IPSS

Vol 16 – 7 | Oct. 2022

Policy Brief

THE MALABO CONVENTION AND AFRICA'S CYBER POSTURE

Jesutimilehin O. Akamo

CONTENTS

EXECUTIVE SUMMARY

The Malabo Convention is an African Union (AU) legislation aimed at establishing a normative and legal foundation upon which Africa's cyber posture should stand. Unfortunately, the Convention faces two significant gaps: Limited scope, and the poor level of political will and commitment of AU member states towards the Convention. For the former, the scope needs to be more holistic to capture all forms through which AU member states may experience cyberattacks. These forms include cybercrime, cyberterrorism, hacktivism, cyberespionage, and cyberconflict/warfare.[1] While the Convention demonstrates the intent of the AU to respond to emerging challenges, the scope of the Convention needs to be more holistic and therefore requires a revision to capture the full range of cyber risks. However, if political commitment to the Malabo Convention remains where it is, cybersecurity development at policy and programmatic levels will be stalled to the detriment of African countries. The Malabo Convention and its gaps are at the governance-peace and security nexus, which constitute the essence of the AGA-APSA synergy. This piece concludes by arguing the instrumentality of the synergy between African Governance Architecture (AGA) and the African Peace and Security Architecture (APSA), also known as the AGA-APSA synergy to address the challenges impeding the success of the Malabo Convention.

KEY POINTS

- The cybersecurity challenges of one African country cannot be adequately analysed or resolved independently of continental realities and vice versa. On this premise, the African Union recognises the need for a continental framework and multilateral approach to Africa's cyber posture which birthed the Malabo Convention.
- Contemporary realities show that the Convention is yet to come into force as it struggles with political will coupled with its inability to address most key emerging issues.
- Although different manifestation of cyberattacks employ similar tools, their (political) objectives, type of solution required (political, technical or both), and contextual differences - in terms of who the aggressor is/sponsor of the attack (state or non-state) - creates a situation where the peculiarities related to each manifestation of cyberattacks have to be accounted for.
- The Malabo Convention and its gaps (limited scope and political will) are at the intersection of governance, peace and security, which constitute the essence of the AGA-APSA synergy towards improved governance and security. Fortunately, the synergy offers itself as a structural tool and pathway through which the convention's gap can be resolved.

INTRODUCTION

Recognising the need for a structured and coherent framework towards cyber safety, African leaders gathered at Malabo, Equatorial Guinea, where the African Union Convention of Cyber Security and Personal Data Protection (AUCCSPDP), also known as the Malabo Convention, was created. The Convention aimed to define the objectives and broad orientations of the information society in Africa, and also strengthen existing legislation on Information and Communication Technologies (ICTs) of the Member States and the Regional Economic Communities (RECs).[2] The content of the Convention was based on the continent's needs and context at the time of its development, its adoption (on September 2012 by the AU Expert Group on Cybersecurity) and also its approval (during the 22nd Ordinary Session of the AU Executive Council in January 2013). The Convention is an AU instrument at the foundation of Africa's cyber posture. Cyber posture refers to the status of Africa's information security resources and capabilities in place for management, defence, and responses.

The Convention, in terms of management at continental level, ought to be concerned with mitigating current and potential cyber risks.[3] It aims to set the stage to attain the benefits cyberspace offers Africa's socio-economic development, which is one of the main objectives of the AU's cybersecurity agenda.[4] This approach allows cyberspace to create value while mitigating risks. Analysing cyber risks accurately is crucial to developing well-informed response strategy which all AU member states may leverage. Understanding cyber risks involves what/who the threat agents are, what is being compromised, and its impacts. This necessitates a holistic spectrum that covers the different manifestations of cyberattacks because without them a coherent response is not feasible.[5] Thus, a continental framework such as the Malabo Convention ought to capture these manifestations, especially since they already (or prospectively) impact the social, development and security plan of the AU and its member states.

THE MALABO CONVENTION: AN OVERVIEW

TThe Malabo Convention focuses on three areas: Electronic commerce, Personal data protection, and Cybersecurity and Cybercrime. First, it presents the continent's position on how electronic commerce should be handled from a legal standpoint, including marketing, contractual issues and security of electronic transactions. Second, it places human rights concerns at the centre of data protection by prioritising the global and continental human rights normative frameworks, particularly the African Charter on Human and Peoples' Rights (ACHPR), and establishing a framework relating to the personal data protection of Africans. This includes data collection, processing, transmission, storage or use by any state or non-state actor, data governance, the data subjects' rights and obligation of the data controller. The Convention also recognised the role of National Protection Authorities (NPA), thereby establishing that the framework will, in operation, be treated with the same importance as other human rights issues.

Third, the Convention further prescribes cyber security measures to be taken at the national and AU levels. This specifically involves the development of national cybersecurity policies and implementation strategies; adoption of legal measures to respond to cybercrime; establishment of national regulatory authorities; promoting a cybersecurity culture; establishment of cybersecurity monitoring structures and rights. In addition, it reiterates the importance of international cooperation for national governments. Indeed, there is no doubt that the AU recognises the importance of having a multilateral framework involving all member states for a cyber-safe Africa. This is well justified considering the nature of cyber space through the regional security complex lens. As far as a starting point is concerned, the Convention's provisions are feasible, operable and beneficial. At the time of adoption and approval of the Convention, 2012 and 2013 respectively, the cogent needs were electronic transactions, cybercrime and personal data protection. This framed the context of what the Convention perceived as cybersecurity. In this light, the development of the Convention focused on electronic commerce, data protection and cybercrime.

Almost a decade after, emerging challenges have risen to the point that the scope of the Convention has become insufficient as contemporary realities demonstrate the need to go beyond security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating

cybercrime. Other forms of cyberattack such as cyberterrorism, hacktivism, cyberespionage and cyberconflict/ warfare have come to the fore, and they require policy attention. The continent's preparedness from management level therefore needs to attend to it and this begins with the principal instrument at the root of Africa's cyber posture - the Malabo Convention.

Alongside the limited scope vis-à-vis emerging challenges, the weak political commitment of AU member states remains a constant challenge. The Convention never came into force. This is because the required number of ratifications has not been met: that is fifteen (15). Member states. Since 2013, only thirteen (13) member states have ratified the Malabo Convention as of 2022.

DIMENSIONAL DEFECT: MISSING ELEMENTS IN THE CONVENTION'S SCOPE

- ## Cybercrime and Cyberterrorism

The empirically based compilation in Ogunlana (2019)'s study shows the various dimensions through which cyber criminals and terrorist groups use cyberspace; thereby, establishing major distinctions between cybercrime and cyberterrorism. Hence, even though there are similarities in the tools employed to prosecute both, major differences still remain. The Malabo Convention's focus on cybercrime makes sense as a first-line effort because cybercrime is the most prominent form of cyberattack in Africa. However, cyberspace is increasingly being exploited by terrorist and extremist groups, typically referred to as cyberterrorism. Cyberterrorism generally encompasses two types of threats.[6] The first encompasses the physical act (or threat of) using computer network tools to shut down critical national infrastructures (such as energy, transportation, and other national infrastructures to coerce or intimidate the government or civilian population. The "Cyber_Horus Group" attack on Ethiopia over the Grand Ethiopian Renaissance Dam (GERD) which Ethiopia was building on the Nile is an example under this category.

The second refers to the use of the internet by terrorist groups to communicate and share information and data to radicalise or recruit new members, as well as for financial and logistical purposes.[7,8] Boko Haram and the Islamic State in West Africa have used this tactic.[9]

- ## Hacktivism

Hactivism is the combination of hacking and activism.[10] This is when hacking is used as a strategy to execute a campaign for political or social change. According to a 2012 report by the Chalmers University of Technology and University of Gothenburg, hacktivists leverage their technical skills to divert and bypass security systems to extend the frontiers of their campaign and increase its impact.[11] Examples include; Anonymous (who have targeted African governments over corruption allegations under the operation OpAfrica banner in Ethiopia, Rwanda, Uganda, Zimbabwe, among others.)[12] and Anonymous Africa, a group which launched an attack on South African political parties over racism and websites like Gupta over corruption allegations.[13]

- ## Cyberespionage

Cyber spying tools exist. African leaders have been victims and users of spyware systems like Pegasus. Pegasus is an advanced surveillance tool that grants the attacker access to the victims' data through their mobile phones. While African leaders like South Africa's Cyril Ramaphosa, Morocco's King Mohammed VI, both current and former prime ministers of Egypt, Burundi, Uganda, Morocco, and Algeria have been victims, other leaders have used the same tools on citizens, journalists, activists, and politicians.[14] These unauthorised access is a cyberattack that undermines human rights, freedom, security, and democracy when used to assist unconstitutional change of government).[15] While this falls within the Africa Governance Architecture (AGA) Africa Peace and Security (APSA) spectrum, the Convention neither addresses its political nor corporate dimensions.

Africa is moving towards a single market through the African Continental Free Trade Agreement (AfCFTA). The projectionis positive, but rivalries and competitions are also likely to emerge. This means emphasis on states and corporations acquiring, consolidating and exploiting competitive advantage(s). In addition, as Africa's digital and internet penetration increases, digital/e-commerce expands. The success of AfCFTA would mean a rise in Africa's profile in the global political economy. This will no doubt attract acts of cyberespionage which may manifest as state-state, corporation-corporation, state-corporation, or corporation-state; and potential attacks may be from within or outside the continent – like the 2018 discovery of a Chinese espionage attack on the AU Headquarters.

- ## Cyberconflict/warfare

Assessing the cyberconflict/warfare dimension from a geopolitical stance, intelligence experts predict Africa's increased relevance to global political and economic affairs within the next 20 to 30 years as crucial.[16] Hence, in light of Russia and China's move towards cyber dominance and the Russia-Ukraine war dynamics, alliances and

the likely great power confrontations over cyberspace, would mean that AU as a political bloc may need to take a stand: eastward, westward, or neutral – if not divided. Meanwhile the East and West have stakes in Africa. Herein lies the complication, whatever cyberconflict/warfare happens, Africa's non-involvement does not translate to insulation from its impact, and such impact will be exacerbated by the increased level of interdependence in the international system.

At the continental level, the fact that the Cyber_Horus Group that attacked Ethiopia is based in Egypt, a country with a long history of officially opposing the success of the GERD or any Ethiopian dam on the Nile has the potential to stir up cyberconflict/warfare between both countries, or at best heighten distrust to the detriment of reaching a common ground during negotiations. This is a typical case in which cyberconflict/warfare can be stirred or used to impede conflict prevention and peacebuilding in the physical domain.

In addition, Africa grapples with violent conflicts involving non-state armed groups. The diffusion of power in cyberspace facilitated by the low cost of entry, anonymity and non-attribution offer them leverage.[17] Thus, in addition to the fading of states' monopoly of the use of force, armed groups may exploit cyber tools to prosecute hybrid actions (that is cyber plus physical), which many African countries are not prepared for.

On this premise, Africa needs to prepare for, and not discard, the possibilities of a cyber or hybrid security engagement/warfare initiated or influenced by external, state and non-state actors. The AU must however be conscious of the fact that a solid cyber posture is needed for security order and Africa's collective (cyber)security against internal and external threats.

RATIONALE TO BROADENING THE SCOPE

The tools employed to prosecute cybercrime, cyberterrorism, hacktivism, cyberespionage, and cyberconflict/warfare are often similar. However, contextual differences may occur in cases that are state led/sponsored compared to when it is an action of a non-state actor. The political will needed to address cyberespionage/warfare, for example, is very different from the political will needed to address non state actors, because countries are essentially binding themselves, not enhancing their enforcement powers. This gap is not peculiar to the Malabo Convention in that the Malabo Convention echoes this reality from the Budapest Convention on Cybercrime of the Council of Europe.

Another important distinction to be noted is their varying (political) objectives. For example, the political objective that informs Boko Haram's use of cyber tools is different from a state actor that employs cyberespionage against another AU member state. Furthermore, there are differences in terms of the kind of solution required. For example, boosting technical capacity might be sufficient for an AU member state to respond to hacktivism or cybercrime. This does not necessarily address the externalities resulting from cyberespionage or state-sponsored cyberattack which may have political and diplomatic implications, bilaterally or regionally, in addition to whatever technical problems that surface. Another instance includes continental responses to state-sponsored cyberattack against its citizens, which may be an extension of state-led repression.

THE POLITICAL SETBACK

The Convention is yet to come into force because only thirteen (13) out of 55 AU member states have ratified (and deposited) the Convention.[18] But that number is close to the required 15 states. This gap means what is covered in the Convention is still inoperative, and its implementation is on hold.[19] The non-ratification of the Convention is symptomatic of either a weak political will or a lack of political will, which deepens the weakness of Africa's cyber posture. The root causes for this inadequate prioritisation lie in a low fiscal and technical capacity, lack of interest, detrimental political landscape of these member states and regional political considerations.[20] Some AU member states lack the financial capacity, technical and human skill set for implementation. Others are preoccupied with political and human security crises at the physical level, or their governments do not consider cybersecurity a priority, relevant, or in alignment with their internal or foreign policy objectives.[21]

FORGING AHEAD: ENTRY POINT FOR THE AGA-APSA SYNERGY

The AGA-APSA linkage is well established and policy-relevant.[22] AGA focuses on promoting and protecting rights, consolidating democratic institutions and culture, ensuring good governance and the rule of law, and implementing the African Charter on Democracy, Elections and Governance (ACDEG). Its scope covers norms and standards, institutions and other stakeholders, mechanisms and processes of interaction, and the African

Governance Facility. APSA, on the other hand, is made up of key mechanisms for promoting peace, security and stability in Africa. In recent times, synergising AGA and APSA have become the priority of the Political Affairs, Peace and Security (PAPS) Department of the AU Commission. This is because of the inextricable link between governance and peace and security in Africa and its policy implications in light of emerging realities on the continent. In this regard, it is argued as a means through which AU's responses to instability can be enhanced.[23] This reflects in the AU reforms to fulfil its obligation towards governance, conflict prevention and management. It also flows with the merger of the Political Affairs and Peace and Security departments of the AU Commission.

The close connection between physical space and cyberspace in modern times as well as its position within the scope of the merger inspires the need to explore the opportunities it presents to enhance Africa's cyber posture. There is a cyber dimension to Africa's political, security and governance affairs and both frameworks offer a valid entry point to resolve the highlighted gaps. The Malabo Convention and its gaps which were mentioned earlier are at the nexus of governance, peace and security which constitute the essence of the AGA-APSA synergy towards improved governance and security.

Therefore, a first step could be that the Africa Governance Platform needs to take on cyberspace governance in Africa as a priority issue to bring to the fore the deficiency in the scope of Africa's cyber posture at management level. Serving as a catalyst to achieve AGA's goals, the Platform is an entry point to establish a framework for dialogue towards expanding the Convention's scope, enhancing compliance, implementation and complementarity of related instruments at cyber level, and information sharing.[24] Against this backdrop, AU member states may be stirred towards proposing the amendment and revision of the Malabo Convention. In this regard, the Africa Governance Platform already provides an institutional framework to enhance the content, relevance and impact of the Malabo Convention while also driving the political aspect in terms of enhancing AU member states' attention towards amendment and revision of the Convention: results of the dialogue.

Furthermore, since its inception and based on the factors that necessitated the institution of APSA, the focus had always been on physical security. However, the AU's resilience and adaptation capacity proves that this is insufficient to hinder the strengthening of Africa's cyber posture as Africa's ownership of its cyber agenda demonstrates.[25] Thus, entry points to expand the scope of the Malabo Convention are not impossible. Prevention approach to conflict, as well as peacebuilding and conflict early warning are viable entry points which can be adopted to justify the expansion

of APSA to mainstream cybersecurity – in view of the different manifestations of cyberattacks listed earlier. This can be achieved through a systematic framing of a cyber-peace programme in coordination with the efforts of the AGA Platform, such that its conceptualisation encapsulates everything there is to the cyber dimensions of security and governance issues which the PAPS Department of the AU may oversee. Through dedicated empirical studies and consultations/dialogues, the prime focus would be to redefine the Convention's scope and explore political and diplomatic means to secure member state buy-in towards its amendment, revision and ratification which can be achieved.

CONCLUSION

Through the regional security complex lens, the cybersecurity challenges of one African country cannot be reasonably analysed or resolved independently of continental realities and vice versa. The Malabo Convention's scope and AU member states' buy-in are therefore essential to improving Africa's cyber posture. This can be achieved by leveraging the pathway AGA and APSA offers if cybersecurity is prioritised. Consequently, a broader Malabo Convention, reinforced by the political will and commitment of AU member states, will enhance Africa's cyber posture and re-envision the Convention to be fit for purpose. The framing and implementation of the Convention is a vital issue at the AGA-APSA intersection, which includes in its scope rights, institutions, governance, the rule of law and security. AGA and APSA's framework are ready-made pathways to addressing the gaps impeding the success of the Malabo Convention.

POLICY RECOMMENDATIONS

- The AU Commission through the PAPS Department should prioritize cyberspace governance and (re)define cybersecurity's situation within the AGA and APSA framework. In this regard, a Cyber Peace Programme that encompasses everything there is to the cyber dimensions of the governance-security nexus in Africa may be considered. This proposed programme will include both technical and political projects required to enhance the Convention as well as gain political buy-in from AU member states.
- The AGA Platform needs to actively facilitate dialogues and consultations with the view of expanding the Convention's scope, enhance compliance, implementation and complementarity of related instruments to cybersecurity/ governance, and information sharing.
- The PAPS Department of the AU should harmonize a cyber agenda within the AGA-APSA synergy from a viewpoint that is inclusive of all manifestations of cyberattacks, and on that basis engage state parties that ratified the Malabo Convention with the aim of encouraging them to submit proposals for the amendment and revision of the Malabo Convention. Article 37 of the Malabo Convention gives State parties the authority to submit such proposal to the Chairperson of the Commission of the AU if deemed necessary.
- In the same vein, private sector and civil society may lobby national governments that have ratified the Convention to submit a proposal on the

premise of the various dimensions through which the limited scope of the Convention impacts them.

- Regional Economic Communities' (RECs) role in APSA's success and facilitating regional economic integration positions them as a key stakeholder in the weakness and strength of the Malabo Convention. Therefore, the AU Commission may engage REC in the revision of the Malabo Convention in view of ensuring coordination within the APSA framework in terms of capturing the different manifestations of cyberattacks, enhancing political buy-in with state parties, and encouraging the ratification implementation of the Convention's provision.

ENDNOTES

1. Renard, T. (2014). The Rise of Cyber Diplomacy: the EU, its Strategic Partners and Cyber Security. ESPO Working Paper 7, 7-25; Neutze, J., & Nicholas, J. P. (2013). Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms. Georgetown Journal of International Affairs, 3–15.
2. African Union Convention On Cyber Security And Personal Data Protection, Adopted By The 23rd Ordinary Session Of The Assembly Of The Union, (Malabo, 2014), EX.CL/846(XXV).
3. Philip, J., & Salimath, M. S. (2018). A Value Proposition for Cyberspace Management in Organizations. Business Information Review, 35(3), 122-127.
4. See the African Union Press Release: African Union Cybersecurity Expert Group holds its first inaugural meeting. Available at https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting
5. Ibid
6. Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Centre for Strategic and International Studies.
7. Cox, K., Marcellino, W., & Bellasio, J. et al. (2018). Social Media in Africa: A Double-Edged Sword for Security and Development. United Nations Development Programme (UNDP).
8. Dingji Maza, K., Koldaş, U., & Aksit, S. (2020). Challenges of Combating Terrorist Financing in the Lake Chad region: A Case of Boko Haram. SAGE Open, 10(2), 1-17.
9. Ogunlana, S. O. (2019). Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. Journal of Strategic Security, 12(1), 72–106.
10. Chopitea, T. (2012). Threat modelling of hacktivist groups Organization, chain of command, and attack methods. Chalmers University of Technology and University of Gothenburg.
11. Ibid
12. See https://www.hackread.com/anonymous-targets-african-countries-because-corruption/
13. Seehttps://www.news24.com/fin24/tech/cyber-security/expect-more-hack-attacks-in-sa-anonymous-20160725 and https://www.africanews.com/2016/06/14/anonymous-africa-hacks-websites-of-racist-eff-and-zanu-pf/
14. Allen, N. & van der Waag-Cowling, N. (2021, July 15). How African States can Tackle State-Backed Cyber Threats. Brookings Tech Stream. https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/
15. Allen, N. & La Lime, M. (2021, November 19). How Digital Espionage Tools Exacerbate Authoritarianism Across Africa. Brookings Tech Stream. https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/
16. Discussion, Anonymous, Intelligence Expert, Research Institute for European and American Studies (RIEAS), 15 March 2021.
17. Nye, J. S. (2011). The future of power. Public Affairs..
18. The countries are Angola, Cape Verde, Congo, Ghana, Guinea, Mauritius, Mozambique, Namibia, Niger, Rwanda, Senegal, Togo and Zambia.
19. Blount, P. J. (2016). Reprogramming the World: Cyberspace and the Geography of Global Order (Publication No. 10.7282/T3KK9F01). [Doctoral Dissertation, Rutgers, The State University of New Jersey].
20. Turianskyi, Y. (2020). Africa and Europe: Cyber Governance Lessons. Policy Insights 77, 1-13.
21. Ibid

22. Wachira, G. M. (2017). Strengthening the Peace and Governance Nexus within the African Union: Enhancing synergy between the African Governance Architecture (AGA) and the African Peace and Security Architecture (APSA). NUPI Report 7, 1-49.
23. Bedzigui, Y. (2018). Enhancing AU Responses to Instability: Linking AGA and APSA. ISS Policy Brief 113, 1-11.
24. See About AGA here https://au.int/aga/about
25. See Fidler, M. (2021). Infrastructure, Law, and Cyber Stability: An African Case Study Mailyn Fidler. In: Chesney, et. al. (Forthcoming 2023). Cyberspace and Instability. SSRN

ABOUT THE AUTHOR

Jesutimilehin O. Akamo is the Research Coordinator at the Africa Peace and Security Programme (APSP), Institute for Peace and Security Studies (IPSS), Addis Ababa, Ethiopia. Prior to his current role at IPSS, he served briefly as a consultant to North Atlantic Treaty Organisation Joint Force Command (NATOjfc), participated in various studies under the auspices of African Union (AU) Youth for Peace (Y4P) and Gender, Peace and Security Programme (GPSP), GIZ (the German Corporation), United Nations Educational Scientific and Cultural Organisation International Institute for Capacity Building in Africa (UNESCO IICBA), the Nanjing Peace Forum, United Nations (UN) Office of the High Commissioner on Human Rights – East Africa Regional Office (OHCHR-EARO), the World Bank, and the European Union (EU). His research interests include international institutions, democratisation, governance and institutions, identity politics, information politics, cyber studies, youth, gender, human rights, intelligence studies, migration, terrorism and violent extremism, theories of international relations and the philosophy of technology. He prefers to work on these issues within the context of development, peace and security in Africa. Also, providing technical support to youth-led establishments within these contexts dominates his civil society and entrepreneurial engagements. He holds a B.Sc. and M.Sc. in International Relations from the Obafemi Awolowo University (OAU), Ile-Ife, Nigeria.

IPSS Institute for Peace & Security Studies Addis Ababa University

german cooperation DEUTSCHE ZUSAMMENARBEIT

Supported by giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

IPSS Policy briefs are peer-reviewed quarterly publications that highlight a specific policy gap and provide concrete policy recommendation(s). They aim at providing a platform for practitioners, scholars and decision makers to showcase their evidence- based and policy-focused analysis and recommendations on African peace and security issues/topics. The briefs are premised on the philosophy of 'African Solutions to African Problems'.

Addis Ababa University
ppP.O.Box: 1176
Addis Ababa, Ethiopia

T + 251 (1) 11 245 660
E info@ipss-addis.org
W www.ipss-addis.org

www.facebook.com/ipss.addis
www.twitter.com/ipss_addis
www.instagram.com/ipss_addis