures, as well as the role and obligations of major players dealing with cybersecurity. To ensure the security and respects of peoples' rights in cyber environment, special laws to fight cybercrime and protect privacy online are mandatory to regulate the national cyberspace.

African governments are at different levels of enacting cyber legislations to accommodate new legal challenges in the digital environment. Even though many countries have proposed draft cyber laws, the majority struggles to pass them in the national parliaments which, in many cases, are characterized by lengthy processes and lack of awareness on the danger associated with cyber technologies.

The current state of cybercrime legislations in Africa show that, among the 55 countries of Africa, only few have the basic legal frameworks in place. As reported by the Council of Europe, only 11 States have adopted substantive and procedural law provisions to combat cybercrime (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia). While 12 other States have partially adopted cybercrime legislations such as: Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe (CoE, 2015).

Many African countries are amending the existing laws to effectively fight against illicit use of ICTs, while some African States have not yet adopted any specific legal provisions to ensure the security and confidentiality of electronic communication and electronic transaction data .

2.2.3.3.1. Online Privacy& Personal Data Protection laws

Every day a big amount of data is collected, stored and used every day across the globe. The volume of cross-border data flows, more specifically personal data and the daily reported violation of online privacy and data breaches, have made data protection regulations a central component of the security of people in cyberspace.

For African countries, protecting citizen's personal data is considered as a real challenge, according to the AUC report on Cybersecurity and Cybercrime trends in Africa, published in collaboration with Symantec, only 17 of the 55 Members of the African

Union have adopted comprehensive privacy laws, namely: Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia, and Western Sahara (Symantec, 2016).

At present, just few African countries are advanced in creating their own Data Protection Authority (DPA) to build digital trust, namely Benin, Burkina Faso, Cote D'Ivoire, Gabon, Mali, Morocco, Senegal and Tunisia (Rich, 2017).

Table 3

Country	**Name and/or reference of the Cyber laws.**
Algeria	-Protection of individual in processing personal data, Law N° 18-07 -Rules for the prevention and fight against offences related to Information and Communication Technologies (Law n° 09-04) adopted in 2010 -Criminal Code of 2004 for substantive law -Cybercrime act 2008 (Government of Algeria, 2018)
Angola	Personal Data Law (Law N˚. 22/11) effective since June 2011 (Government of Angola, 2011)
Benin	-Protection of Personal Data Law (Law N˚. 2009-09) enacted in 2009. (Hounkpe, 2011) - Criminal cyber activities provisions are included in a Law related to corruption (law N˚. 2011-20), adopted in 2011

	-Draft law on cybercrime
Botswana	-Electronic (Evidence) Records Act 2014 -Electronic Communications Transactions Act (N˚14 of 2014) came into force in 2016. -Cybercrime and Computer Related Crimes Act. (Government of Botswana, 2018)
Burkina Faso	-Law on the Protection of Personal Data (Law N˚. 010-2004 AN) enacted in 2004. (Government of Burkina Faso, 2004) -Draft law on cybercrime
Burundi	No cyber laws enacted
Cameroon	-Law on Cybersecurity and Cyber criminality (Law N˚2010/012) -Cybercrime Act 2011
Cabo Verde	- A comprehensive data protection regime was enacted in 2001 (Law N ° 133-V-2001) and amended in 2013 as Law N˚. 41/VIII/2013 (Government of Cabo Verde, 2013) - Draft law on cybercrime following Budapest Convention (2016) - E-commerce law adopted in 2013. - Law N°8/IX/2017 Provisions on cybercrime, on the collection of digital evidence and on international cooperation in criminal matters (UNIDIR, 2018) - Article 212 on computer fraude (UNIDIR, 2018)
Centre Africa Republic (RCA)	No cyber laws enacted
Chad	- Protection of Personal Data (Act 007/PR/2015) which was enacted in 2015. - Law N° 006/PR/2015, enacted in 2015, related to the establishment of National Agency for Computer Security and Electronic Certification. (Government of Chad, 2015) - Loi relatifs au cyber sécurité et la lutte contre la cybercriminalité (July 2014)
Comoros	No Cyber legislation in place
Congo	Legislations are in the process of adoption by the parliament

Cote 'Ivoire	-A Protection of Personal Data law was enacted in 2013 (Law N˚2013-450) (Government of Cote D'Ivoire, 2013). This law is the transposition of ECOWAS Supplementary Acts on data protection. -Law to fight cybercrime (Law N˚2013-451) (2013) -Law on e-transactions (Law N˚ 2013-546) (2013)
RDC	No cyber laws enacted
Djibouti	No cyber laws enacted
Egypt	-e-Signature Law No. 15, 2004 To complete
Equatorial Guinea	Law on Personal Data Protection (Law N˚ 1/2016) which was enacted in 2016. (Rich, 2017) No cybercrime laws enacted
Eritrea	No cyber laws enacted
Ethiopia	Criminal Code (Law N˚ 414) adopted in 2004
Gabon	In 2011 Gabon enacted the Protection of Personal Data Law N˚ 001/2011) (Government of Gabon, 2011) Draft cybercrime and e-transaction laws.
Gambia	Information and Communications Act 2009 which embodies cybercrime law and e-transaction Provisions.
Ghana	-Ghana Data Protection Act 843 was enacted in 2012. (Government of Ghana, 2012) - Mutual Legal Assistance Act 2010 (MLAA 2010) with provisions on international cooperation on cybercrime and electronic evidence -Electronic Transactions Act 2008 (Law N˚ 772). - Electronic Communications Act, 2008 (Law N˚ 775). - National Information Technology Agency Act, No.771, 2008

Guinea	Draft Law on Cyber Crime adopted by the Government in April 2016 Adoption de la loi L/2016/035/an relative aux transactions électroniques Adoption de la loi L/2016/037/AN relative à la cybersecurité et la protection des données à caractère personnelles
Guinea Bissau	No cyber laws enacted
Kenya	-Kenya Information and Communication Act 2009 To complete
Lesotho	-Lesotho's Data Protection Act N˚5 was published in 2012 (Government of Lesotho, 2012). -Bill on computer crime and cybercrime 2013
Liberia	-Electronic Transactions Law adopted in 2002 -No laws on cybercrime and data protection so far
Libya	No cyber laws enacted
Madagascar	-Personal Data Protection Law (Law N˚. LOI N° 2014 – 038) enacted in 2015. (Graham, 2015). -Law to fight against Cybercrime (Law N˚ 2014-006) adopted in 2014)
Malawi	No cyber laws enacted
Mali	-Personal data Protection Law (Law no. 2013/015) enacted in 2013. It is a transposition of ECOWAS Additional Act A / SA.1 / 01/10 on national law on data protection (Government of Mali, 2013). -Draft law on cybercrime
Mauritania	Law on cybercrime (Law N˚2016-007) enacted in 2016.
Mauritius	- The Data Protection Act 2017 - Introductory Guidelines on the Data Protection Act 2017 -Computer Misuse and Cybercrimes Act 2003

	- Electronic Transaction ACT 2000 - National Computer Board Act
Morocco	- Enacted in 2009, a Law on the protection of individuals with regard to processing personal data (Law N˚. 09-08) (Government of Morocco, 2009) -Penal Code, additional Law No. 07.003 of Morocco, 2003 concerning offenses relating to automated data processing systems -Law 75-12 approving the Arab Countries Convention on Cybercrime - Law 53-05 on the Electronic Exchange of Legal Data
Mozambique	No cyber Laws enacted
Namibia	-Draft law with substantive provisions (Electronic Transactions and Cybercrime Bill 2013) -Draft Cybercrime law -Finalized Electronic transaction Bill
Niger	-Draft Cybercrime Law - Draft data protection Law
Nigeria	-Cybercrime Act 2015 -Evidence Act 2011 -Computer Security and Critical Information Infrastructure Protection Bill-Sb 254 2005 -Nigerian Criminal Code, Cap. 77 LFN 1990 -Nigerian Communications Act 2003 -Nigerian Cybersecurity and Data Protection Agency Bill- HB, 154 C 4443, 2008 -Personal Information and Data Protection which is applicable to the private Sector only (2013).
Rwanda	Draft data Protection Law

	ICT Law: Governing Information and Communication Technologies (Law N°24/2016) Law on Establishing the National Cyber Security Authority and Determining Its Mission, Organisation and Functioning (Law No 26/2017) Law on Establishing Rwanda Information Society Authority and Determining Its Mission, Organisation and Functioning (Law N°02/2017) Law on prevention and punishment of cybercrime. Prevention And Punishment Of Cyber Crimes (Law Nº 60/2018).
Saharawi	No cyber Laws enacted
Sao Tome &Principe	Amendments to the Penal Code (Law 6/2012) which included illegal interception, computer-related fraud and child pornography
Senegal	-Protection of Personal Data law (Act N˚ 2008-12) enacted in 2008 (Government of Senegal, 2008) - Cybercrime law (N˚2008-11) -e-transactions Law (Law N˚. 2008-08) of 25 January 2008
Seychelles	-Law N˚ 9 of 2003 or Data Protection Act 2003 (SeyLII, 2003) -Computer Misuse Act 1998
Sierra Leone	Right to Access Information Act 20013
Somalia	No cyber Laws enacted
South Africa	-The Protection of Personal Information Act 4 of 2013 (Government of South Africa, 2013) -Draft law (Cybercrimes and Cybersecurity Bill) in National Assembly - Electronic Communications and Transactions Act N˚ 25 which was enacted in 2002 -Regulation of Interception of Communications and Provision of Communication Related Information Act (RICPCRIA) 2002
South Sudan	No cyber Laws enacted

Sudan	- National Telecommunication Corporation (Administrative decree N˚ 49) of 2009 on the establishment of the Sudan's Information Security Center -Cybercrime Act 2007
Swaziland	-Draft Computer Crime and Cybercrime Bill -National Information and Communication Infrastructure (NICI) Policy 2003
Tanzania	-Cybercrimes Act 2015
Togo	To see (No cyber laws in place
Tunisia	-Personal Data Protection Law (Law N˚ 2004-63) which entered into force in 2004 - Provisions on Cybercrime in Penal Code -Cybercrime Act100 (Law N°1999-89) -Electronic Signature and e-commerce Law, N° 2000-83
Uganda	-Computer Misuse Act 2011 -Electronic Signatures Act, 2011 -Electronic Transactions Act, 2011 - Regulation of Interception of Communications Act, 2010 - Uganda Communications Act, 2013 -Data Protection and Privacy Bill, 2015
Zambia	-Electronic Communications and Transactions (ECT) Act of 2009 -Computer Misuse and Crimes Act 2004
Zimbabwe	-Computer Crime and Cyber Crime Bill in preparation

Cyber legislations in Africa

2.3. Why Cybersecurity should be a top priority on the political agenda

In recent years, the worldwide proliferation of ransomware, the growing sophistication of malwares, the expansion of social media scams and the daily reported data breaches and disruptive cyber operations affect negatively Africa society and business as they rely more and more on cyberspace to perform critical activities.

For instance, in 2017, the massive and unprecedented ransomware attack WannaCry that infected more than 300,000 computers in over 150 countries worldwide causing billions of dollars of damage (BBC, 2017) has affected ten (10) African countries, namely Morocco, Tunisia, Egypt, Mozambique, Angola, South Africa, Tanzania, Kenya, Niger and Nigeria. The ransomware disturbed the functioning of networks and caused financial damage to Internet businesses within these countries (Mabika, 2017).

In Africa, banks and financial firms are regularly targeted by cybercriminals. For instance in 2017 a number of banks in West Africa (Cameroon, Congo (DR), Equatorial Guinea, Ghana, and the Ivory Coast) suffered at the same time and several times hacking attacks (CISOMAG, 2019).

Cybercrime is on the rise in Africa and represents a real threat for local economy. The cost of Cybercrime reached $3.5 billion annually across the Continent and many countries registered significant financial loss, such as Nigeria with $ 649 Million, Kenya with $210 Million, Tanzania with $99 Million, Uganda with $ 67 Million and Ghana with $54 Million (Serianu, 2017).

Even though the majority of cyber-attacks targeting Africa organisations and citizens remain unreported, because of the lack of technical cybersecurity skills and means to monitor and control ICT networks, as only 34 % of African countries have established their national CERT. The most widespread type of Cyber-attacks affecting African Countries are related to mobile scams, Government websites defacement, credit card fraud from banks, social engineering, Denial of service Attacks (DDoS), malwares and Botnet (Symantec, 2016). According to Dahir (2018), it is the Africa's banking sector and the mobile payment systems that face the highest risk from cybercrime in most African countries.

An analysis of cyber threat landscape in Africa shows a very low level of cybersecurity maturity within government agencies and businesses and lack of awareness on the risks associated with the use of digital technologies among populations. To tackle cybercrime and reduce the risks of financial loss that may slow the pace of digitalization of the continent, cybersecurity shall be on the top of the agenda of African states.

2.4. Conclusion

A secure digital environment is a shared and collective responsibility; it is a necessary condition for maximizing the potential of the ongoing Africa digital transformation and supporting its positive impact on human and economic developments across the continent.

An analysis of Africa cybersecurity landscape shows that cybersecurity is not a priority of African Governments and it is not high on the political agenda. Among the African States that already adopted their national cyber security policy and governance structure, cyber security is still considered as a purely technical issue as generally it is under the oversight of the Ministry of ICT. The majority of countries focus only on technical partnerships through CERTs to secure their national digital infrastructures and networks.

Furthermore, in most African countries, the Ministry of Foreign Affairs (MoFA) is not dealing with cyber issue while cyber security concerns are broader than national security and require regional and international cooperation to ensure coordinated actions to combat trans-border criminal use of digital technologies.

While some regional initiatives and processes are in place at continental level, through the African Union, and at regional level, through RECs, it is worth noting that the complexity and cross border nature of cybersecurity risks require coordination among all cyber actors to effectively prevent, respond and recover from cyber-attacks.

From a strategic perspective, a continental and harmonized approach on the main cybersecurity issues is necessary to facilitate intra-Africa collaboration to prevent and counter criminal activities carried out over Internet. while developing cyber diplomacy capacities is necessary to enable African countries to exchange information on cyber security policy, engage in bilateral and multilateral cyber dialogues and participate in

international discussions, namely at the United Nations, to mitigate the geopolitical implications of malicious operations in cyberspace such as cyber espionage and cyber terrorism.

Chapter 3

What are the driving forces for Cybersecurity in Africa?

3.1. Introduction

ICTs are of strategic importance for all people and governments across the world. They are the driving force of social development, economic growth and human progress.

Many governments consider ICT networks as critical national infrastructures, as they become the backbone of modern economies and essential for operating almost all relevant sectors today.

In Africa, the impact of using digital technologies is impressive, as it transformed the lives of millions of people in many ways. For instance, the large adoption of mobile communication technologies by population has significantly contributed to empowering people through enabling new development and creating innovative digital solutions that address some issues specific to the Continent.

Furthermore, the digital revolution and, particularly, the rapid expansion of mobile Internet services has largely contributed to the Africa's economic and social development. This is noticeable in specific areas, such as financial inclusion (mobile banking), health (mobile health) and farmers' productivity, as well as good examples of smart applications and programmes developed by African and responding to their community needs.

It is well known that Africa is a worldwide leader in mobile money transfer and payments, the success of M-Pesa as an enabling platform in Kenya is now expanded to seven other African countries and they are largely supporting the financial systems in these countries and enabled the financial inclusion of millions of people (Kende, 2017).

Moreover, the emergence of online platforms and applications in almost all African countries which are used for different purposes, such as helping farmers getting and exchanging information on weather and prices, as well as helping small business and entrepreneurs to expand their market access by facilitating and boosting intra Africa trade of goods and services. These experiences are a demonstration of the power of digitalization and influence of cyberspace in shaping economies and advancing humanity.

3.2. Africa digital agenda

Digital transformation is on the agenda of African countries. In 2017, during the fifth AU/EU Summit, African leaders expressed strong political commitment to embrace the fourth industrial revolution by supporting investment in digital infrastructures, mainstreaming ICTs as an enabler to increase efficiency and effectiveness of all sectors, developing Africa digital economy and cooperating with European Union on ICT policy, legal and regulatory frameworks including cybersecurity (Council of the European Union, 2017b).

While some African countries have already adopted their national plans to mainstream ICT & digital technologies in other sectors, as well as the rules to secure their national cyber space, African Heads and Governments have highlighted in Assembly decision AU/Decl.3(XXX) the need for building comprehensive and continental approach for safe and resilient African Cyberspace and pledged to make Internet & ICT central to Africa's development Agenda and work together to fight against any misconduct in African cyberspace (AUC, 2018a).

The Chairperson of the African Union recognizes digital transformation as a major element of change that can be used to address development challenges of important sector, such as education and health. He called Member States of the Union for positioning Africa Digital Transformation among the top priorities for the coming years to help achieving the Agenda 2063 aspirations which envision a peaceful, integrated and prosperous continent (AUC, 2019).

South Africa, through the establishment of the Digital Industrial Revolution Commission in 2018, with participation of five African countries, is leading a continental initiative aiming at coordinating the development of a common approach and plans to enable Africa to seize the huge opportunities coming with the 4th industrial revolution (Government of South Africa, 2018).

On the other hand, the smart Africa initiative, which gathers more than 20 African countries, private sector and partner organization, is gaining momentum in laying the foundations for a collective move towards an ICT and knowledge driven economy. As stated by H.E Paul KAGAME – President of Rwanda and Chairman of the Smart Africa Board – "Investment in ICTs is essential in taking any country to the next level of productivity and efficiency. Investing in ICTs is not at the expense of other sectors, investing in ICTs results in benefits for every sector and the earlier you start the better" (Smart Africa, 2015).

However, to fully benefit from digitalization, African countries need to develop adequate cybersecurity measures to prevent cyber incidents that may damage critical infrastructures and negatively impact the economy and social wellbeing of Africa citizens.

In this regard, the AU Summit endorsed a decision in 2018 elevating cybersecurity to a flagship project within the commission and requested the latter to support Member States in the process of developing national, regional and continental cybersecurity frameworks (AUC, 2018). But much remains to be done to push cybersecurity on the top of the political agenda of African governments and organization.

3.3. Impact of secured cyberspace on social and economic developments

As highlighted by Zhenmin in his speech, the world is in the middle of a digital revolution and it is not just about technological changes, but also about the centrality and interdependence of people and services (UNDESA, 2018b).

However, digitalization have brought additional security risks and challenges, as stated by United Nations Secretary-General António Guterres "governments and international organizations may not be prepared for rapid developments in the cyber environment, and existing regulations on how to address cybercrime may no longer be applicable" (UNDESA, 2018a, p.68), which means that technological changes require new policy and institutional frameworks to ensure the protection of public and social interests, as well as increase citizen's trust in using digital services and tools.

For African countries, this digital revolution offers a unique opportunity to develop new and innovative economic solutions, according to the United Nations e- government survey of 2018, many African countries are well advanced in implementing e-government and e-administration policies and strategies by capitalizing on ICT innovations and transforming the way public sector operates (UNDESA, 2018a). Though, cybersecurity of e-government systems remains a challenge for the majority of them, since it requires coordination at national level, with participation of all sectors and institution to ensure the protection of the huge amount of personal and sensitive data being collected and processed every day, within the framework of the delivery of online services to citizens.

In Africa, empowering financial ecosystem is among the priorities of the continent. For instance, the impact of Mobile Broadband on Africa economy is transformational and according to GSMA (2018), the Mobile ecosystem and related services generated in 2017 a total of $110 billion which is the equivalent of 7, 1 % GDP of Subsahara Africa. While, a study of Mckinsey Global Institute (2014) predicts a productivity gains between 148 billion dollars and 318 billion dollars in Africa for six important sectors, notably education, health, financial services, agriculture, retail and government.

Therefore, the security of networks and transactions is a condition for promoting financial inclusion and e-commerce within the region and, consequently, developing strong digital economy and society in Africa.

Moreover, with the adoption and operation of the Continental Free Trade Area (CFTA), which is in the process of entering into force after the adhesion of a large member of African countries as indicated by Commissioner Muchanga (2019), the development of intra-Africa digital trade requires strong cybersecurity measures and data protection legal frameworks to ensure digital trust and guaranty the security of African people.

Digital economy is a driver for global economic growth and affects all sectors of development, as it increases productivity, enhances efficiency, creates new markets and offers real opportunities for underdeveloped countries to catch up with the rest of the world, through getting access to global marketplace and joining international supply

chains. As stressed by Wladawsky-Berger (2017), the global digital economy in 2016 reached 11.5 trillion dollars which represented 15.5% of global GDP and it is expected to reach 25% in less than a decade.

Even though digital growth is centralized in advanced economies, Internet economy is growing fast in Africa and the ICT sector is already recognized as a pillar of national economy in several countries where ICT contributions to national GDP are substantial. For instance, in Kenya, it reached 9.2 % of national GDP in 2019 (Kenya Engineer, 2019), Mauritius it reached 5.6% contribution to national GDP in 2017 (Mauritius Economic Development Board), 11.81% to Nigeria's economic growth (Daka, 2018), reached in 2011 7% to national GDP in South Africa and 10% of National GDP in Tunisia (Essoungou, 2011).

On the social development aspect, cyber technologies and, more precisely, Internet have changed people's lives in Africa. They enabled social, financial and political inclusion, and gave access to online marketplaces and online education, through the proliferation of digital platforms and created direct interactions between citizens and governments. (Barnes, 2015).

3.4. Relation between Cyber security and Security

Cyberspace is becoming an area of political and economic stakes and cybersecurity as a national concern, directly related to security and prosperity of nations. As revealed in the Organization for Economic Cooperation and Development report (OECD, 2012), the

emergence of sovereignty considerations, in addition to the economic and social aspects, increased the importance of cyberspace. Therefore, many cybersecurity strategies highlight three aspects related to national security, namely the protection of critical infrastructure, the protection of the economy and the implications of cyber technologies (Lindstrom, 2012).

Moreover, cyberspace is increasingly used for military purposes, as stated by Prof. Ghernaouti-Hélie (2010) "Cyberspace is increasingly considered as a global economic and military battleground where all kind of cyber conflicts can arise, reflecting all kinds of political and economic competition ". To address cybersecurity issues related to national security, some African states are introducing cyber warfare in their military planning and organization, but the majority still do not see real threats related to cyber environment that can endanger their nations. At present, very few African countries have engaged in developing cyber capabilities. As reported by the Digital Watch observatory, only three countries, namely South Africa, Nigeria and Kenya, have engaged in developing offensive and defensive cyber capabilities, while seven countries (07), namely Algeria, Nigeria, Ghana, Uganda, Botswana, Zimbabwe and Gambia have developed only Cyber defense capabilities (GIP Digital Watch observatory, no date).

African countries are in the process of building their digital ecosystems and cyberspace. Therefore, the security of networks and critical information infrastructures are not yet the main concern, as the majority of countries focus only on increasing access to the global

cyberspace while neglecting the associated cyber threats (Van Vuuren, *et al*, 2013). Consequently and as stated by Tamarkin (2015), African states that fail to combat cybercrime will jeopardize their economic growth and national security.

3.5. Conclusion

The growing number of reported cyber-attacks with geopolitical implications targeting African countries such as the alleged Cambridge Analytica influence on 2017 Kenya elections results (Nyabola, 2018) and the misinformation campaigns known as the "coordinated inauthentic behaviour" using Facebook platform to spread fake news during elections in some Africa countries such as Nigeria, Senegal, Togo, Angola, Niger and Tunisia demand African governments to come up with a strategic response to prevent major cyber incidents or potentially devastating cyber-attacks that may disrupt the functioning of national institutions and economies. (BBC News, 2019)

On the other hand, the political will of African leaders to invest in digital developments and digital integration of the Continent require governments to take more decisive steps and put cybersecurity at the heart of their political agenda to create a safe, inclusive and resilient African online environment that attracts investments and allows innovations. The nascent cybersecurity ecosystem in the majority of African countries, marked by lack of awareness, scarcity of skilled personnel and lack of adequate regulations, exposes the continent to all types of cyber threats, as reported by Serianu, cybercrime cost the continent an estimated $3.5 billion in 2017 with almost 90% of African businesses not able to protect themselves against cyber-attacks. For most African states developing and

strengthening cybersecurity capacities and frameworks is a pre-condition for enabling digitalization of key sectors and reaping the enormous economic potentials of cyberspace.

In summary, the recognized impact of cyber technologies on national economy, security and social progress of people as well as Africa digital agenda, Africa security policy and Africa socio-economic development programs may act as a driver for change and boost the development of cybersecurity within the continent. It is for African states to see how to consider cybersecurity as top national priority and also see how to use the existing policy organs and mechanisms to address cybersecurity issues at regional and continental levels to ensure security and stability in Africa cyber space.

Chapter 4

How to use existing African Union decision making organs, special agencies, platforms and mechanisms to address cyber security related issues in Africa.

4.1. Organization of the peace and security landscape in Africa

Ensuring peace and stability across the Continent is one of the top priorities of the African Union (AU) towards the realization of agenda 2063 aspirations "the Africa we want". So far, many efforts and initiatives are undertaken by the AU, in close partnership with the United Nations, through signing a Joint Framework for Enhanced Partnership for a peaceful Africa in April 2017, and with the International Community to make peace a reality to all African people.

Although, the focus remains on preventing, resolving conflicts and addressing crisis situations in African countries, a significant progress has been made, these last years, in establishing institutions and mechanisms to search for sustainable peace and political solutions and enable development across the Continent. However, it is noticeable that existing mechanisms and programs do not include the threats and risks stemming from the use Information Communication Technologies (ICTs), as well as the new possibilities that cyberspace offers to perpetrate transnational criminal and terrorist activities that may also disrupt the functioning of African nations.

As highlighted by the UNGGE report in 2010, "existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century".

Cyber security issues are not fully addressed in Africa, both at policy and operational levels, while many African countries are in the process of developing their national cyber security frameworks and capacities, there is no regional and/or continental framework to discuss and develop a common African cybersecurity policy, as well as mechanisms to facilitate cooperation among African states in fighting against misuse of cyber technologies.

Furthermore, cybersecurity is not yet a topic on the political agenda of African leaders which make it a challenge for African states to secure their cyberspace and to collectively react to the international cyber threats.

4.2. Organs and Mechanisms dealing with Peace, Security and Stability in Africa

The overall vision of the African Union is “An integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in global arena”, to implement this vision and meet African people aspirations for a better life, the African Union established mechanisms and platforms that enable dialogues and cooperation on relevant issues (AUC, 2015).

In 2000, the African leaders adopted the Constitutive Act of the Union, which defined the principals of the African Union, namely sovereign equality and interdependence among Member States of the Union, peaceful co-existence of Member States and their right to live in peace and security, respect for democratic principles, human rights, the rule of law and good governance, as well as establishment of a common defense policy for the African Continent (AUC, 2000).

The constitutive Act identifies key decision and policy organs of the Union that have responsibility to promote peace and prosperity of the Continent, namely:

Assembly of the Union: As the supreme decision-making organ of the Union, it is composed of Heads of States and Governments. It has the mandate to determine the common policies of the Union, as well as monitoring their implementation.

The Executive Council: Composed of the Ministers of Foreign Affairs. This council takes decisions on policies in areas of common interest to the Member States and, as per its mandate, it monitors the implementation of decisions and policies formulated by the Assembly.

The Permanent Representatives Committee (PRC): Composed of Permanent Representatives to the AU and other Plenipotentiaries of Member States accredited to the

Union. It is charged with the responsibility of preparing the work of the Executive Council and acting on its instructions. It also establishes ad hoc committees and sub-committees when it is necessary.

Specialized Technical Committees (STCs): These AU organs are carried out by various sectorial ministerial conferences. They deal with a range of thematic areas, including ICT & Communication, as well as Peace and Security matters. The STCs are composed of Ministers and/or Senior Government Officials and have the responsibility to prepare and harmonize AU projects and programmes.

The Commission: it represents the African Union's secretariat and is composed of an elected Chairperson, Deputy Chairperson and eight Commissioners as well as Staff representing whole Africa. The AU Commission specific functions include, but not limited to, Represent the AU and defend its interests under the guidance of and as mandated by the Assembly and Executive Council; Initiate proposals to be submitted to the AU's organs, as well as implement decisions taken by them; prepare AU draft common positions and coordinate Member States' actions in international negotiations.

In an effort to address the existing and emerging security challenges within the continent, the AU established the African Peace and Security Architecture (APSA) in 2002 as a framework for promoting peace, security and stability in Africa. The operation of the whole architecture is supported by a number of structures, notably: Peace and Security

Council (PSC), Continental Early Warning System (CEWS), Peace Fund, AU Stand by Force, Panel of Wise, as well as Regional Mechanisms within Regional Economic Communities RECs / RMs (AUC, 2002). The Peace and Security Council (PSC) is the main pillar of APSA and it was established in 2004 as the standing decision-making body of the Union on peace and security issues.

The AU also established in 2010 the African Governance Architecture (AGA) as a comprehensive platform to facilitate dialogues and engagement of various stakeholders across the Continent on issues related to good governance, human and humanitarian rights and democratic practices.

While APSA is considered as an operational structure that plays an important role in preventing and responding to threats affecting peace and security across the Continent, AGA is seen more as a coordinating body that enables policy processes and dialogues on relevant topic of common interest for African nations. According to Bedzigui (2018), we need to link the two AU instruments APSA and AGA to enhance AU response to instability within the Continent, since both architectures include PSC and most security crisis or conflicts are related to either instability in Africa, bad governance or non-respect of democratic rules and human rights

Whilst the AU member states and International Community recognize and commend the progress made by AU through establishing and using APSA and AGA institutions and

mechanisms to promote development and social wellbeing of African People. These two Architectures (APSA and AGA) did not include policy dialogues on cybersecurity, Internet policy or any other topic related to Digital policy as an emerging issue to enable the Continent to tackle the challenges of the digital era.

4.3. Addressing Cyber security at continental level through existing platforms

The increasing proliferation of cyber-attacks has triggered international discussions and negotiations on the security and governance of cyberspace. Many regions have crated platforms for formal and informal cybersecurity discussions and proposed strategies and norms to regulate states behaviour in their cyberspace.

For Africa, despite the adoption of the Malabo convention in 2014, discussions on cyber issues are still handled at the technical level and most of the time do not include other aspects, such as security, economy, development and diplomacy.

As African countries are embracing their digital future, there is a need to adapt the existing regional and continental platforms, mechanisms and agencies to the reality of digital environment to fully harness the potential cyber technologies and mitigate cyber risks.

Through the African Union, African governments can rely on existing instruments and mechanisms to establish common policy approaches and norms of responsible behaviour

in African cyber Space, and this may include all cyber security aspects, such as security, international cooperation and protection of African human rights in Cyberspace.

For instance, APSA and AGA Architectures can be used to address challenges posed by the digital technologies advancements like the increasing risks associated with very sophisticated, dangerous and global scale cyberattcks that may have negative implications on individuals, societies, national security, as well as inter-states diplomatic relations.

4.3.1. Distribution of cyber related tasks among AU organs and structures.

As highlighted by Chergui, AU Commissioner for Peace and Security, the strategic priorities of APSA roadmap (2016-2020) are five and focus on conflict prevention, post conflict reconstruction and peace building, crisis management, coordination and partnership, as well as dealing with strategic security issues such as the security challenges in relation to the illicit use of ICTs (AUC, 2015).

4.3.1.1. African Peace and Security Architecture (APSA)

4.3.1.1.1. Continental Early Warning Systems (CEWS)

The Continental Early Warning Systems (CEWS) is an AU organ established under article 12 of the PSC Protocol, with the main objective of anticipating and preventing conflicts by providing timely information and analysis response options (AUC, 2015).

Considering the increasing pace of digitalization in Africa and the growing importance of cyberspace, this organ can include in its portfolio reducing the risks associated with

the use of digital technologies for political and/or military reasons and prevent any disruptive or destabilizing cyber operations in the region.

Nowadays, cyber incidents represent a serious threat to national security and economy. As reported by the BBC (2018b), the alleged interference of Russia in USA presidential elections of 2016 has drawn the attention of the world on new risks of espionage and interference in states internal affairs and on the tensions that may result from this kind of cyber operation. Many Regional inter-governmental organisations have already adopted their confidence and trust measures, known as Confidence Building Measures (CBMs), to enhance inter-states cooperation and ensure security and stability in their cyberspace. In this regard, Pawlak (2016) described CBMs in Cyberspace or Cyber CBMs as preventive diplomacy measures aiming to avoid the use of force in cyber domain through practical steps that increase transparency, predictability and stability.

The Organization for Security and Co-operation in Europe (OSCE), as the world's largest regional security organization, with 57 Member States from Europe, North America and Asia, adopted the first set of initial CBMs in 2013 (OSCE, 2013) and expanded the list in 2016 (OSCE, 2016a). As stated by Steinmeier (OSCE, 2016b), a Germany's Foreign Minister and OSCE Chairperson for the year 2016 "Through its engagement in cyber-related activities, the OSCE underlines its capacity for enhancing confidence between States". Indeed, the CBMs adopted by OSCE aim, on voluntary basis, to mitigate cyber-attacks within the territory of its state members through enabling direct dialogues,

transparent exchanging of relevant information between competent authorities on vulnerabilities and incidents to enable collective response to cyber-attacks.

The Foreign Ministers of the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) also engaged in developing CBMs and agreed in 2012 to develop "A work plan on security in the use of ICTs focused on practical cooperation on Confidence Building Measures". The work plan was adopted in 2015 and put in place an Inter-Sessional Support Group composed of Senior Officials and ARF Foreign Ministers to promote CBMs and Preventive Diplomacy through practical cooperation actions among states (ASEAN, 2015).

And recently, the Organisation of America States (OAS) engaged in the development of Regional CBMs to facilitate collaborative efforts to increase trust and stability in its cyberspace, while promoting peaceful uses of cyberspace. (OAS, no date).

Although, African countries are at early stage of developing their cyber capabilities, both offensive and defensive, and the majority do not consider yet the risks related to the militarization of cyberspace. There is a need to initiate cyber dialogues and adopt confidence measures to avoid misperceptions, prevent tensions and facilitate cooperation among African states and non-states actors in responding to major and complex cyber incidents targeting African countries.

Therefore, to prevent cyber conflicts in Africa, CEWS can play a critical role in warning on cyber risks, preventing the use of cyberspace for criminal and terrorist activities through elaborating CBMs and preventive cyber diplomacy principals that should be adapted to the reality of Africa cyber domain and consistent with international laws, as well as Africa security frameworks.

4.3.1.2. African Union Mechanism for Police Cooperation (AFRIPOL)

The proliferation of digital Technologies, notably mobile phones, has created new possibilities to perpetrate transnational and organized criminal activities at a large scale, using ICTs and amplified security challenges in Africa.

Although cybercrime is mentioned as a transnational organized crime, under the strategic security issues that needs to be addressed by AU, the APSA roadmap 2016-2020 highlighted the absence of collective anti-cybercrime policy at continental level which are due to the lack adequate legal instruments and the absence of national cybersecurity frameworks, as well as the absence of agreements on mutual assistance in combating cybercrime within RECs and also from REC-to-REC (AUC, 2015).

As indicated in the policy framework "the Status of the African Mechanism for Police Cooperation (AFRIPOL)", Afripol as the technical body of the AU has the mandate to coordinate actions of African Police at the strategic, operational and tactical levels to facilitate the prevention, detection and investigation of transnational and organized crime across Africa.

During the Second African General Assembly of the African Police Organization held in Algiers in 2018, Afripol members agreed to establish three task forces to counter transnational crime, terrorism and cybercrime as key priorities for the region (Technomag, 2018). This shows the commitment of AU Member States to collectively engage in fighting illicit activities in cyberspace. However, considering the borderless and complexity of cybercrime, there is a need to harmonize cybercrime laws and enhance cooperation with other AU organs and structures to effectively tackle misuse of cyber technologies within the territory of AU Member States.

Therefore, each Afripol members should establish a cybercrime agency/ unit to deal with cybercrime at a national level and Afripol secretariat should establish a Continental Cybercrime Center devoted to preventing, coordinating efforts and fighting cybercrime at continental level, in close collaboration with AU Peace and Security Department and AU structures dealing with security issues, as well as with all relevant ministries in the Member States of the African Union.

4.3.1.3. Committee of Intelligence & Security Service of Africa (CISSA)

The Committee of Intelligence & Security Service of Africa (CISSA) was established by Heads of Intelligence and Security Services of Africa in 2004 to provide leadership with regard to intelligence and security matters and further peace, security and stability in Africa. CISSA is a platform for cooperation that aims to assist AU policymaking organs to effectively address security challenges among intelligence and security organisations

of AU Member States, through facilitating dialogues, studies, strategic intelligence analysis on peace and security threats, consulting and concerting to develop harmonized approaches for common security threats within the continent (CISSA, no date).

The 12th CISSA Conference, held in June 2015, requested CISSA members to host a workshop on cyber security as a response to the growing threats posed by cybercrime in African countries. The workshop underscored the security challenges emanating from cyberspace and came up with recommendations where they called African countries to "consider a cyber-attack targeting one African country as an attack on the continent" and emphasized on the need for CISSA Members to support the development of CERTs, both at national and regional levels (CISSA, 2015, p.11). The need to establish National and Regional CERTs was further emphasized in the 627th PSC meeting statement (AU Peace and Security Council, 2016) and the 2017 ICT ministers` declaration [AU/STC-CICT-2/MIN/Decl. (2)]

To counter cybercrime and use of ICT for terrorism in Africa, there is a need for CISSA Members to work in close collaboration with their national CERTs, cooperate with RECs for the establishment of Regional CERTs and support the establishment and operationalization of AU-CERT to be integrated under CISSA structure to effectively coordinate investigations, exchange of sensitive information among AU Member States.

Considering the Organisation of American States (OAS), experience in creating and managing the CSIRTAmericas.org, the establishment of AU-CERT can be supplemented by a virtual platform to interconnect National & Regional CERTs and AU-CERT to facilitate timely information sharing, coordination and better understanding of cyber incidents targeting the region (Subero, 2018).

4.3.1.4. African Centre for the Study and Research on Terrorism (ACSRT)

The AU Plan of Action on Preventing and Combating Terrorism in Africa was adopted by the AU High-Level Inter-Governmental Meeting in 2002. Two years later, the African Centre for the Study and Research on Terrorism (ACSRT), structure of the AU Commission, was established as a forum that enables cooperation among AU Member States and Regional Mechanisms to counter terrorism in the region. ACSRT mandate includes the conduct of research, analysis and studies on terrorist threats in Africa, maintaining a terrorism database and sharing information as well as promoting Mutual Legal Assistance and cross-border counterterrorism operations among African countries.

Terrorist operations using ICT networks and Internet are taking place in several African countries, as recognized by the PSC members in the press statement [PSC/AHG/COM. (DCCXLIX)] related to the 749th meeting held at the level of Heads of States, AU Summit 2018, where they reaffirmed "the need to counter the use of ICT technologies by terrorist groups, whether in their fundraising, narrative promotion, and recruitment of others to commit terrorist acts" (AU Peace and Security Council, 2018).

To address the use of digital technologies for terrorist purposes within Africa sub regions, there is a need for joint efforts and enhanced cooperation between ACSRT, CISSA, AFRIPOL, RECs Regional Mechanisms and AU Member States. This can be facilitated by creating Continental Coordination Mechanism to be supplemented by virtual platform to raise awareness, monitor and combat online terrorism and terrorist use of ICTs in Africa.

4.3.1.5. Africa Governance Architecture (AGA)

AGA architecture is the coordinating body of the AU and it is composed of several organs and institutions, namely Continental Early Warning System (CEWS), Economic, Social and Cultural Council (ECOSOCC), New Partnership for Africa's Development (NEPAD), AU Advisory Board on Corruption, the African Commission on Human and Peoples' Rights (ACHPR), the African Court on Human and Peoples Rights, the African Peer Review Mechanism (APRM) Secretariat, Permanent Representatives of Member States, in addition to the AU Commission, RECs and PSC.

AGA secretariat is hosted by the AU Commission and coordinates policy debates and concerted approaches on issues related to the socio economic development, human and people rights, as well as governance and knowledge management and engagement with citizens. Furthermore, AGA plays a role in updating and raising awareness of the member of the PRC, the PSC and even the Executive Council on possible threats to the security of African States as well as on relevant issues of common interest.

Considering the growing and strategic importance of cybersecurity and taking into account that digital developments affect also political elections, public policy deliberations, social cohesion, education, entertainment and even inter states diplomatic relations (Kurbalija, 2017), there is a need to use AGA architecture to organize open dialogues on cyber related issues with participation all concerned stakeholders across the continent.

Moreover, the emergence of privacy issues and security threats in the use of cyberspace require adequate policy, legal and regulatory frameworks as well as norms and rules that ensure the security of and in the use of digital technologies and services.

For this reason, Getao, ICT secretary Ministry of ICT of Kenya highlighted the need for African countries to build a common cybersecurity culture and values, as well as to agree on basic principles that reflect the expectations of African governments, businesses and individuals to fully harness the benefits of cyberspace. From Getao perspective, Malabo Convention can serve as a source to develop and agree on norms of responsible state behavior in African cyberspace, since it has reached the consensus of all AU Member States (ICT4Peace Foundation, 2015).

For instance, Article 24 of the Convention defines national cybersecurity framework and called each state to adopt national cybersecurity policy and strategy that respects the nation identity. Article 27 provides guidance to AU Member States on cybersecurity

governance and the organizational structures at a national level, while Article 25 outlines the need for legislative reforms and points out the cyber legislations that need to be in place in each African country to ensure secure and safe cyber domain.

Furthermore, the Convention provisions have emphasized on important principals to govern African cyber domain, such as the protection of personal data, the protection of critical infrastructures and investment in education and cyber capacity building.

Within AGA framework, the AU Commission on Human and People rights (ACHPR), the Economic, Social and Cultural Council (ECOSOCC), the Regional Economic Communities (RECs) and the AU Commission, Africans can engage in multi stakeholder discussions and policy debates on ways to ensure the protection of African people rights and fundamental freedoms in the digital environment.

For instance, Privacy is considered as a fundamental human right in the Universal Declaration on Human Rights (article12), as well as in the International Covenant on Civil and Political Rights (article19) and online privacy is recognized by the UN General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 as the right to privacy in the digital age.

In Africa, in addition to the “African Charter on Human and People Rights”, most states recognize the right to privacy in their national constitutions but do not have the legal and

technical tools to protect the online privacy of their citizens, due to the complexity of privacy concerns in the digital environment.

As stated in the "Personal Data Protection Guidelines for Africa", for Africa to increase the legal certainty that enables electronic transactions and the development of sustainable digital economy , there is a need to develop a common African approach on online privacy and data protection that responds to the African context, notably: the culture and legal diversity across the Continent, variations in access and adoption of digital technologies, as well as the level of cyber laws and governance among African countries. (ISOC, 2018)

Another sensitive topic in the global digital policy is how to conciliate between security of information systems and online freedoms and how to balance security of digital assets and human rights in the online environment. These aspects are still a challenge for a number of African countries. The News 24 (2019) reported a number of 21 Internet shutdowns across Africa in 2018 against 13 in 2017 which unfortunately had economic implications in the region. For instance, CIPESA (2017) points out that Internet shutdowns have cost up to US$ 237 million in Sub-Saharan Africa since 2015. Moreover, Internet Shutdowns, restrictions and content blocking affect negatively the everyday life of African citizens as they rely on Internet to access knowledge and perform important activities, such as communicating with others.

The relationship between the respect of people's digital rights, the principal of free flow of information and socio-economic development is recognized by the G20 Digital Economy Ministerial Conference in its declaration in 2017 that reads: "We recognize that freedom of expression and the free flow of information, ideas and knowledge are essential for the digital economy and beneficial to development".

Africa digital transformation relies on adapting African Laws and institutions to the evolving online environment and empowering African citizens to enable them to maximize the benefits of the digital revolution. In this context, AU policy organs, such as AUC, ACHPR, ECOSOCC and RECs under AGA coordination need to see how to conciliate the technological changes with the existing human and people rights principals and see how to align them to the digital era.

In Africa, we need to promote cyber security culture and agree on common norms of Africa states conduct in cyberspace in accordance with the declaration on the code of conduct on Inter-africa relations (AU, 1994), as well as on ways to enable dialogues among relevant stakeholders to address cyber risks threatening Africa economy and social cohesion.

4.3.1.6. AU Commission, NEPAD and African Peer Review Mechanism (APRM)

The increasing uptake of ICTs and the growing dependence of societies and economies on cyber technologies for performing daily activities, have made it mandatory to all actors to build cyber security capacities.

To address the technical and political implications of digitalization, it is mandatory for all nations and stakeholders to promote cyber security culture and build cyber capacity. For Africa, as per the decision AU/STC-CICT-2/MIN/Decl. (2), the ICT Ministers tasked the AU Commission to dedicate appropriate resources and develop comprehensive cybersecurity programs to assist Member States in developing their national cybersecurity frameworks.

Furthermore, the AU Executive Council adopted a decision in 2018, calling for the creation of Africa Cyber Security Collaboration and Coordination Committee (ACS3C) to advise AUC and policymakers on cyber strategies. This cyber security expert group is being created by the AU Commission and will address aspects related to capacity building in Africa (AUC, 2018).

Furthermore, the AU Commission, in collaboration with New Partnership for Africa's Development (NEPAD) will play a critical role in building cyber capacities of African States through implementation of long term capacity building and education programs for African professionals and citizens on necessary measures and actions to ensure the safe use of cyber technologies.

In addition, the two organisations can collaborate and create the African Cybersecurity Center of Excellence to assist AU Member States in developing comprehensive and

detailed national cyber security awareness and sensitization programs and also equip African Experts with the cyber security knowledge, both on the technical and operational aspect, to enable African states to build and strengthen their cyber capacities.

On the other hand, the African Peer Review Mechanism (APRM) can play an important role in assessing the cybersecurity readiness of African countries and review their compliance with international standards, notably the national Cyber security governance, institutional and legal frameworks as a first step to identify the adequate assistance for each country and sub-region.

The AUC Chairperson Office can create a special Unit to coordinate cyber security activities and relevant digital policy issues within the Commission and AU organs and structures. The AUC Chairperson Office will spearhead the development of Africa cyber security strategy in line with AU global policy and vision.

4.3.1.7. Peace and Security Council (PSC)

As indicated in the protocol related to the establishment of the PSC of the African Union (AU, 2002), the main objective of PSC is "to promote peace, security and stability in Africa, in order to guarantee the protection and preservation of life and property, the well-being of the African people and their environment, as well as the creation of conditions conducive to sustainable development". However, in today digital and interconnected world, where almost all strategic activities and services are shifting to cyber space, the AU declaration on security policy and other security policy documents and instruments

such as the solemn declaration on a common African defense and security policy, the AU Peace and Security roadmap for Africa, as well as the AU Chairperson reports do not consider cybersecurity issues as a threat to the security of the continent. (AUC, 2015).

The Peace and Security Council, in its 627th meeting of 26 September 2016, dedicated an open session to the theme: "The crucial role of cybersecurity in the promotion and maintenance of peace and security in Africa". The Council members and participants highlighted the important impact of ICTs & Internet on human and economic developments. They also stressed the need for effective Internet governance, as well as regional and global frameworks for promoting security and stability in the cyberspace, as matters of strategic importance for the Continent (AU Peace and Security Council, 2016).

In this meeting, the Council Members underscored the importance of regional and international cooperation in promoting security and stability in the global cyberspace. They welcomed the ongoing consultations of the United Nations Group of Governmental Experts (UNGGE) on the establishment of a global cybersecurity framework and encouraged AU Member States to take advantage of international capacity building initiatives and programs, such as the Global Forum on Cybersecurity Experts (GFCE) to build their cyber capacities.

Moreover, since both CEWS and AGA report to PSC, the latter can be a platform for discussing and framing the African CBMs and the African Cyber Norms, in addition to

effectively coordinating efforts and initiatives emanating from different structures, such as CISSA, AFRIPOL and ACSRT to combat cybercrime and terrorist use of ICTs in Africa.

4.3.1.8. Permanent Representative Council

Considering the strategic stakes of international negotiations and discussions on cyber related issues, Africa as a region needs to come up with a common approach to guide African states engagement in international cybersecurity policy dialogues, either on bilateral or multilateral levels.

To understand today international cyber politics and coordinate Africa participation in international cybersecurity fora and process, namely at the United Nations level, and enable African countries to adopt common cyber policy positions that reflect and respond to the African people's aspirations for a prosperous digital future. There is need to organize formal discussions among the members of the African Union on international cybersecurity policy and its implication on Africa digital development, as well as on Africa peace, security and stability.

Therefore, it is urgent for AU Member States at the level of Permanent Representatives Committee (PRC) of the AU to engage in interactive discussions on cyber policy and elevate the outcomes to the AU Executive Council to agree and adopt Africa positions on

important international information security and cybersecurity geopolitics to avoid divergent African views on the governance of global cyber space

4.3.1.9. Executive Council

The rapid developments in cyberspace and the implications of cybersecurity dialogues on inter-States and international relations have raised the need to develop and engage in diplomatic practices related to cyber issues.

For instance, the Council of the European Union adopted in 2015 recommendation on Cyber diplomacy aiming at promoting the EU values in cyberspace, safeguarding EU digital interests, coordinating the political, economic and strategic engagements of the Union with partners and international organisations on cyber issues, as well as promoting the Budapest Convention as a treaty for international cooperation (Council of the European Union, 2017a).

Furthermore, according to Radunovic (2017), in the absence of consensus on global treaty to regulate and govern cyber operations and due to the geopolitical and economic consequences of cyber-attacks, many digitally advanced states rely on diplomacy (cyber diplomacy), either on bilateral or multilateral basis, to advance their cyber security agenda.

In Africa, despite the Peace and Security Council calling Member States to develop cyber diplomacy capabilities and participate in international discussions on the governance of

the internet and cybersecurity issues (AU Peace and Security Council, 2016), not all African countries involve the Ministry of Foreign Affairs in cyber related discussions or equip their diplomats with the necessary skills on such technical topics.

In 2018, Cyber security debates were very divisive between the super powers, with the emergence of two cyber blocks: Western states against China, Russia and their allies, especially after the failure of the UNGG (2017-2016) to issue a consensus report and the endorsement of UNGA in 2018 of two parallel and competing processes which may change the direction of inter-governments cyber discussions (Meyer, 2018).

As stressed by Tikk (2018), prediction for 2019 will mainly focus on the consultations of the Open Ended Working Group under UN auspices to further develop rules, norms and principles of responsible states' behavior in cyberspace and see how to accommodate all states' needs and priorities. This is a great opportunity for African states to coordinate their cyber policy positions and participate as region in this global discussions on international information security.

To engage African leaders and Ministries of Foreign Affairs in cyber dialogues and international cybersecurity politics, there is need to create the African Union Senior Government Officials Group (AUSGOG) that will report to The Permanent Representatives Committee (PRC) and then to the Executive Council for endorsement of

decisions related to international cyber security policy where Africa's position is necessary.

The AUSGOG, through open and regular dialogues at the level of PRC, will coordinate the participation of African countries in cybersecurity multilateral debates, namely the UNGGE (2019 -2021) and the UN Open-Ended Working Group and will facilitate the adoption of political decisions on common African positions on relevant issues in line with AU vision and digital development agenda.

The Permanent Representations of the AU in Geneva, Brussels and New York in close collaboration with AUSGOG will advocate for a coordinated Africa cyber diplomacy in line with Africa foreign and security policy.

Furthermore, the creation of Governmental Expert Group on Cybersecurity, composed of Senior Governments Officials, will help in raising awareness of African leaders on the huge opportunities of cyberspace, as well as on cyber threats and the required policy and operational measures to be taken, both at national, regional and continental levels, to build digital trust for safe, inclusive and secure African Cyber space.

4.3.1.10. AU Summit

Along with the implementation of Africa Agenda 2063 Aspirations and the digital transformation strategy of the Continent to build a sustainable and strong digital economy

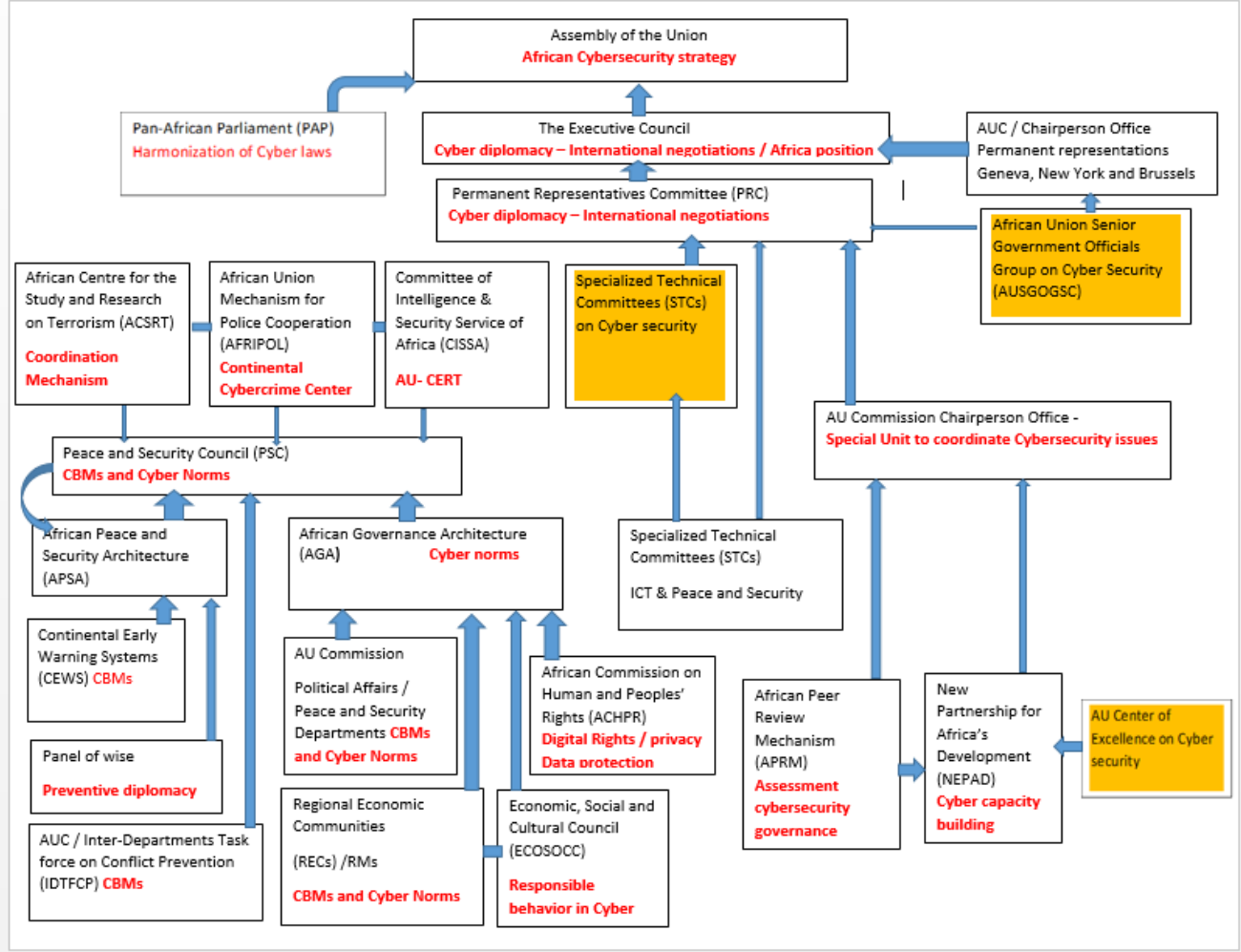
in all AU Member States, African countries need to mainstream digital policies and cybersecurity in all sectors.

The AU Summit may include cybersecurity in its political agenda, through establishing a Specialized Technical Committee (STC) on Cybersecurity like ASEAN Ministerial Conference on Cybersecurity (Koh, 2017) and encouraging an active and coordinated participation of African states and non-state actors in international cybersecurity policy debates.

The Summit may also adopt Africa International Cybersecurity Strategy to be guided by Africa various foreign policy documents and strategies to help African countries to speak with one voice in international fora.

4.3.2. The structure to adopt to address cybersecurity issues in Africa

To comprehensively address cybersecurity issues in Africa, by involving all the actors and using the existing platforms and mechanisms to enable discussions, develop policies and react to international cybersecurity threats by engaging in diplomatic responses, I propose the below structure:



Conclusion Chapter

Cyber security has become a major concern across the world, as the emergence of security issues associated with malicious use of Information Communication Technologies and Internet have led to international cyber policy discussions and negotiations, both in formal and informal fora, to define how cyberspace can be used, regulated and secured for the benefit of all people and states worldwide.

Considering the growing number of cyber-incidents, protection and prevention against illicit online activities become a collective responsibility that requires cooperation and coordination among a wide variety of stakeholders, both within and between states, to promote peace, security and stability in cyber domain.

Cybersecurity is a complex and cross cutting issue, Kurbalija (2017) identified the link between cybersecurity, human rights and the economy or Business as the "digital social contract" where governments need to balance between security, free follow of information and respect of people's rights. In this regards, the UN recognizes the rights of people in the digital age and calls for the preservation in the digital space of the same rights people enjoy offline (UNHRC, 2014).

African leaders committed themselves to seize the opportunities of technological development by investing in digital infrastructures and mainstreaming digitalization as an enabler for achieving national development agenda (Council of the European Union,

2017b). After the adoption of the AU Convention on Cybersecurity and Personal Data Protection "Malabo Convention" in 2014, which is yet to enter into force due to the low number of ratifications. To accelerate the ratification process within AU Member States, the commission has to escalate the issue to the Ministerial Committee on the Challenges of Ratification/ Accession and Implementation of AU Treaties and engage in reflections to find the appropriate way of transposing the Malabo convention provisions to national laws to harmonize cybersecurity frameworks at continental level.

Furthermore, considering the highly sensitive nature and international implications of cybersecurity policy on economy, social wellbeing of people and even on inter states diplomatic relations, Africa needs to elevate cybersecurity among its top priorities and put in place technical and institutional measures to mitigate cyber threats.

For Africa, ensuring secure and safe cyberspace is a pre-condition and key enabler to foster its digital transformation for more inclusive and integrated socio-economic development that meets the aspirations of African people.

In light of the criticality of cybersecurity issues, African countries should care about mainstreaming cyber security into their foreign and security policies, along with the development of their digital agenda. While some African countries reached a certain level of cybersecurity maturity and have put in place their national cybersecurity frameworks, the majority is still in the process of developing its national strategies, reforming legal

frameworks and establishing incidents response mechanisms, this exposes the Continent to dangerous cyber incidents that may disrupt African nations' economy and security.

Although, almost all adopted national cyber security strategies and policies across Africa acknowledge the importance of international cooperation to fight against criminal activities in cyberspace, the level of participation of African representatives in international cybersecurity debates remains low and limited to some countries. Furthermore, the reported cyber cooperation of African states is generally limited to technical aspects, such as membership in FIRST and membership in the CoE Glacy+ Project, and generally it does not involve policy makers or the Ministries of Foreign Affairs.

While bilateral cyber agreements are on the rise among developed states (GCSC, 2017), African countries need to engage more in cyber diplomacy efforts to position themselves in international fora, as a region that aims to play an active role in shaping the governance of global cyberspace, as the latter impacts directly the national security and sovereignty of states as well as the global economy and international peace and security.

For this reason, African countries need to come up with common understanding on international cyber policy and cyber politics to identify and promote Africa interests in the digital world and move from the actual position where African countries are seen as

demanding and focusing only on capacity building at the expense of their foreign and security policy (Segal and Waxman, 2011).

Moreover, It's imperative for African countries to move towards more harmonized and concerted reactions and positions to international proposals, such as the outcomes of the UNGGEs, implementation of the UNGA resolutions on cybersecurity, the Paris call for Digital trust in cyberspace, the adhesion to Russia Convention on cybercrime which was submitted at the UN level, the EU General Data Protection Regulation (GDPR) and its impact on Africa business and government institutions as well as the ratification of Budapest Convention as an international instrument to counter cybercrime.

Although there are many policy organs, structures and processes in place, both at regional and continental levels, that address issues of common interests for African states, such as security, governance and human rights, there is not yet a regional or continental strategic approach on cyber security for Africa.

To raise awareness of African leaders on the strategic importance of cybersecurity, enable the development of African CBMs and Cyber norms, promote cybersecurity culture, establish incident response mechanisms at regional and continental levels, facilitate the adoption of Africa Cybersecurity strategy to effectively coordinate and guide Africa participation in international cyber debates, the African Union can play a coordinating role and bring together all stakeholders and actors for inclusive and interactive

discussions on cybersecurity related matters, such as security, socio-economic development and digital right of people.

This research paper proposes an AU cybersecurity structure based on the use of existing platforms and mechanisms within the African Union to develop and strengthen cybersecurity and cyber diplomacy capacities of AU Member States and coordinate Africa participation in international negotiations, notably at the UN level.

The structure will enable African states to debate, at different levels, on cyber policy as well as emerging digital policy issues. For instance existing platforms such as APSA, AGA, PSC and PRC can be used to develop Cyber Norms and CBMs that respond to African context and which will help African governments to address new challenges associated with the misuse of ICTs. While AFRIPOL, ASCERT, CISSA and AUC Peace and Security Department will coordinate efforts to counter cybercrime and use of ICTs for terrorist purposes. In addition to proposing new organs such as a Specialized Technical Committee on Cybersecurity and the creation of an African Union Senior Government Officials Committee on Cyber security to advise the Executive Council and AU Summit on Cyber diplomacy and international cyber politics and work towards adopting Africa cyber security strategy.

The pace of technological innovation and technical changes is very fast, notably the significant advances in Artificial Intelligence (AI), Internet of Things (IoT), Big Data

Analytics and the Cloud Computing, which, for sure, will revolutionize the world in the near future (Richards, 2019). This digital revolution requires more participation and forward looking policies from African states to maximize the potential of cyber technologies, as a key enabler to achieve the Agenda 2063 goals for a peaceful, prosperous and digitally integrated Continent.

References

Access Now (2017). A *Policy Maker's Guide to the Global Conference on Cyberspace 2017.* Available at: https://www.accessnow.org/cms/assets/uploads/2017/11/A-Policy-Makers-Guide-to-GCCS-2017-digital-v.pdf [Accessed 15 March 2019]

AfricaCERT (no date). *Countries.* Available at: https://www.africacert.org/home/countries/ [Accessed 15 August 2018]

African Union Peace and Security (no date). *About the African Centre for the Study and Research on Terrorism (ACSRT).* Available at: http://www.peaceau.org/en/page/2-3591-static-about-african-centre-for-study-and-research-on-terrorism-ACSRT [Accessed 15 August 2018]

African Centre for the Study and Research on Terrorism [ACSRT] (no date). *Homepage.* Available at: https://caert.org.dz/ [Accessed 15 August 2018]

African Commission on Human and Peoples' Rights [ACHPR]. *African Charter on Human and Peoples' Rights*. Available at: http://www.achpr.org/instruments/achpr/ [Accessed 15 August 2018]

African Internet Governance Forum [AfIGF] (no date). *Homepage.* Available at: https://www.afigf.africa/ [Accessed 15 August 2018]

African Union [AU] (1994). *Declaration on the Code of Conduct on Inter-Africa Relations.* Available at: https://academic.oup.com/rsq/article-abstract/13/2-3/169/1561447 [Accessed 15 March 2019]

African Union [AU] (2002). *Protocol relating to the establishment of the peace and Security Council of the African Union.* Available at: http://www.peaceau.org/uploads/psc-protocol-en.pdf [Accessed 15 March 2019]

African Union [AU] (2017). *The second Ordinary Session of the AU Specialized Technical Committee (STC) on Communication and ICT (CCICT-2),* 20-24 November. Available at: https://au.int/en/ccict2 [Accessed 15 March 2019]

African Union [AU] Peace and Security Council (2016). *Press Statement*, 627th Meeting PSC/PR/BR (DCXXVII). Available at: www.peaceau.org/uploads/psc-pr-627-cyber-security-26-9-2016.pdf [Accessed 15 March 2019]

African Union [AU] Peace and Security Council (2018). *Press Statement*, 749th Meeting PSC/AHG/COM (DCCXLIX). Available at: www.peaceau.org/uploads/psc.summit.749.com.ahg.terrorism.27.01.2018.pdf [Accessed 15 March 2019]

African Union Commission [AUC] (no date). *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection*. Available at: https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_2.pdf [Accessed 23 March 2019]

African Union Commission [AUC] (2000). *Constitutive Act of the African Union.* Available at: http://www.peaceau.org/uploads/au-act-en.pdf [Accessed 15 August 2018]

African Union Commission [AUC] (2010). *AU Summit of Heads of States and Governments declaration*, Assembly/AU/11(XIV). Available at: https://au.int/en/decisions-102 [Accessed 15 August 2018]

African Union Commission [AUC] (2014). *African Union Convention on Cyber Security and Personal Data Protection.* Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [Accessed 15 August 2018]

African Union Commission [AUC] (2015). *Roadmap 2016-2020*. Available at: http://www.peaceau.org/uploads/2015-en-apsa-roadmap-final.pdf [Accessed 18 August 2018]

African Union Commission [AUC] (2016). *Speech of H.E. Dr Elham M. Ibrahim, Commissioner for Infrastructure and Energy, AUC, at the Extraordinary Special Technical Committee Meeting on CCICT*, 14-16 September, Bamako, Mali. Available at: https://au.int/en/speeches/20160916-0 [Accessed 23 March 2019]

African Union Commission [AUC] (2017a). *Statute of the African Union Mechanism for Police Cooperation* (AFRIPOL). Available At: https://au.int/en/treaties/statute-african-union-mechanism-police-cooperation-afripol [Accessed 18 August 2018]
African Union Commission [AUC] (2017b). *African Union Specialized Technical Committee on Communication and Information Technologies (STC-CICT) 2nd Ordinary Session*, Addis Ababa, Ethiopia, 20-24 November. Available at: https://au.int/en/ccict2 [Accessed 15 August 2018]

African Union Commission [AUC] (2018a). *Declaration on Internet Governance and Development of Africa's Digital Economy*, Assembly/AU/Decl.3 (XXX). Available at: https://au.int/sites/default/files/decisions/33908-assembly_decisions_665_-_689_e.pdf [Accessed 15 March 2019]

African Union Commission [AUC] (2018b). *Workshop on Cyber strategies, Cyber legislation and National CERTs*. 23-27 July. Available at: https://au.int/en/cybersecurityworkshop [Accessed 23 March 2019]

African Union Commission [AUC] (2018c). *Call for Experts: African Union Cyber Security Expert Group.* Available at: https://au.int/en/announcements/20180920/call-experts-african-union-cyber-security-expert-group [Accessed 15 March 2019]

African Union Commission [AUC] (2019). *African Leaders Redefine the Future through Digital Transformation*, Press Release NXXX/2019. Available at: https://au.int/en/pressreleases/20190211/african-leaders-redefine-future-through-digital-transformation [Accessed 1 August 2019]

African Union Commission [AUC], Symantec (2016). *Cyber Crime and Cyber Security Trends in Africa*. Available at: https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa [Accessed 18 August 2018]

Amazouz, S (2018). African Union Convention on Cybersecurity and Personal Data Protection "Malabo Convention". African Cybercrime Forum, African Union Commission. Available at: https://au.int/sites/.../34851-wd-malabo_convention_-_african_cybercrime_forum.pdf [Accessed 15 March 2019]

Association of Southeast Asian Nations [ASEAN] Regional Forum (2015). *Work Plan on Security of and In the Use of Information and Communications Technologies*. Available at: http://aseanregionalforum.asean.org/librarycat/icts-security/ [Accessed 18 August 2018]

Barnes, S (2015). *How better connectivity can transform Africa's economies.* World Economic Forum (16 June). Available at: https://www.weforum.org/agenda/2015/06/how-better-connectivity-can-transform-africas-economies/ [Accessed 18 August 2018]

BBC News (2017). *Cyber-attack: WE and UK blame North Korea for WannaCry*. Available at: https://www.bbc.com/news/world-us-canada-42407488 [Accessed 15 March 2019]

BBC News (2018a). *UK and U.S. blame Russia for 'malicious' NotPetya cyber-attack.* Available at: https://www.bbc.com/news/uk-politics-43062113# [Accessed 20 May 2019]

BBC News (2018b). *Russia-Trump inquiry: Russians charged over US 2016 election tampering.* Available at https://www.bbc.com/news/world-us-canada-43092085 [Accessed 20 May 2019]

BBC News (2019). *Facebook bans "inauthentic" accounts targeting Africa.* Available at: https://www.bbc.com/news/business-48305032 [Accessed 20 May 2019]

Beaver, M (2016). *The United Nations and Cyberwarfare.* Global Risk Advisors blog, 28 September. Available at: https://globalriskadvisors.com/blog/united-nations-cyber-warfare/ [Accessed 18 August 2018]
Bedzigui, Y (2018). *Enhancing AU responses to instability: linking AGA and APSA.* Institute for Security Studies (ISS), Available at: https://issafrica.org/research/policy-brief/enhancing-au-responses-to-instability-linking-aga-and-apsa [Accessed 18 December 2018]

Bishumba, N (2017). Parliament passes Cyber Security Bill. *The New Times.* Available at: https://www.newtimes.co.rw/section/read/211223 [Accessed 18 August 2018]

Botswana Communication Regulatory Authority [BOCRA] (2014*). bw CIRT - Botswana Computer Incidence Response Team*. Available at: https://www.bocra.org.bw/bw-cirt [Accessed 18 August 2018]

Brown, D (2019). *UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online.* Association for Progressive communication [APC]. Available at: https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed [Accessed 1 March 2019]

Carnegie Mellon University (2019). *National Computer Security Incident Response Teams (CSIRTs).* Available at: https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/ [Accessed 20 May 2019]

CISOMAG (2019). *West African banks and financial firms suffer cyber-attacks: Symantec*, 18 January. Available at: https://www.cisomag.com/west-african-banks-and-financial-firms-suffer-cyber-attacks-symantec/ [Accessed 20 May 2019]

Clapper, J *et al* (2017). *Foreign cyber threats to the United States.* Joint statement for the record to the Senate Armed Services Committee, 5 January. Available at: https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2017/item/1614-joint-statement-for-the-record-on-foreign-cyber-threats-to-the-u-s-to-the- [Accessed 18 August 2018]

Collaboration on International ICT Policy for East and Southern Africa [CIPESA] (2017). *Calculating the Economic Impact of Internet disruptions in Sub Sahara Africa.* Available at: https://cipesa.org/2017/09/economic-impact-of-internet-disruptions-in-sub-saharan-africa/ [Accessed 18 August 2018]

Committee of Intelligence & Security Service of Africa [CISSA] (no date). *Homepage.* Available at: https://cissaau.org/ [Accessed 18 August 2018]

Committee of Intelligence & Security Service of Africa [CISSA] (2015). *Communique,* Workshop on Cyber Security CISSA/WS/18/4. Available at: https://docplayer.net/9330570-Cissa-cissa-workshop-on-cyber-security-07-11-november-2015-khartoum-sudan-cissa-ws-18-4-original-english-communique.html

Computer Emergency Response Team of Algeria [DZ-CERT] (2015). *Homepage.* Available at: http://cerist.dz/ [Accessed 18 August 2018]

Computer Emergency Response Team Cote d'Ivoire [CI CERT] (2009). *Homepage.* Available at: http://www.cicert.ci [Accessed 18 August 2018]

Computer Emergency Response Team of Egypt [EG-CERT] (2009). *Homepage.* Available at: http://egcert.eg/ [Accessed 18 August 2018]

Computer Emergency Response Team of Egypt [EG-CERT] (2017). *First ITU Regional Symposium & Cyber Drill for Africa and Arab Regions*. Available at: http://egcert.eg/first-itu-regional-symposium-cyber-drill-for-africa-and-arab-regions/ [Accessed 18 August 2018]

Computer Emergency Response Team of Ghana [ghCERT] (2014). *Homepage.* Available at: https://www.cert-gh.org/ [Accessed 18 August 2018]

Computer Emergency Response Team of Libya [LibyaCERT] (2013). *Homepage.* Available at: www.nissa.gov.ly [Accessed 22 August 2018]

Computer Emergency Response Team of Morocco [maCERT] (2011). *Homepage.* Available at: http://www.macert.ma/ [Accessed 22 August 2018]

Computer Emergency Response Team of Nigeria [ngCERT] (2015). *Homepage.* Available at: https://www.cert.gov.ng [Accessed 22 August 2018]

Computer Emergency Response Team of Sudan [CERTSudan] (2010). *Homepage.* Available at: http://www.cert.sd [Accessed 22 August 2018]

Computer Emergence Response Team of Tanzania [TZ-CERT] (2010). *Homepage.* Available at: https://www.tzcert.go.tz [Accessed 30 August 2018]

Computer Emergency Response Team of Tunisia [tunCert] (2004). *Homepage.* Available at: http://www.ansi.tn/ [Accessed 30 August 2018]

Computer Emergency Response Team of Uganda [ugCERT] (2011). *Homepage.* Available at: http://www.ug-cert.ug/ [Accessed 22 August 2018]

Computer Incident Response Team of Cameroun [cmCIRT] (2012). *Homepage.* Available at: https://www.cirt.cm/?language=en [Accessed 22 August 2018]

Computer Incident Response Team of Burkina Faso [CIRT-bf] (2012). *Homepage.* Available at: www.cirt.bf [Accessed 22 August 2018]

Computer Incident Response Centre of Mauritius [CERT-MU] (2008). *Homepage.* Available at: http://www.cert-mu.org.mu/ [Accessed 22 August 2018]

Computer Incident Response Team of Kenya [KE-CIRT/CC] (2012). *Homepage.* Available at: http://www.ke-cirt.go.ke [Accessed 22 August 2018]

Computer Incident Response Team of Zambia [zmCIRT] (2012). *Homepage.* Available at: http://www.cirt.zm [Accessed 22 August 2018]

Computer Security and Incident Response Team of Rwanda [Rw-CSIRT] (2014). *Homepage.* Available at: http://rw-csirt.rw/eng/about-us/v_and_m.php [Accessed 22 August 2018]

Computer Security Incident Response Team of South Africa [ECS-CSIRT] (2003). *Homepage.* Available at: http://www.e-comsec.com/ECSCSIRT/tabid/109/Default.aspx [Accessed 30 August 2018]

Computer Security Incident Response Team of South Africa, First National Bank [CSIRTFNB] (2009). *Homepage.* Available at: www.fnb.co.za/ [Accessed 30 August 2018]

Council of Europe [CoE] (2015). The state of cybercrime legislation in Africa. Available at: https://rm.coe.int/16806b8a79 [Accessed 30 August 2018]

Council of Europe [CoE] (2018). *Cabo Verde: Cybercrime policies/strategies.* Available at: https://www.coe.int/hy/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/cape-verde/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_v [Accessed 20 May 2019]

Council of Europe [CoE] (2019a). *Budapest Convention: Signature and ratification*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=jtWNtLty [Accessed 20 May 2019]

Council of Europe [CoE] (2019b). *CyberSouth*. Available at: https://www.coe.int/en/web/cybercrime/cybersouth [Accessed 20 May 2019]

Council of Europe [CoE] (2019c). *Global Action on Cybercrime Extended (GLACY)+*. Available at: https://www.coe.int/en/web/cybercrime/glacyplus [Accessed 20 May 2019]

Council of Europe [CoE] (2019d). *Global Project Cybercrime@Octopus*. Available at: https://www.coe.int/en/web/cybercrime/cybercrime-octopus [Accessed 20 May 2019]

Council of Europe [CoE] (2019e). *GLACY+: Burkina Faso prepares law on Cybercrime.* Available at: https://www.coe.int/en/web/cybercrime/-/glacy-burkina-faso-prepares-law-on-cybercrime [Accessed 20 May 2019]

Council of Europe [CoE], Economic Community for Africa [ECOWAS] (2017) *ECOWAS and the Council of Europe join forces to help West African countries in the fight against cybercrime.* Available at: https://rm.coe.int/a/16807486c8 [Accessed 30 August 2018]

Council of the European Union (2017a). *Cyber attacks: EU ready to respond with a range of measures, including sanctions.* Available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ [Accessed 30 August 2018]

Council of the European Union (2017b). *5th African Union - EU Summit, 29-30/11/2017*. Available at: https://www.consilium.europa.eu/en/meetings/international-summit/2017/11/29-30/ [Accessed 2 April 2019]

Council of the European Union (2017c). *Investing in Youth for Accelerated Inclusive Growth and Sustainable Development*, Declaration AU-EU/Decl.1 V. Available at: https://www.consilium.europa.eu/en/meetings/international-summit/2017/11/29-30/ [Accessed 20 May 2019]

Cyber Emergency Readiness and Response Team of Ethiopia [Ethio-CERT] (2012). *Homepage.* Available at: http://ethiocert.insa.gov.et [Accessed 2 April 2019]
Dahir, A.L. (2012). Cybercrime is costing Africa's businesses billions. *Quartz Africa*, 12 June. Available at: https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/ [Accessed 15 March 2019]

Daka, T (2018). ICT boosts GDP by 12% in second quarter. *The Guardian*, 6 November. Available at: https://guardian.ng/news/ict-boosts-gdp-by-12-in-second-quarter/ [Accessed 23 March 2019]

DiploFoundation (2017). *Offensive and Defensive Cyber-Capabilities Map*. Available at: https://public.tableau.com/profile/publish/Offensivecyberdefence/Story2#!/publish-confirm [Accessed 2 April 2019]

Ebert, H.; Maurer, T. (2013). Cyberspace and the Rise of the BRICS. Columbia SIPA, Jour*nal of International Affairs*, 12 October. Available at: https://jia.sipa.columbia.edu/online-articles/cyberspace-and-rise-brics [Accessed 5 April 2019]

Economic Development Board Mauritius (2019). *Transitioning towards a Digital Industry*. Available at: http://www.edbmauritius.org/opportunities/ict/ [Accessed 23 March 2019]
Essoungou, A (2011). Africa's rising information economy. *Africa Renewal*. Available at: https://www.un.org/africarenewal/magazine/april-2011/africas-rising-information-economy[Accessed 23 March 2019]

European Commission (no date). *Data protection in the EU.* Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [Accessed 2 April 2019]

European Commission (2019a). *EU-AU Digital Economy Task Force.* Available at https://ec.europa.eu/digital-single-market/en/africa#title2 [Accessed 20 March 2019]
European Commission (2019b). *Operational Guidance for the EU's international cooperation on cyber capacity building.* Available at: https://ec.europa.eu/europeaid/operational-guidance-eus-international-cooperation-cyber-capacity-building_en [Accessed 2 April 2019]
European Network and Information Security Agency [ENISA] (2012). *National Cyber Security Strategies.* Available at: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper [Accessed 20 March 2019]

FIRST (2019). *FIRST Teams.* Available at: https://www.first.org/members/teams [Accessed 2 April 2019]

Geneva Internet Platform [GIP] Digital Watch observatory (no date). *Trends in Cyber-armament.* Available at: https://dig.watch/processes/ungge#Armament (Accessed 17 August 2018)

Ghernaouti-Hélie, S (2010). We need a Cyberspace Treaty Regional and bilateral agreements are not enough. *Inter Media* 38(2). Available at: https://serval.unil.ch/resource/serval:BIB_5C4235C9986E.P001/REF [Accessed 2 April 2019]

Global Conference on Cyberspace (2015). *Chair's Statement*. Available at: https://www.mofa.go.jp/mofaj/files/000076862.pdf [Accessed 2 April 2019]

Global Commission on the Stability of Cyberspace [GCSC] (2017). *Briefings and Memos from the Research Advisory Group*. Available at:

https://cyberstability.org/research/briefings-and-memos-of-the-research-advisory-group/ [Accessed 2 April 2019]

Global Forum on Cyber Expertise [GFCE] (no date). *Homepage.* Available at: https://www.thegfce.com [Accessed 2 April 2019]

Global Forum on Cyber Expertise [GFCE] (no date). *About the GFCE.* Available at: https://www.thegfce.com/about [Accessed 18 August 2018]

Global Forum on Cyber Expertise [GFCE] (2017). *Delhi Communiqué*. Available at: https://www.thegfce.com/delhi-communique [Accessed 18 August 2018]

Government of Algeria (2018). *Protection of Individual in Processing Personal Data Law*, N° 18-07, Official Gazette No. 34. Available at: https://www.joradp.dz/HFR/Index.htm [Accessed 1 February 2019]

Government of Angola (2011). *Personal Data Protection Law*, No. 22/11). Available at: https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf [Accessed 1 February 2019]

Government of Botswana (2018). *Cybercrime and Computer Related Crimes Act 2018*. Available at: https://www.bocra.org.bw/cybercrime-and-computer-related-crimes-act-2018 [Accessed 18 August 2018]

Government of Burkina Faso (2004). *Law on the Protection of Personal Data*, No. 010-2004AN. Available at: https://www.afapdp.org/wp-content/uploads/2012/01/Burkina-Faso-Loi-portant-protection-des-donn%c3%a9es-%c3%a0-caract%c3%a8re-personnel-20042.pdf [Accessed 1 February 2019]

Government of Cabo Verde (no date). *Cyber Strategy*. Available at: https://governo.cv/index.php/destaques/6422-conselho-de-ministros-aprova-estrategia-nacional-para-a-ciberseguranca [Accessed 1 February 2019]

Government of Cabo Verde (2013). *National Commission of Data Protection (CNPD),* Law 42/VIII/2013. Available at: www.cnpd.cv/leis/CNPD%20Law%2042.pdf [Accessed 1 February 2019]

Government of Cabo Verde (2016). *Conselho de Ministros aprova Estratégia Nacional para a Cibersegurança*. Available at: https://www.governo.cv/conselho-de-ministros-aprova-estrategia-nacional-para-a-ciberseguranca/ [Accessed 15 March 2019]

Government of Chad (2015). *Protection of Personal Data (Act 007/PR/2015) and Law N° 006/PR/2015 on the establishment of National Agency for Computer Security and*

Electronic Certification. Available at: https://juriafrique.com/boutique/tchad-jo-15-au-28-fevrier-2015/ [Accessed 1 February 2019]

Government of Cote D'Ivoire (2013). *Law on the Protection of Personal Data*, No. 2013-450. Available at: http://www.artci.ci/images/stories/pdf-english/lois_english/loi_2013_450_english.pdf [Accessed 1 February 2019]

Government of Cuba (2017). *UNGA: Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security.* Available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information [Accessed 1 February 2019]

Government of Egypt (no date). *National Cybersecurity Strategy 2017- 2021.* Available at: http://www.mcit.gov.eg/Publication/Publication_Summary/6132/ [Accessed 18 August 2018]

Government of France (2018). *Paris call for Digital trust in cyberspace*. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in [Accessed 5 April 2019]

Government of Gabon (2011). *Law on the Protection of Personal Data*, No. 001/2011. Available at: https://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%c3%a0-la-protection-des-donn%c3%a9es-personnelles-du-4-mai-20112.pdf [Accessed 5 April 2019]

Government of Germany (2017). *G20 Digital Economy Ministerial Declaration.* Available at: https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.html [Accessed 23 March 2019]

Government of Ghana (2012). *Data Protection Act.* Available at: https://www.dataprotection.org.gh/data-protection-act [Accessed 5 April 2019]

Government of Ghana (2015). *Ghana National Cyber Security Policy & Strategy*. Available at: https://www.cert-gh.org/guidelines/national-cyber-security-policy-strategy-document-2/ [Accessed 5 April 2019]

Government of Ghana (2017). *National Cyber Security Centre to Be Established.* Available at: http://www.ghana.gov.gh/index.php/news/4103-national-cyber-security-centre-to-be-established [Accessed 5 April 2019]

Government of India (2011). *India's proposal for a United Nations Committee for Internet-Related Policies (CIRP).* Available at: https://internetdemocracy.in/wp-

content/uploads/2014/07/India-UN-CIRP-Proposal-at-UNGA-2011.pdf [Accessed 5 April 2019]

Government of Kenya (2014). *National Cyber Security Strategy.* Available at: http://icta.go.ke/national-cyber-security-strategy/ [Accessed 20 March 2019]

Government of Lesotho (2012). *Data Protection Act*, No. 5. Available at: https://www.imf.org/external/np/loi/2012/lso/111212.pdf [Accessed 5 April 2019]

Government of Mali (2013). *Personal Data Protection Authority*. Available at: https://apdp.ml/ [Accessed 5 April 2019]

Government of Mauritania (2018). *National Strategy on Cybersecurity (2017-2022) of Mauritania.* African Union Commission [AUC], Addis Ababa, 23-27 July. Available at: https://au.int/en/cybersecurityworkshop [Accessed 5 April 2019]

Government of Mauritius (no date). *Legislations: Acts and Regulations.* Available at: http://mtci.govmu.org/English/Rules-Regulations-Policies/Pages/default.aspx [Accessed 25 February 2019]

Government of Mauritius (2004). *Data Protection Act*, Act 13 of 2004. Available at: http://www.ncb.mu/English/Legislations/Pages/Data-Protection-Act-2004.aspx

Government of Mauritius (2014). *National Cybersecurity Policy and Strategy (2014 – 2019)*. Available at http://mtci.govmu.org/English/Pages/default.aspx [Accessed 25 February 2019]

Government of Mauritius (2017). *Data Protection Act*, No. 20 of 2017. Available at: http://dataprotection.govmu.org/English/Legislation/Pages/Data-Protection-Act-2017-.aspx [Accessed 25 February 2019]

Government of Mauritius (2017). *Cybercrime strategy (2017-2019)*. Available at: http://mtci.govmu.org/English/Pages/Policies.aspx [Accessed 25 February 2019]

Government of Mauritius (2018). *Regional Centre of excellence on cybersecurity and cybercrime being set up, states Minister Sawmynaden.* Available at: http://mtci.govmu.org/English/Pages/default.aspx [Accessed 25 February 2019]

Government of Morocco (2009). *Law on the protection of individuals with regard to processing personal data*, No. 1-09-15 du 22 safar 1430. Available at: https://anrt.ma/content/dahir-ndeg-1-09-15-du-22-safar-1430-18-fevrier-2009 [Accessed 25 February 2019]

Government of Morocco (2012). *National Cyber Security Strategy.* Available at: https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf [Accessed 25 March 2019]

Government of Nigeria (2014). *National Cybersecurity Strategy.* Available at: https://www.cert.gov.ng/resources [Accessed 15 March 2019]

Government of Rwanda (2015a). *National Cybersecurity Policy.* Available at: https://minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf [Accessed 25 February 2019]

Government of Rwanda (2015b). *National Cybersecurity Strategic Plan*. Available at: https://minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/NCSP_Implementation_Plan.pdf [Accessed 25 February 2019]

Government of Rwanda (2017a). *ICT sector strategic plan (2018-2024): Towards digital enabled economy*. Available at: http://minict.gov.rw/policies-publications/strategy/ [Accessed 25 February 2019]

Government of Rwanda (2017b). *Law on establishing the National Cyber Security Authority and determining its Mission, Organisation and Functioning*, No. 26/2017. Available at: http://minict.gov.rw/policies-publications/policies-and-regulations/ict-laws/ [Accessed 25 February 2019]

Government of Rwanda (2018). *Law on Prevention and Punishment of Cybercrimes*, No 60/2018. Available at: http://minict.gov.rw/policies-publications/policies-and-regulations/ict-laws/ [Accessed 25 February 2019]

Government of Senegal (2008). *Protection of Personal Data Law*, Act No. 2008-12. Available at: http://www.jo.gouv.sn/spip.php?page=imprimer&id_article=7207 [Accessed 20 February 2019]

Government of Senegal (2017). *Senegalese National Cybersecurity Strategy (SNC 2022).* Available at: http://www.numerique.gouv.sn/mediatheque/documentation/strat%C3%A9gie-nationale-de-cybers%C3%A9curit%C3%A9-snc2022 [Accessed 25 March 2019]

Government of Seychelles (2003). *Data Protection Act.* Available at: https://seylii.org/sc/legislation/act/2002/9 [Accessed 20 February 2019]

Government of South Africa (2013). *Protection of Personal Information Act*, Government Gazette No. 37067. Available at: https://www.greengazette.co.za/pages/national-gazette-37067-of-26-november-2013-vol-581_20131126-GGN-37067-00140 [Accessed 20 February 2019]

Government of South Africa (2015a). *Department of Defence: Annual Report (2014-2015).* Available at: https://www.gov.za/documents/department-defence-annual-report-20142015-7-oct-2015-0000 [Accessed 20 February 2019]

Government of South Africa (2015b). *National Cybersecurity Policy Framework,* Gazette No. 39475. Available at: https://www.greengazette.co.za/departments/security [Accessed 7 February 2019]

Government of South Africa (2017). *Department of Telecommunications and Postal Services: Cybersecurity*. Parliamentary Report. Available at: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/170822Cybersecurity.pdf [Accessed 20 February 2019]

Government of South Africa (2018). *President's Speech during ITU Telecom World 2019, 10 September*. *Available* at https://telecomworld.itu.int/speeches/h-e-matamela-cyril-ramaphosa-president-south-africa/ [Accessed 20 February 2019]

Government of Tunisia (2002). *National Agency for Computer Security*. Available at: https://www.ansi.tn/fr/pages/documentation/publications.html [Accessed 20 February 2019]

Government of Tunisia (2004). Per*sonal Data Protection Law*, No 2004-63. Available at: http://www.legislation.tn/en/detailtexte/Loi-num-2004-63-du----jort-2004-061__20040610006 31?shorten=QliE [Accessed 20 February 2019]

Government of Uganda (2014). *National Information Security Framework (NISF)*. Available at: https://www.nita.go.ug/publication/national-infomation-security-framework [Accessed 25 March 2019]

Government of Uganda (2016). *Cyber Security Capacity Review of the Republic of Uganda*. Available at: https://www.nita.go.ug/publication/cyber-security-capacity-review-republic-uganda [Accessed 20 February 2019]

Government of the UK (2011). *Chair's statement*, London Conference on Cyberspace, 2 November. Available at: https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement [Accessed 20 February 2019]

Government of the USA (2008). *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23)*, 8 January 2008. Available at: https://www.hsdl.org/?view&did=815341 [Accessed 5 March 2019]

Government of the USA (2017). Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of

Information and Telecommunications in the Context of International Security. Available at: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm [Accessed 18 August 2018]

Graham, G (2015). Global Tables of Data Privacy Laws and Bills. *Privacy Laws & Business International Report,* 133: 18-28. Available at: www.austlii.edu.au/au/journals/UNSWLRS/2015/28.pdf [Accessed 5 March 2019]

GSMA (2017). *The Mobile Economy Sub-Saharan Africa in 2017.* Available at: https://www.gsma.com/subsaharanafrica/resources/the-mobile-economy-sub-saharan-africa-2017 [Accessed 5 March 2019]

GSMA (2018). *The Mobile Economy Sub-Saharan Africa in 2018.* Available at: https://www.gsma.com/r/mobileeconomy/sub-saharan-africa/ [Accessed 1 November 2018]

Hathaway, M (2018). Managing National Cyber Risks. Organisation of American States [OAS], White paper series (2). Available at: https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf [Accessed 1 November 2018]

Homri, A (2018). *Cyber -Strategy, Cyber-legislation and the establishment of CERTs for Member States of the African Union. Experience from Tunisia.* African Union Commission [AUC], Addis Ababa, 23-27 July. Available at: https://au.int/en/cybersecurityworkshop [Accessed 1 November 2018]

Hounkpe, J.C. (2011). *Legal framework for the protection of personal data in Republic of Benin.* Available at: http://works.bepress.com/julien-coomlan-hounkpe/18/ http://www.cerist.dz/index.php/en/rechercheetdevelop-en/147-projets-de-recherche-innovants/537-dz-cert-algerian-computer-emergency-response-team [Accessed 15 March 2019]

ICT4Peace Foundation (2015). *The Government of Kenya and ICT4Peace Foundation co-organize the first Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace.* Available at: https://ict4peace.org/activities/the-government-of-kenya-and-ict4peace-foundation-co-organize-the-first-regional-training-workshop-in-africa-on-international-security-and-diplomacy-in-cyberspace/ [Accessed 1 November 2018]

International Telecommunication Union [ITU] (no date). *Computer Incident Response Teams (CIRT) program*. Available At: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx [Accessed 18 August 2018]

International Telecommunication Union [ITU] (2005). *World Summit on Information Society: Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6. Available

at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2007). *Global Cybersecurity Agenda (GCA).* Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [Accessed 5 April 2019]

International Telecommunication Union [ITU] (2008a). *Definition of Cybersecurity.* Study Group 17 (ITU-T X.1205) Available at: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en [Accessed 18 August 2018]

International Telecommunication Union [ITU] (2008b). *Support for harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA).* Available at: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2012). *Statement by the Secretary General during the World Conference on International Communications (WCIT-12),* 13 December. Available at: https://www.itu.int/en/wcit-12/Pages/statement-toure.aspx [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2017). *Global Cyber Security Index 2017.* Available at: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2018a). *New ITU statistics show more than half the world is now using the Internet.* Available at: https://news.itu.int/itu-statistics-leaving-no-one-offline/ [Accessed 5 March 2019]

International Telecommunication Union [ITU] (2018b). *The State of Broadband 2018: Broadband catalyzing sustainable development*. Available at: https://www.itu.int/pub/S-POL-BROADBAND.19 [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2018c). *Measuring the Information Society Report.* Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx [Accessed 1 November 2018]

International Telecommunication Union [ITU] (2019). *National CIRT: CIRT assessment*. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx [Accessed 15 March 2019]

Internet Governance Forum [IGF] (no date). *Africa National IGFs*. Available at https://www.intgovforum.org/multilingual/content/african-regional-group [Accessed 15 August 2018]

Internet Society [ISOC] (2017). *Internet Infrastructure Security Guidelines for Africa.* Available at: https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/ [Accessed 23 March 2019]

Internet Society [ISOC] (2018), *Personal Data Protection Guidelines for Africa*. Available at: https://www.internetsociety.org/resources/doc/2018/personal-data-protection-guidelines-for-africa/ [Accessed 23 March 2019]

Internet World Stats (2019). *World Internet Usage and Population Statistics*. Available at: https://www.internetworldstats.com/stats.htm [Accessed 1 April 2019]

Kende M (2017). *Promoting the African Internet Economy.* Internet Society [ISOC]. Available at: https://www.internetsociety.org/resources/doc/2017/africa-internet-economy/ [Accessed 1 April 2019]

Kenya Engineer (2019). *ICT to Drive Kenya's 2022 GDP Growth Ambition*, 21 February. Available at: https://www.kenyaengineer.co.ke/ict-to-drive-kenyas-2022-gdp-growth-ambition/ [Accessed 23 March 2019]

Koh D (2017). Singapore's approach to international cyber cooperation. Global Cyber Expertise Magazine [GFCE] (3) Available at: https://www.thegfce.com/about/news/2017/05/31/robust-and-coordinated-capacity-building-for-a-secure-and-resilient-cyberspace [Accessed 1 April 2019]

Kurbalija, J (2016) *An Introduction to Internet Governance*, 7th edition. Malta: DiploFoundation. Available at: https://www.diplomacy.edu/resources/books/introduction-internet-governance [Accessed 16 March 2019]

Kurbalija, J (2017). *Digital politics in 2017: Unsettled weather, stormy at times, with sunny spells.* DiploFoundation. Available at: https://www.diplomacy.edu/blog/digital-politics-2017-unsettled-weather-stormy-times-sunny-spells [Accessed 16 March 2019]

Kurbalija, J (2018). *A tipping point for the Internet: Predictions for 2018.* DiploFoundation. Available at: https://www.diplomacy.edu/policybriefs [Accessed 10 March 2019]

Lavion, D (2018). *Pulling fraud out of the shadows*. Global Economic Crime and Fraud Survey 2018, PwC. Available at: www.pwc.com/fraudsurvey [Accessed 1 April 2019]

Lewis, J.A. (2013). *The Cyber Index: International Security Trends and Realities*. Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-index-international-security-trends-and-realities [Accessed 1 April 2019]

Lindstrom, G (2012). *Meeting the Cybersecurity Challenge*. Geneva Papers, Research Series 7. Geneva Centre for Security Policy [GCSP]. Available at: https://www.files.ethz.ch/isn/147788/7-2012.pdf [Accessed 1 April 2019]

Loghmari, N (2016). *Tunisian experience in the National Cyberspace Security* [presentation]. Presented during the Joint ITU-ATU Workshop on Cybersecurity Strategy in African Countries, ITU, 24-26 July, Sudan. Available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S7P2_Nadhir_L.pdf [Accessed 1 April 2019]

Mabika, V (2017). *WannaCry Ransomware Attacks: A Test of Africa's Cybersecurity Preparedness*. Available at: https://www.internetsociety.org/blog/2017/05/wannacry-ransomware-attacks-a-test-of-africas-cybersecurity-preparedness/ [Accessed 15 March 2019]

Madowo, L (2019). Is Facebook undermining democracy in Africa? *BBC News*, 24 May. Available At: https://www.bbc.com/news/world-africa-48349671 [Accessed 1 April 2019]

Maurer, T (2011). *Cyber norm emergence at the United Nations. An Analysis of the Activities at the UN Regarding Cyber-security*. Available at: https://www.belfercenter.org/sites/default/.../maurer-cyber-norm-dp-2011-11-final.pdf [Accessed 20 March 2019]

McKinsey Global Institute (2014). *Lions go digital: The Internet's transformative potential in Africa*. Available at: https://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa [Accessed 1 April 2019]

Metcalf, J (2018). Facebook may stop the data leaks, but it's too late: Cambridge Analytica's models live on. *MIT Technology Review*, 9 April. Available at: https://www.technologyreview.com/s/610801/facebook-may-stop-the-data-leaks-but-its-too-late-cambridge-analyticas-models-live-on/ [Accessed 8 March 2019]

Meyer, P (2018). *Global Cyber Security Norms: A Proliferation Problem?* ICT for Peace Foundation. Available at: https://ict4peace.org/wp-content/uploads/2018/12/Cyber-SecNormsProlifICT4PNov2018.pdf [Accessed 1 April 2019]

Muchanga, A (2019). *The Entry into Force of the Agreement Establishing the African Continental Free Trade Area (AfCFTA) and its Implementation*, 12 January, Addis Ababa, Ethiopia. Available at: https://au.int/en/pressreleases/20190112/commissioner-muchanga-2nd-stc-trade-industry-and-mineral-resources-%E2%80%9Cwe-now [Accessed 1 April 2019]

News 24 (2019). *Explainer: 2019 a busy year for African internet shutdowns.* Available at: https://www.news24.com/Africa/News/explainer-2019-a-busy-year-for-african-internet-shutdowns-20190121 [Accessed 20 March 2019]

Nyabola, N (2018). Politics in the digital age: Cambridge Analytica in Kenya. *Aljazeera*, 22 March. Available at: https://www.aljazeera.com/indepth/opinion/politics-digital-age-cambridge-analytica-kenya-180322123648852.html [Accessed 1 April 2019]

Ogutu, J (2015). How ICT drives Kenya's economic growth. *Standard Digital*, 18 May. Available at: https://www.standardmedia.co.ke/article/2000162611/how-ict-drives-kenya-s-economic-growth [Accessed 1 April 2019]

Organisation for Economic Co-operation and Development [OECD] (2012). *Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy.* Digital Economy Papers, 211. Available at: https://read.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en#.WhGLVTdRUb4#page1 [Accessed 1 April 2019]

Organisation of American States [OAS] (no date). *Confidence Building Measures in Cyberspace.* Available at: https://www.oas.org/en/sms/cicte/Documents/2016/.../JAMES%20LEWIS%20CSIS.pd... [Accessed 1 April 2019]

Organization for Security and Co-operation in Europe [OSCE] (2013). *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict stemming from the Use of Information and Communication Technologies*, Permanent Council, Decision No. 1106. Available at: https://www.osce.org/pc/109168 [Accessed 1 April 2019]

Organization for Security and Co-operation in Europe [OSCE] (2016a). *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, Permanent Council, Decision No. 1202. Available at: https://www.osce.org/pc/227281 [Accessed 1 April 2019]

Organization for Security and Co-operation in Europe [OSCE] (2016b). *OSCE participating States, in landmark decision, agree to expand list of measures to reduce risk of tensions arising from cyber activities*. Available at: http://www.osce.org/cio/226656 [Accessed 1 April 2019]

Orji, U.J. (2015). *Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?* Prepared for the 2015 7th International Conference on Cyber Conflict, NATO CCD COE. Available at:

https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf [Accessed 9 March 2019]

Pawlak P (2016). Confidence-Building Measures in Cyberspace: Current Debates and Trends, in Osula A.M. *et al.* (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*. NATO Cooperative Cyber Defence Centre of Excellence Publications, Tallinn, pp.129-153. [Accessed 1 April 2019]

Privacy International [PI] (2017). *New Documents Reveal Kenya's Worrying Attempts to Monitor the Internet*, 5 July. Available at: https://privacyinternational.org/feature/709/new-documents-reveal-kenyas-worrying-attempts-monitor-internet [Accessed 1 April 2019]

Radunovic, V (2017a). *Toward a Secure Cyberspace via Regional Co-operation.* DiploFoundation / Geneva Internet Platform. Available at: https://www.diplomacy.edu/resources/general/towards-secure-cyberspace-regional-co-operation [Accessed 20 March 2019]

Radunovic, V (2017b), *Cyber Armament: A growing trend (Part I)*. DiploFoundation. Available at https://www.diplomacy.edu/blog/cyber-armament-growing-trend-part-i [Accessed 18 March 2018]

Radunovic, V (2018). *At the table with the Paris Call for Trust and Security in Cyberspace*. DiploFoundation. Available at: https://www.diplomacy.edu/blog/table-paris-call-trust-and-security-cyberspace [Accessed 1 April 2019]

Rich, C (2017). A Look at New Trends in 2017: Privacy Laws in Africa and the Near East. *Bloomberg Law, Privacy and Security Law Reports*. Available at: https://media2.mofo.com/documents/170911-privacy-africa.pdf [Accessed 1 April 2019]

Richards, C (2019). *Digital Transformation in 2019 = Artificial Intelligence + Big Data + IoT*. Open Access Government. Available at: https://www.openaccessgovernment.org/digital-artificial-intelligence/56564/ [Accessed 5 April 2019]

Rõigas, H (2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* NATO Cooperative Cyber Defence Center of Excellence [CCDCOE]. Available at: https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html [Accessed 1 April 2019]

Russian News Agency (2018). *Russia to propose draft cybersecurity convention to UN General Assembly.* Available at: http://tass.com/politics/1011749 [Accessed 5 April 2019]

Segal, A; Waxman, M (2011). Why a cybersecurity treaty is a pipe dream. *CNN*, 27 October. Available at: http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/ [Accessed 1 April 2019]

Serianu (2017). *Africa Cybersecurity Report 2017: Demystifying Africa Cyber security line.* Available at: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf [Accessed 15 March 2019]

Smart Africa (2015). *Strategic Vision.* Available at: https://smartafrica.org/strategic-vision/ [Accessed 1 April 2019]

South African National Cybersecurity Hub (2015). *Homepage.* Available at: https://www.cybersecurityhub.gov.za [Accessed 20 March 2019]
Southern African Development Community [SADC] (2018) *Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill*. Available: https://www.sadc.int/news-events/news/sadc-convenes-cyber-security-workshop-and-sadc-regional-cyber-drill/ [Accessed 20 March 2019]

Stadnik, I (2019). *Discussing state behaviour in cyberspace: What should we expect?* DiploFoundation. Available at: https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect [Accessed 1 April 2019]

Subero, D (2018). CSIRTAmericas.org: Strengthening Incident Response Capabilities in the Americas. *Global Cyber Expertise Magazine*, 5. Available at: http://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/overlay/strengthening-incident-response-capabilities-in-the-americas/ [Accessed 1 April 2019]

Symantec (2016). *Cybercrime & Cybersecurity trends in Africa.* Available at: https://www.symantec.com/theme/cyber-security-trends-africa [Accessed 20 March 2019]

Tamarkin, E (2015). *The AU's cybercrime response: A positive start, but substantial challenges ahead.* Institute for Security Studies [ISS] 20 January. Available at: https://issafrica.org/research/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead [Accessed 18 August 2018]

Technomag (2018). *African General Assembly of the African Police Organization set up Cybercrime Unit.* Available at: https://www.technomag.co.zw/2018/10/18/african-

general-assembly-of-the-african-police-organization-set-up-cybercrime-unit/ [Accessed 1 April 2019]

Tikk, E (2018). *2018: The year that cyber peace became non-binding*. ICT4Peace Foundation. Available at: https://mailchi.mp/ict4peace/sanjana-hattotuwa-of-ict4peace-at-technonomy-2018-can-facebook-recover-2662409?e=030015c743 [Accessed 1 April 2019]

Tikk, E; Kerttunen, M (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. Cyber Policy Institute [CPI]. Available at: http://cpi.ee/activity/publications/ [Accessed 1 April 2019]

Touré H.I *et al.* (2011). *The Quest for Cyber peace*. ITU and World Federation of Scientists. Available at: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf [Accessed 1 April 2019]

United Nations Trade and Development [UNCTAD] (2015). *Review of e-commerce legislation harmonization in the Economic Community of West African States*. Available at: https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1410 [Accessed 1 April 2019]

United Nations Conference on Trade and Development [UNCTAD] (2017). *Implementing World Summit on the Information Society outcomes of 2016*. Commission on Science and Technology for Development [CSTD], E/CN.16/2017/CRP.2. Available at: https://unctad.org/meetings/en/SessionalDocuments/ecn162017crp2_en.pdf [Accessed 5 April 2019]

United Nations Department of Economic and Social Affairs [UNDESA] (2018a). *Progress in Digital Government Transformation: The 2018 UN E-Government Survey*. Available at: http://publicadministration.un.org/en/news-and-events/calendar/ModuleID/1146/ItemID/2999/mctl/EventDetails [Accessed 1 April 2019]

United Nations Department of Economic and Social Affairs [UNDESA] (2018b). *E-Government Survey Launch*, speech by Under-Secretary-General. Available at: https://www.un.org/development/desa/statements/mr-liu/2018/07/2018-e-govt-survey-launch.html [Accessed 1 April 2019]

United Nations General Assembly [UNGA] (1948). *Universal Declaration of Human Rights*, A/RES/3/217A. Available at: http://www.un.org/en/universal-declaration-human-rights/ [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (1966). *International Covenant on Civil and Political Rights*, resolution 2200A (XXI). Available at:

https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (1998). *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/53/70 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2000). *Combating the criminal misuse of information technologies*, A/RES/ 55/63. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/55/63 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2001). *Combating the criminal misuse of information technologies*, A/RES/ 56/121. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/56/121 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2002). *Creation of a global culture of cybersecurity*, A/RES/57/239. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/57/239 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2003a). *Developments in the field of information and telecommunications in the context of international security*, A/RES/ 58/32. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/58/32 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2003b). *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*, A/RES/ 58/199. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/58/199 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2005*). Report of the Secretary-General,* A/60/202. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/60/202 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2009). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, A/RES/64 /211. Available at:

http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/64/211 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2010). *Note by the Secretary-General*, A/65/201. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/65/201 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/66/359. Available at: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2013). *Note by the Secretary-General*, A/68/98. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/68/98 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2013). *The right to privacy in the digital age*, A/68/167. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167&Lang=E [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2014). *The right to privacy in the digital age*, A/69/166. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/166 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2015a). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, A/69/723. Available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2015b). *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/70/237. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/70/237 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2015c). *Note by the Secretary-General*, A/70/174. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at: http://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/174 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2018a). *Developments in the field of information and telecommunications in the context of international security*, A/RES/73/27. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2018b). *Advancing responsible State behaviour in cyberspace in the context of international security*, A/RES/73/266. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266 [Accessed 20 March 2019]

United Nations General Assembly [UNGA] (2018c). *Official record of the 45th plenary meeting 5 December*, A/73/PV.45. Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/73/PV.45 [Accessed 1 April 2019]

United Nations General Assembly [UNGA] (2018d). *Official record of the 65th plenary meeting 21 December*, A/73/PV.65. Available at: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/73/PV.65 [Accessed 1 April 2019]

United Nations Human Rights Council [UNHRC] (2014). *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/26/13. Available at: https://undocs.org/en/A/HRC/RES/26/13 [Accessed 5 April 2019]

United Nations Human Rights Council [UNHRC] (2015). *The right to privacy in the digital age*, A/HRC/28/L.27. Available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/28/L.27 [Accessed 5 April 2019]

United Nations Institute for Disarmament Research [UNIDIR] (no date). *Cabo Verde.* Cyber Policy Portal. Available at: https://cyberpolicyportal.org/en/states/caboverde [Accessed 1 April 2019]

United Nations Institute for Disarmament Research [UNIDIR] (2011). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization.* Available at https://css.ethz.ch/en/services/digital-library/publications/publication.html/134215 [Accessed 1 April 2019]

United Nations Office for Disarmament Affairs [UNODA] (2019). *Developments in the field of information and telecommunications in the context of international security*. Available at: https://www.un.org/disarmament/topics/informationsecurity/ [Accessed 5 April 2019]
Van Vuuren J, *et al* (2013). *Development of a South African Cybersecurity Policy Implementation Framework* [conference paper]. International Conference on Cyber Security and Warfare (ICCWS), 2013. Available at: https://www.researchgate.net/publication/266145673_Development_of_a_South_African_Cybersecurity_Policy_Implementation_Framework [Accessed 1 April 2019]

Volz, D (2017). *U.S. blames North Korea for 'WannaCry' cyber-attack.* Reuters. Available at: https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q [accessed 18 August 2018]

Wladawsky-Berger I (2017). GDP Doesn't Work In A Digital Economy. *The Wall Street Journal*, 3 November. Available at: https://blogs.wsj.com/cio/2017/11/03/gdp-doesnt-work-in-a-digital-economy/ [Accessed 1 April 2019]

Yankson, H (2018). *Cyber Security Development: Ghana Perspective.* Available at: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-02.pres_cyber_security_development_ghana_in_perspective_h.yankson.pdf [Accessed 1 April 2019]