Part II
Security

Rethinking the African Union Non-Aggression Treaty as a Framework for Promoting Responsible State Behavior in Cyberspace

Uchenna Jerome Orji

Abstract In Africa, regional organisations have established legal measures with a view to promoting norms for cybersecurity governance. However, such measures do not explicitly address State aggression in cyberspace. This appears to create legal uncertainty in determining the behavior of States with respect to activities that can constitute aggression in cyberspace. In 2005, the African Union established the Non-Aggression and Common Defense Pact to put an end to 'conflicts of any kind within and among States in Africa.' Given the absence of an explicit regime to govern the behavior of Member States with respect to activities that can constitute aggression in cyberspace, the question arises as to whether it is possible to apply the AU Non-Aggression and Common Defense Pact for such purposes. This chapter considers the prospects and challenges of applying the Pact to State behavior in cyberspace. It makes a case for the application of the Pact's principles to promote responsible State behavior in cyberspace and suggests that such an approach will enhance legal certainty with respect to activities that can constitute aggression in cyberspace.

I. Introduction

It is no longer in doubt that cyber capabilities can be deployed to achieve objectives that endanger international peace and security.[1] Accordingly, there are growing concerns that malicious activities by State actors in cyberspace can harm the critical infrastructure and information systems of other States.[2] States are also increasingly developing offensive cyber capabilities for military objectives.[3] Consequently, there have been several calls for international norms and legal regimes to govern the conduct of

1 Alexander Kosenkov, 'Cyber Conflicts as a New Global Threat,' Future Internet, 8 (2016), 1–9.

2 Martin Rudner, 'Cyber – Threats to Critical National Infrastructure: An Intelligence Challenge,' International Journal of Intelligence and CounterIntelligence 3 (2013), 453–481.

3 James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, D.C.: CSIS 2012), 3–4; Paul Cornish et al., *On Cyber Warfare* (London: Chatham House 2010).

States with respect to cyber activities that can endanger international peace and security.[4]

Such calls have sought to promote international peace and stability by proposing the establishment of rules to ensure responsible State behavior in cyberspace.[5] More importantly, such calls have led to the establishment of international initiatives to promote cyber stability. For example, between 2004 and 2017, the United Nations convened the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) to examine 'existing, and potential threats arising from the use of ICTs [information and communication technologies] by States' and also propose measures to address them, including norms, rules, principles and confidence-building measures.[6] Also, between 2009 and 2012, the Tallinn based NATO Cooperative Cyber Defence convened an international group of distinguished international law academics to study how international law applies to cyber oppressions conducted by States.[7] The study resulted in the publication of an academic and non-binding treatise known as the Tallinn Manual in 2013,[8] with the second edition in 2017.[9] Generally, the Manual clearly advances the position that general principles of existing international law apply to cyber operations without the need for new international legal regimes. At the regional level, intergovernmental organisations such as the Council of Europe, the European Union, the League of Arab States and the Shanghai Cooperation have sought to promote cyber stability by establishing legal and policy regimes on cybersecurity

4 Camino Kavanagh, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* (Geneva: UNIDR 2017), 15–36.

5 Uchenna J. Orji, *Cybersecurity Law and Regulation* (The Netherlands: Wolf Legal Publishers 2012), 75–76.

6 UN General Assembly, *Report of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), 2; UN Office for Disarmament, Fact Sheet – Developments in the Field of Information and Telecommunications in the Context of International Security (July 2018), 2.

7 The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual*, available at: https://cdcoe.org/research/tallinn-manual/.

8 Michael N. Schmitt (ed.), *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press 2013).

9 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press 2017).

governance and the control of cybercrime.[10] In addition, bilateral arrangements that aim to promote cyber stability and responsible State behavior in cyberspace are beginning to feature prominently in the dialogue on international cyber stability.[11]

However, existing initiatives to promote cyber stability have not established binding rules that explicitly address the issue of State aggression in cyberspace. For example, the UN GGE addressed issues relating to State aggression in terms of its recommendation that a State should not conduct or knowingly support ICT[12] activity contrary to its obligations under international law, that intentionally damages or impairs the operation of critical infrastructure used to provide services to the public.[13] This recommendation is, however, not legally binding on States but rather provides a framework of international best practices that States should consider with a view to promoting cyber stability.

Similarly, in Africa, regional organisations have established legal measures with a view to promoting norms for cybersecurity governance. For example, the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA), the Southern African Development Community (SADC) and the African Union (AU) have all adopted regional legal instruments requiring the Member States to establish cybersecurity governance measures.[14] Thus, in 2011, the ECOWAS adopted a Directive to fight cybercrime within the ECOWAS

---

10 The Council of Europe Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23 November 2001); Directive 2013/40/EU of 12 August 2013 on Attacks against Information Systems; Arab Convention on Combating Information Technology Offences (2010); Agreement between the Governments of Member States of the Shanghai Cooperation Organization on Cooperation in the Field of international Information Security (2009).

11 Alex Grigby, 'Overview of Cyber Diplomatic Initiatives' in: Global Commission on the Stability of Cyberspace, *Briefings from the Research Advisory Group to the Global Commission on the Stability of Cyberspace*: *Issue Brief No.1* (The Hague, NL: The Hague Centre for Strategic Studies 2018), 6–38 (24–26).

12 Information and communication technologies.

13 UN General Assembly, *Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (22 July 2015), 8 at paragraph 13(f).

14 ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime (2011); Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) 16 (2011); SADC Model Law on Computer Crime and Cybercrime (2012), available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf; AU Convention on Cybersecurity and Personal Data Protection, EX.CL/846 (XXV) (2014).

region.[15] Also, in October 2011, COMESA developed a Model Cybercrime Bill with a view to providing a uniform framework that would serve as a guide for the development of cybercrime laws in the Member States.[16] In 2012, the SADC adopted a Model Law on Computer Crime and Cybercrime to serve as a guide for the development of cybersecurity laws in the SADC Member States.[17] And in 2014, the AU adopted the Convention on Cyber Security and Personal Data Protection to harmonize the laws of African States on electronic commerce, data protection, cybersecurity promotion and cybercrime control.[18]

The above regional instruments have been adopted following the increasing penetration of information ICTs in Africa[19] and their growing integration in critical national sectors.[20] However, Africa is yet to achieve a high level of digitalisation that is comparable to developed countries. Nevertheless, the rise of digitalisation in Africa has increased the reliance of critical national sectors on information infrastructure to the extent that the disruption of such infrastructure by accidents or cyber attacks will also cause the disruption of economic and social activities and public services in a manner that could trigger serious national security concerns.[21]

Recent research indicate that attacks on critical infrastructure are becoming 'frequent' in Africa, with banks particularly being the common targets and losing billions of dollars to theft and service disruption.[22] There are also reports of the critical infrastructure of African regional organisati-

15 ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty-Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

16 Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) 16 (15 October 2011).

17 SADC Model Law on Computer Crime and Cybercrime (n.14).

18 African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV), adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27 June 2014).

19 See the regional reports provided by GSMA, available at: https://www.gsma.com/mobileeconomy/.

20 Blessings T. Mbatha Dennis Ocholla and Cjb Le Roux, 'Diffusion and adoption of ICTs in Selected Government Departments in KwaZulu-Natal, South Africa,' Information Development 27 (2011), 51–263.

21 Uchenna J. Orji, 'Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa,' International Journal of Criminal Justice 3 (2021), 60–98 (70).

22 Nathaniel Allen, 'Africa's Evolving Cyber Threats,' African Center for Strategic Studies, 19 January 2021, available at https://africacenter.org/spotlight/africa-evolving-cyber-threats/.

ons being targets of hacking. For example, in January 2018, China denied that the computer network equipment it had supplied to the AU allowed it access to confidential information from the AU.[23] In December 2020, it was reported that Chinese hackers had been accessing the security footage from cameras installed at the AU headquarters.[24] Also, in December 2020, it was reported that Facebook found that Russians and individuals affiliated with the French military were using fake Facebook accounts to conduct dueling political information operations in Africa.[25]

However, to a large extent, the focus on cybersecurity governance in Africa appears to be mainly directed towards curbing cybercrimes.[26] Accordingly, although African regional cybersecurity governance measures aim to promote cyber stability, they do not explicitly address the issue of State aggression in the cyber domain. This appears to create legal uncertainty in terms of determining the behavior of African States with respect to activities that can constitute aggression in cyberspace. In 2005, the AU established the Non-Aggression and Common Defense Pact[27] with a view 'to putting an end to *conflicts of any kind within and among States in Africa*' and 'promoting cooperation in the area of non-aggression and common defense.'[28] Could this instrument thus fill the gap and be applied in the context of cyberspace? The aim of this chapter is to consider the prospects and challenges of applying the Pact to State behavior in cyberspace. In so doing, the chapter will make a case for the application of the Pact's principles to promote responsible State behavior in cyberspace. It will suggest that the application of the Pact's principles to promote responsible State behavior in cyberspace would enhance legal certainty with regard to respect to activities that can constitute aggression in cyberspace.

This chapter comprises four sections. Following this introduction, the second section explores the concept of cyber stability within the context of promoting responsible State behavior. The third section discusses the principles of the Pact and considers how they can be applied as a frame-

23 Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents* (Washington, D.C.: CSIS 2021), 35, available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

24 Ibid, 7.

25 Ibid.

26 Orji (n. 21), 60–98.

27 AU Non-Aggression and Common Defense Pact (Addis Ababa, 2005), opened for signature 31 January 2005 (entered into force 18 December 2009).

28 Preamble, AU Non-Aggression and Common Defense Pact (2005), (emphasis added).

work to govern activities that can constitute aggression in cyberspace. It also considers the limits of the Pact in governing cyber activities that can constitute aggression. The fourth section concludes the chapter.

II. Cyber Stability and Responsible State Behavior in Cyberspace

The concept of 'cyber stability' has been defined in various contexts. For example, 'cyber stability' has been defined as 'the ability of all countries to utilize the Internet for both national security purposes and economic, political and social benefit while refraining from activities that could cause unnecessary suffering and destruction.'[29]

Another definition refers to 'cyber stability' as 'a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits of political, civil, social and economic life while preventing and managing conduct that may undermine those benefits at the national, regional and international level.'[30] It has been observed that this definition creates a basis from which to identify when stability is the goal and also to discern what is potentially relevant, useful and strategic information about activity in the cyber domain from what is not.[31]

'Cyber stability' has also been defined as referring to 'a state of relations between States characterised by the absence of serious hostile cyber actions against one another, where the States have a sufficient common understanding of each other's capabilities and intentions so as to be inclined generally to avoid such actions, likely associated with a common belief that the costs of such conduct would outweigh the benefits.'[32]

The Report on a Framework for International Cyber Stability which was commissioned by the United States, refers to 'cyber stability' as 'an environment where all participants, including nation-States, non-governmental organisations, commercial enterprises, and individuals, can positively and dependably enjoy the benefits of cyberspace; where there are benefits

29 Jody R. Westby, 'Cyber War v. Cyber Stability,' presented at the 42nd session of the World Federation of Scientists International Seminars on Planetary Emergencies (Eric, Italy, 19–22 August 2009), 1.

30 Lisa Rudnick, Derek B. Miller and Leeor Levy, *Towards Cyber Stability: A User Centered Tool for Policy Makers* (Geneva: UNIDR 2015), 7.

31 Ibid.

32 R. Gorchayev et al., *Cyber Deterrence and Stability: Assessing Cyber Weapon Analogues through Existing WMD Deterrence and Arms Control Regimes* (Washington D.C.: US Department of Energy, 2017), 1.16.

to cooperation and to avoidance of conflict, and where there are disincentives for these actors to engage in malicious cyber activity.'[33]

A common thread that appears to run through the above definitions of cyber stability is that the concept aims to prevent conflict or hostilities in cyberspace. Therefore, the concept can be used to generally classify measures that aim to prevent or minimize conflict between actors, including States in cyberspace. As such, the concept aims to minimize cyber activities that can escalate tensions between States. However, despite the above definitions of cyber stability, the concept is to a large extent regarded as an emerging concept that has not been developed as an analytic category.[34]

On the other hand, the concept of 'responsible State behavior' is regarded as vague, and its definition is generally dependent on the context in which it is used and therefore varies in each context.[35] For example, the general concept of responsible behavior in cyberspace has been defined as 'behavior by a given actor in a given set of circumstances that can be said to conform to the laws, customs and norms generally expected from that actor in those circumstances.'[36] If the elements of the above definition were to be adapted to the context of State behavior in cyberspace, 'responsible State behavior' would simply refer to a State's compliance with established laws, customs and norms generally expected of such State in cyberspace. The concept of responsible State behavior in cyberspace aims to promote cyber stability by requiring States to ensure that cyber activities which are conducted within their jurisdiction do not cause harm to other individuals or infrastructure located in another jurisdiction. This implies that a State should ensure that cyber activities conducted within its jurisdiction or on the basis of its authority do not escalate cyber instability or create conflicts.

Generally, the need to promote cyber stability through responsible State behavior arises from the increasing interconnectedness of information networks in different countries. This state of affairs has ushered in a new age of network interdependence where the security of each country's network is also dependent on the actions of State and non-State actors around the

33 International Security Advisory Board, *Report on a Framework for International Cyber Stability* (US Department of State, 2014) Appendix B.1, 33.

34 Rudnick (n. 30), 7.

35 Andrijana Gavrilovic, 'What is Responsible Behavior in Cyberspace,' Diplo, 30 October 2018, available at https://www.diplomacy.edu/blog/webinar-what-responsible-behaviour-cyberspace/.

36 Gavrilovic (n. 35).

world.[37] Hence, malicious cyber activities conducted in a particular State can harm individuals or infrastructure located in another State. This also has the potential to affect relations between States in a manner that endangers international peace and security. Therefore, the concept of responsible State behavior in cyberspace requires States to promote cyber stability by ensuring governance responsibility for cyber activities on their territory.

Within the context of cyber stability, the concept of responsible State behavior can be seen as enshrining elements of the international law principle on State responsibility for transboundary harm. This principle has been recognised in different contexts in the *Corfu Channel Case*, where the International Court of Justice (ICJ) held that a State might not 'allow knowingly, its territory to be used for acts contrary to the rights of other States,'[38] and also in the *Trail Smelter Case*.[39] This principle has been recognised in international law that applies to the regulation of communication networks. For example, Article 38.5 of the Constitution of the International Telecommunication Union (ITU) requires Member States not to cause harm to the operation of telecommunication installations in other States.[40] However, while existing principles of international law on State responsibility can be broadly interpreted to promote responsible State behavior in cyberspace, they do not explicitly address activities that can constitute aggression in cyberspace. In the next section, the chapter will consider how the AU Non-Aggression and Common Defense Pact can be applied to govern the behavior of African States with respect to activities that can constitute aggression in cyberspace.

III. The AU Non-Aggression and Common Defense Pact

Africa comprises 55 sovereign States and is classified as the world's second-largest and second most-populous continent after Asia, with a terrestrial mass of 30,2044,049 million square kilometers and a human population of

37 Harry D. Raduege, 'Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad' in: Andrew Nagorski (ed.), *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (New York: East West Institute 2010), 5.

38 ICJ, *Corfu Channel Case* (UK v. Albania), merits, judgement of 9 April 1949, ICJ Reports 1949, 4, at paragraph 22.

39 *The Trail Smelter Arbitration Case (United States of America v. Canada)*, (1938) 3R.I.A.A 1905; Judicial Decision, 'The Trail Smelter Arbitral Decision,' AJIL *35* (1941), 684.

40 Art. 38.5 Constitution of the ITU (2010).

over one billion people.[41] The African Union (AU) is the most prominent regional intergovernmental organisation in Africa, and its membership comprises and unites all the 55 sovereign States in Africa.[42]

The African continent has been challenged by incidents of inter-state conflicts.[43] This state of affairs led the AU to declare that 'the scourge of conflicts in Africa constitutes a major impediment to the socio-economic development of the continent.'[44] Some causes of Africa's interstate conflicts have been traced to colonialism and the subsequent processes of decolonisation and State formation, as well as the ensuring crisis of nation-building.[45] In this regard, it has been observed that 'modern Africa was created by colonial powers out of ethnic and regional diversities [with] gross inequalities in power relations and in the uneven distribution of national wealth and development opportunities.'[46] In some cases, colonial boundaries 'forced starkly different rival cultures to cohabit within the confines of a single State.'[47] This resulted in the creation of fragile political units which divided ethnic groups in several cases while also combining many warring ethnic groups in many cases. Given this state of affairs, most inter-state conflicts in post-colonial Africa have arisen as a result of the boundaries set by colonial powers to demarcate the continent into States.[48]

In order to address the incidence of inter-state conflicts in Africa, the Constitutive Act of the AU recognizes the need to promote peace, security and stability as a prerequisite for implementing Africa's development and integration agenda.[49] Accordingly, the core objectives of the AU include to 'achieve greater unity and solidarity between African countries and the

41 Matt Rosenberg, *The 7 Continents Ranked by Size and Population* (April 2020), available at https://www.thoughtco.com/continents-ranked-by-size-and-population-4163436.

42 'AU Member States,' available at https://au.int/en/member_states/countryprofiles2.

43 Aremu J. Olaosebikan, 'Conflicts in Africa: Meaning, Causes, Impact and Solution,' Africa Research Review 4 (2010), 551.

44 Preamble to the Constitutive Act of the African Union (2000).

45 Herman J. Cohen, 'What Should We Do When Nations Get Angry?,' *Nexus Africa*, 1 (1995), 11–14; Fonken Achankeng, 'Conflict Resolution in Africa: Engaging the Colonial Factor,' AJCR, 2 (2013), available at https://www.accord.org.za/ajcr-issues/%Ef%BFbconflict-and-conflict-resolution-in-Africa/.

46 Cohen (n. 45).

47 Olaosebikan (n. 43), 551.

48 Timothy Gachanga, 'Inter-State Conflicts in Africa,' 7 January 2018, available https://medium.com/@gachannga/inter-state-conflicts-in-africa-2f378a03fa8.

49 Preamble to the Constitutive Act of the AU.

peoples of Africa,'[50] and to 'promote peace, security and stability on the continent.'[51] In addition, the Constitutive Act of the AU establishes a range of principles to prevent inter-state conflicts. These principles include: a) the prohibition of the use of force among the Member States;[52] b) the peaceful co-existence of the Member States and their right to live in peace and security;[53] c) the peaceful resolution of conflicts among the Member States;[54] and d) the establishment of a common defense policy for the AU.[55]

On the basis of the above objectives and principles, the AU has adopted a range of related regional security instruments such as the Protocol Relating to the Establishment of the Peace and Security Council of the African Union,[56] the Common African Defense and Security Policy,[57] and the Non-Aggression and Common Defense Pact. The Protocol Relating to the Establishment of the Peace and Security Council of the African Union creates a framework for the prevention and resolution of conflicts and also establishes the AU Peace and Security Council as collective security and early-warning arrangement to facilitate timely and efficient response to conflict and crisis situations in Africa.[58] The Common African Defense and Security Policy aims to ensure collective responses to both internal and external security threats that affect Africa and serve as a framework for promoting defense cooperation between the African States.[59] On the other hand, the Non-Aggression and Common Defense Pact aims to prevent aggression among African States while also promoting cooperation amongst them in the areas of common defense.[60] However, the discussion in this chapter will focus on the Non-Aggression and Common Defense Pact.

The AU Non-Aggression and Common Defense Pact recognizes the devastating impact of intra and inter-state conflicts on peace, security,

50 Art. 3 lit. a) Constitutive Act of the AU.
51 Art. 3 lit. f) Constitutive Act of the AU.
52 Art. 4 lit. f) Constitutive Act of the AU.
53 Art. 4 lit. i) Constitutive Act of the AU.
54 Art. 4 lit. f) Constitutive Act of the AU.
55 Art. 4 lit. d) Constitutive Act of the AU.
56 Protocol Relating to the Establishment of the Peace and Security Council of the AU.
57 Solemn Declaration On A Common African Defense and Security Policy.
58 Art. 2 Protocol Relating to the Establishment of the Peace and Security Council of the AU.
59 Protocol Relating to the Establishment of the Peace and Security Council of the AU.
60 Art. 2 AU Non-Aggression and Common Defense Pact.

stability and economic development in Africa and therefore seeks 'to put an end *to conflicts of any kind within and among States in Africa* in order to create conditions for socio-economic development and integration of the continent as well as the fulfillment of the aspirations of [African] peoples.'[61] As such, the Pact aims to address threats to peace, security and stability in the continent so as to ensure the wellbeing of African peoples.[62] The Pact entered into force on 18 December 2009 after its ratification by 15 Member States of the AU. As of August 2021, 44 Member States of the AU had signed the Pact, while 22 Member States had ratified it.[63] To a large extent, the Pact is regarded as containing by far 'the most elaborate political commitment of African States not to commit aggression against each other.'[64] To minimize ambiguity in its interpretation, the Pact provides elaborate definitions of terms such as 'aggression,'[65] 'acts of subversion,'[66] 'non-aggression,'[67] 'destabilisation,'[68] 'threat of aggression,'[69] and 'transnational organised criminal group.'[70]

The objectives of the Pact include: a) to promote cooperation among the African States in the areas of non-aggression and common defense; b) to promote peaceful co-existence in Africa; c) to prevent intra and inter-state conflicts; and d) to ensure that disputes between the Member States, including a breach of the peace and security within the AU, are resolved by peaceful means.[71]

In line with the above objectives, the Pact defines a framework for the AU to address situations of aggression in accordance with African regional instruments such as the Constitutive Act of the AU, the Protocol on the Establishment of the Peace and Security Council and the Common African Defense and Security Policy.[72]

---

61 Preamble AU Non-Aggression and Common Defense Pact.
62 Ibid.
63 The Status List AU Non-Aggression and Common Defense Pact, https://au.int.
64 Global Institute for the Prevention of Aggression, *Preventing Aggression in the African Context*, available at: https://crimeofaggression.info.
65 Art. 1 lit. c) Non-Aggression and Common Defense Pact.
66 Art. 1 lit. a) Non-Aggression and Common Defense Pact.
67 Art. 1 lit. p) Non-Aggression and Common Defense Pact.
68 Art. 1 lit. i) Non-Aggression and Common Defense Pact.
69 Art. 1 lit. w) Non-Aggression and Common Defense Pact.
70 Art. 1 lit.x) Non-Aggression and Common Defense Pact.
71 Art. 2 lit. a) Non-Aggression and Common Defense Pact.
72 Art. 2 lit. b) Non-Aggression and Common Defense Pact.

1. The Concept of 'Aggression' and 'Collective Security' under the Pact

The Pact elaborately defines 'aggression' as 'the use, intentionally, and knowingly, of an armed force or *any other hostile act* by a State, a group of States, an organisation of States or non-State actor(s) or by any foreign or external entity, against the sovereignty, political independence, territorial integrity and human security of the population of a State party to this Pact, which are incompatible with the Charter of the United Nations or the Constitutive Act of the African Union…'[73] To some extent, the above definition of aggression appears to mirror elements of the definition of aggression under UN Resolution 3314 (XXIX) due to its adoption of elements such as 'the use … of armed force,' 'against the sovereignty,' 'territorial integrity,' or 'political independence of a State.'[74] However, the definition under the Pact goes beyond Resolution 3314 (XXIX) because it encompasses more elements and appears more extensive in its elaboration of the meaning of aggression. Some elements of the above definition of aggression under the Pact appear to create a broad scope for classifying hostile cyber activities conducted by a Member State against another Member State within the meaning of aggression. For example, the Pact does not restrict the definition of aggression to the use of 'armed force' but includes 'any other hostile act' conducted by a State or non-State actor against the 'sovereignty' and 'human security' of the population of a Member State. In modern times, hostile acts against the sovereignty of a State would include the disruption of its critical information infrastructure given the strategic importance of such infrastructure to national security.[75] As such, under the Pact, there is scope for classifying a Member State's cyber activities that disrupt another Member State's critical information infrastructure as a hostile act that fits into the definition of aggression under the Pact.

The Pact's definition of 'human security' further provides the basis for qualifying a Member State's hostile cyber activities that affect another Member State's population as fitting within the definitional scope of aggression. In this regard, the Pact defines 'human security' as 'the security of the individual in terms of satisfaction of his/her basic needs. It also includes the creation of social, economic, political, environmental and cultural conditions necessary for the survival and dignity of the individual,

73 Art. 1 lit. c) Non-Aggression and Common Defense Pact (Emphasis added).
74 UNGA Res 3314 (XXIX) of 14 December 1974, A/RES/3314 (XXIX), Art. 1.
75 Art. 1 AU Convention on Cyber Security and Personal Data Protection.

the protection of and respect for human rights, good governance and the guarantee for each individual of opportunities and choices for his/her full development.'[76] Within the context of the above definition, a Member State's hostile cyber acts (such as denial of service attacks, attacks on personal data, or cyber attacks that target critical sectors, including banking and financial systems, health institutions or other critical services) against the population of another Member State would qualify as a hostile act against the human security of the targeted Member State's population. This is because such cyber attacks have the potential to make individuals insecure in the information society while also reducing opportunities for the protection of human rights such as the right to privacy and freedom of expression, which are guaranteed under the Universal Declaration of Human Rights[77] and the International Convention on Civil and Political Rights (ICCPR).[78] In addition, such attacks can hinder the potential of ICTs to enhance social and economic development and promote living standards, which would ultimately affect human security.

The Pact classifies specific acts that will constitute 'acts of aggression.' In this regard, it provides that 'the following shall constitute acts of aggression, *regardless of a declaration of war by a State, group of States, organization of States, or non-State actor(s) or by any foreign entity*:

(i) the use of armed forces against the sovereignty, territorial integrity and political independence of a Member State, or any other action inconsistent with the provisions of the Constitutive Act of the African Union and the Charter of the United Nations;
(ii) the invasion or attack by armed forces against the territory of a Member State, or military occupation, however temporary, resulting from such an invasion or attack, or any annexation by the use of force of the territory of a Member State or part thereof;
(iii) the bombardment of the territory of a Member State *or the use of any weapon against the territory of a Member State*;
(iv) *the blockade of the ports, coasts or airspace of a Member State*;
(v) the attack on the land, sea or air forces, or marine and fleets of a Member State;

76 Art. 1 lit. k) AU Non-Aggression and Common Defense Pact.
77 Universal Declaration on Human Rights, UNGA Res 217A (III) of 10 December, 1948, A/RES/217(III),) Arts. 12 and 19.
78 Arts. 12 and 19 International Covenant on Civil and Political Rights (ICCPR).

(vi) the use of the armed forces of a Member State which are within the territory of another Member State with the agreement of the latter, in contravention of the conditions provided for in this Pact;
(vii) *the action of a Member State in allowing its territory to be used by another Member State for perpetrating an act of aggression against a third State*;
(viii) *the sending by, or on behalf of a Member State or the provision of any support to armed groups, mercenaries, and other organized transnational criminal groups which may carry out hostile acts against a Member State*, of such gravity as to amount to the acts listed above, or its substantial involvement therein;
(ix) *the acts of espionage which could be used for military aggression* against a Member State;
(x) *technological assistance of any kind*, intelligence and training to another State for use in committing acts of aggression against another Member State; and,
(xi) the encouragement, support, harbouring or provision of any assistance for the commission of terrorist acts and other violent trans-national organized crimes against a Member State.'[79]

While the above classification of acts that constitute aggression under the Pact adapt several elements from UN Resolution 3314 (XXIX), the Pact however includes additional elements such as acts of espionage, technological assistance and the support of violent transnational organized groups by a Member State.

Article 2(c) of the Pact declares that 'any aggression or threat of aggression against any Member State shall be deemed to constitute a threat or aggression against all Member States of the Union.'[80] This provision implies that the Pact operates a collective security principle. The concept of collective security has several definitions.[81] For example, 'collective security' has been defined as 'a system whereby States commit not to use force unilaterally in their mutual relations by preferring the peaceful settlement of disputes and to support a collective decision aimed at stopping any

79 Art. 1 lit. c) AU Non-Aggression and Common Defense Pact (Emphasis added).
80 Art. 2 lit. c) AU Non-Aggression and Common Defense Pact.
81 Joseph C. Ebegulem, 'The Failure of Collective Security in the Post World Wars I and II International System,' *Transcience*, 2 (2011), 23–29 (23 f.).; Stefan Aleksovski, Oliver Bakreski and Biljana Avramovska, 'Collective Security – The Role of International Organizations- Implications in the International Security Order,' Mediterranean Journal of Social Sciences 5 (2014), 274–282 (274 f.).

act of aggression or common threat to peace.'[82] Following this definition, within the context of Article 2(c), hostile cyber activities conducted by one or more Member States against another Member State would be considered as aggression against all Member States of the AU and would therefore trigger a response from all Members of the Union. In this regard, the Pact imposes obligations on the Member States 'to provide a mutual assistance towards their common defense and security [with respect to] any aggression or threats of aggression,'[83] and 'individually and collectively respond by *all available means* to aggression or threats of aggression against any Member State.'[84]

The Pact does not define the meaning of 'by all available means.' However, literally, the phrase would imply that the Member States are to adopt all means at their disposal, including military, diplomatic and economic measures in responding to aggression or threats of aggression against any Member State. The collective security principle under the Pact appears largely similar to Article 5 of the North Atlantic Treaty, which provides that:

> 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all, and consequently, they agree that, if such an armed attack occurs, each of them, in the exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. *Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security*.'[85]

---

82 Balingene Kahombo, 'The Peace of and Security Council of the African Union: Rise or Decline of Collective Security in Africa,' *KFG Working Paper Series* 23 (2018), 5. See also Evert Jordan, 'Collective Security in Africa: The Tension between Theory and Practice,' *Strategic Review for Southern Africa*, 39 (2017), 160–184 (163 f.).

83 Art. 4 lit. a) AU Non-Aggression and Common Defense Pact.

84 Art. 4 lit.b) AU Non-Aggression and Common Defense Pact.

85 Art. 5 NATO (emphasis added).

However, unlike the North Atlantic Treaty, the Pact does not include a provision that measures taken by the Member States when individually and collectively responding to aggression or threats of aggression against any Member State shall be reported to the United Nations Security Council or terminated upon measures taken by the Council to restore and maintain peace and security. In practice, the collective security regime in Article 5 of the North Atlantic Treaty has been invoked once on 12 September 2001, following the terrorist attacks on the United States on September 11, 2001;[86] however, there is no record that the collective security in AU Non-Aggression and Common Defense Pact has ever been invoked.

2. *Prospects of Applying the Pact to Promote Responsible State Behavior in Cyberspace*

A major basis for considering the application of the Pact as a framework for promoting responsible State behavior in cyberspace arises from its declaration to end '*conflicts of any kind within and among States in Africa* and promote cooperation in the areas of non-aggression and common defense.'[87] By this explicit declaration, the Pact appears to have been drafted with foresight to include and accommodate future technological developments that can create conflicts among States in Africa. This makes the Pact relevant in the context of State aggression in cyberspace. In addition, the Pact's broad definition of aggression to include '*…any other hostile act* by a State, a group of States, an organization of States or non-State actor(s) or by any foreign or external entity…'[88] provides another major basis for considering the application of the Pact as an African framework for promoting responsible State behavior in cyberspace. As noted earlier, hostile acts that violate the sovereignty of a State would include attacks that target its critical information infrastructure, given the strategic importance of such infrastructure to national security.

Furthermore, the Pact's definition of aggression includes elements such as 'the *use of any weapon against the territory of a Member State*;' 'the blockade of the ports, coasts or airspace of a Member State;' 'attack on the land, sea or air forces, or marine and fleets of a Member State;' 'acts of espionage

86 North Atlantic Treaty Organisation, 'Collective Defence – Article 5,' available at: https://www.nato.int.

87 Preamble AU Non-Aggression and Common Defense Pact (emphasis added).

88 Art. 1 lit. c) AU Non-Aggression and Common Defense Pact (emphasis added).

which could be used for military aggression against a Member State;' 'technological assistance of any kind;' 'the action of a Member State in allowing its territory, to be used by another Member State for perpetrating an act of aggression against a third State;' and, 'the provision of any support to armed groups, mercenaries, and other organized transnational criminal groups which may carry out hostile acts against a Member State.'[89]

The above elements provide a broad scope for considering the Pact as a framework for promoting responsible State behavior in cyberspace. For example, 'any weapon' within the context of the Pact would technically include a cyber weapon such as malware, given that such weapon can be used to execute an attack against critical information infrastructure located in the territory of a Member State. Also, cyber attacks can be used to conduct a blockade of Member State's ports, coasts or airspace,[90] while the use of a cyber weapon to immobilize the armed forces or marine and fleets of a Member State would technically fit within the Pact's definition of aggression. This also applies where a Member State engages in acts of cyber espionage which could be used for military aggression against another Member State or provides another Member State with technological assistance of any kind, such as providing cyber capability to conduct aggression against another Member State. In addition, a Member State that allows its territory to be used by another Member State to conduct cyber attacks against another Member State or provides support to mercenaries or criminal groups to carry out such attacks against another Member State would fit within the Pact's definition of aggression.

Other bases for considering the application of the Pact as a framework for promoting responsible State behavior in cyberspace arise from the interpretation of a range of obligations which it imposes on the Member States. For example, Article 5(a) of the Pact requires the Member States to cooperate in preventing acts aimed at the 'destabilization of any Member State.' The Pact defines 'destabilization' as 'any act that disrupts the peace and tranquility of any Member State or which may lead to mass social and political disorder.'[91]

Following the emergence of the information society, it is possible for hostile cyber acts to disrupt critical services and cause mass social and political disorder in a State. Therefore, the Pact's definition of 'destabilization'

89 Art. 1 lit. c) AU Non-Aggression and Common Defense Pact (emphasis added).
90 Christopher C. Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework,' EJIL 12 (2001), 825–865 (838).
91 Art. 1 lit. i) AU Non-Aggression and Common Defense Pact.

along with the obligation under Article 5(a), provides scope for applying the Pact to cyber attacks that can cause mass social and political disorder in a State. In addition, Article 5(b) of the Pact requires the Member States 'to prevent its territory and its people from being used for encouraging or committing *acts of subversion*, hostility, aggression and other harmful practices that might threaten the territorial integrity and sovereignty of a Member State or regional peace and security.' Under the Pact 'acts of subversion' refers to 'any act that incites, aggravates or creates dissension within or among the Member States with the intention or purpose to destabilize or overthrow the existing regime or political order by, among other means, fomenting racial, religious, linguistic, ethnic and other differences…'[92]

To a large extent, the obligation under Article 5(b) provides a broad scope for applying the Pact as a framework for promoting responsible State behavior. This is because acts of subversion can be carried out through the use of cyberspace. For example, cyberspace can be used to spread disinformation or hate speech with the aim of creating dissension and destabilising a Member State. Therefore, the obligation would require a Member State to prevent its territory and its people from being used to encourage or commit acts of subversion through cyberspace.

3. *Limits of Applying the Pact to Promote Responsible State Behavior in Cyberspace*

There are several limitations that would impede the Pact's application as a framework for promoting responsible State behavior in cyberspace. A major limitation in this regard is the issue of attribution. The challenge of accurately attributing cyber attacks to a particular entity affects the classification of cyber attacks as an act of State aggression. Various incidents of cyber attacks in several countries have been categorised as acts of cyberwarfare.[93]

---

92 Art. 1 lit. a) AU Non-Aggression and Common Defense Pact.

93 Jordan Robertson and Laurence Arnold, 'Cyberwar: How Nations Attack without Bullets or Bombs,' *Washington Post,* (8 June 2021), available at: https://www.washingtonpost.com; Stephen Blank, 'Cyber War and Information War à la Russe' in George Perkovich and Ariel E. Levite (eds), *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown: Georgetown University Press 2017), 81–98 (85); Damien McGuinness, 'How a Cyber Attack Transformed Estonia,' *BBC News* (27 April 2017), available at: https://www.bbc.com; Susan Landau, 'National Security on the Line,' JTHTL 4 (2006), 409–447 (429).

For example, in May 2007, Estonia experienced a series of massive and coordinated cyber attacks which targeted the country's public and private critical information infrastructure.[94] The attacks deployed botnets of over one million computers located in over 50 countries around the world[95] and are classified as the world's first cyberwar and linked to Russia.[96] In 2008, during the brief Russian-Georgia conflict, Georgia alleged that Russia had carried out cyber attacks against its government.[97] Similar attacks were also launched against Georgia in 2019.[98] The 2010 Stuxnet attack, which targeted and destroyed Iran's nuclear centrifuges, was reported to be a joint cyber operation between the United States and Israel code-named Olympic games.[99] In 2015, it was alleged that Russia had launched cyber attacks against Ukraine.[100] Following bilateral tensions between China and India, it was reported in 2021 that China-linked groups were carrying out cyber attacks against India's critical infrastructure.[101] However, given that the above attacks were not traced with certainty to a particular State, it becomes difficult to classify such incidents as cyber warfare.[102] With the challenge of attribution, criminal actors or non-State actors can loop through different computer systems in the process of perpetrating cyber

94 Cooperative Cyber Defence Centre of Excellence Legal Task Team, *Case Study Estonia: Legal Lessons Learned from the April-May 2007 Cyber Attacks against Estonia* (NATO CCD COE, 2008).

95 Ibid.

96 Kertu Ruus, 'Cyber War I: Estonia Attacked from Russia,' *European Affairs* 9 (2008), available at: https://www.europeaninstitute.org; Paul Meller, 'Cyberwar: Russia vs Estonia,' *Networkworld.com*, (Maz 24 2007), available at: http://www.networkworld.coml.

97 'UK says Russia's GRU behind massive Georgia Cyber-Attack,' *BBC News (20 February 2020),* available at: https://www.bbc.co.uk.

98 Przemyslaw Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace,'*Just Security* (6 March 2020), available at: https://www.justsecurity.org.

99 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Powers* (New York, NY: Crown 2012), 188–225; David E. Sanger, 'Obama Order Sped up Wave of Cyberattacks against Iran,' *New York Times* (1 June 2012), available at: https://www.nytimes.com/.

100 Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar,' *Wired* (20 June 2017), available at: https://www.wired.com.

101 'China's Cyber-War with India,' *ANI News* (18 March 2021), available at: https://www.aninews.in.

102 Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks,' AJIL 113 (2019), 202–206 (203ff.); Chris Morgan, 'Cyber Attacks: The Challenge of Attribution,' *Digital Shado*ws (June 2021), available at: https://www.digitalshadows.com.

attacks or even orchestrate attacks to appear to originate from government computers in another country. Thus, the problem of attribution creates uncertainty in identifying the origin of cyber attacks or the motive behind such attacks.[103] The challenge of attribution appears more pervasive in Africa given the absence of capacity to address cyber threats and would therefore limit the ability of African States to attribute cyber attacks whether such attacks emanate from an African State or a foreign entity. For example, as of December 2021, only 23 African States had national Computer Emergency Response Teams (CERTs),[104] while many African States still require technical assistance to address cyber threats.[105]

Another limitation is the seemingly weak position of the African Peace and Security Council in implementing the Pact and the Common African Defense and Security Policy.[106] The African Peace and Security Council was established in 2002 to serve as a standing decision-making organ for the prevention, management and resolution of conflicts within the African Union. The Council functions as a collective security and early-warning arrangement to facilitate timely and efficient response to conflict and crisis situations in Africa.[107] In exercising its mandate, the Council is required to be guided by the principles enshrined in the Charter of the United Nations[108] and also cooperate and work closely with the United Nations Security Council, which has 'the primary responsibility for the maintenance of international peace and security.'[109] The Peace and Security Council

103 Uchenna J. Orji, 'Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States,' DATR 6 (2014), 31- 45 (35, 41).

104 Orji (n. 21), 78-81; ITU, *Cybersecurity Country Profiles*, available at https://www.itu; African Union and Symantec Corporation, *Cyber Crime & Cyber Security Trends in Africa* (Tempa, AR: Symantec Corporation 2016), 53–56.

105 UNODC, *Comprehensive Study on Cybercrime* (New York, NY: United Nations 2013), 178.

106 AU, 'Main Successes of the AU in Peace and Security Challenges and Mitigation Measures in Place,' available at: https://au.int; Kristiana Powell, *The African Union's Emerging Peace and Security Regime: Opportunities and Challenges for Delivering on the Responsibility to Protect* (Ottawa: The North-South Institute 2005).

107 Art. 2 Protocol Relating to the Establishment of the Peace and Security Council of the African Union.

108 Art. 4 Protocol Relating to the Establishment of the Peace and Security Council of the African Union.

109 Art. 17 Protocol Relating to the Establishment of the Peace and Security Council of the African Union: Kwesi Aning, 'The African Union's Peace and Security Architecture: Defining an Emerging Response Mechanism,' *Lecture Series on African Security* 3 (2008), 1–13.

is responsible for implementing the Pact[110] and is required to periodically update the Pact so as to enhance its implementation in light of contemporary security challenges.[111] However, the Council has not carried out any update to reflect cyber security challenges that can constitute State aggression under the Pact. More importantly, a critical limitation that will impede the Pact's application for promoting responsible State behavior in cyberspace is the fact that its application is restricted to the African States. However, given the nature of cyberspace, acts that qualify as State aggression in cyberspace against an African State can emanate from outside the continent, thereby making the application of the Pact impossible.

IV. Concluding Remarks

The adoption of regional cybersecurity governance instruments in Africa indicates a collective interest to promote cyber stability. Although existing cybersecurity governance instruments do not address the issue of State aggression in cyberspace and thereby create legal uncertainty with respect to the governance of responsible State behavior, a broad interpretation of the AU Non-Aggression Pact in the light of contemporary cyber challenges appears to address this vacuum.

Despite its limitations, the Pact provides a framework that can promote responsible State behavior among the African States in cyberspace. Its application to acts of cyber aggression would promote legal certainty on the governance of State behavior in cyberspace in Africa while also contributing an example for the development of norms for responsible State behavior in cyberspace. Achieving this prospect will, however, require responses including rising awareness within the AU and its Peace and Security Council on issues bordering on cyber aggression and responsible behavior State behavior in cyberspace.

This step appears imperative given that the African States and regional institutions appear to have focused on curbing cybercrimes while having low levels of awareness of cyber aggression. In concluding, it is important to highlight that although the Pact in its present form can be broadly interpreted to promote responsible State behavior in cyberspace, the AU Peace and Security Council, in the exercise of its mandate, should nevertheless consider making updates to the Pact so as to clearly reflect elements

110 Art. 9 AU Non-Aggression and Common Defense Pact.
111 Art. 21 AU Non-Aggression and Common Defense Pact.

of cyber operations that can constitute State aggression. Such an update will further enhance legal certainty and also go a long way to increase the needed awareness amongst the African States and regional institutions.