Carnelian Journal of
LAW & POLITICS
Vol. I No. II, 2021

ARTICLE

Cyberspace: A Phishing War Zone of the 21st Century: Is Africa Ready for this?

Joseph Olajide Italoye *

Abstract

Cyber space is a fifth zone of the military theater of war across the globe in the 21st century. This new war zone developed as a result of human technological efforts. As it stands, no internationally recognized treaty is regulating this new war zone, save for attempts at governing it through some extant international law instruments by analogy. This analogical attempt is currently not acceptable to all members of the United Nations (UN). Due to non-availability of a treaty to regulate the new war zone, states have now resorted to the creation of cyber commands for offensive and defensive operations in the cyberspace. Moreover, international organizations have been created amongst states in the same region to jointly address or for the aid of each other in the event of military cyber-attacks on any member. They include North Atlantic Treaty Organization- Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Shanghai Cooperation Organization (SCO). The major finding of this research work reveals that African states are deeply rooted in the kinetic means of prosecuting wars with little or no attention for cyber weaponry. Conclusively, recommendations were made for African states on an effective formation and management of cyber armies and how to enhance cyber sovereignty protection of the African cyber-space in readiness for cyber warfare.

Keywords: Cyber Space, Cyber Warfare, African states, Offensive cyber Operation, Defensive cyber Operation.

Introduction

The development of autonomous technology is raising questions and shifting paradigms in a variety of fields.[1] The possibilities for the military uses of autonomous technology are becoming increasingly apparent.[2] Cyberspace has therefore opened up a relatively new war-fare domain.[3] It is a man-made theatre of war additional to the natural theatres of land, air, sea and outer space and is interlinked with all of them.[4] It is a virtual space that provides worldwide inter-connectivity regardless of borders.[5] The current generation of cyber weaponry demonstrates an enormous potential to alter the means of hostile attack, the 21st Century armed services adjusted to the Revolution in Military Affairs (RMA).[6] Cyber weapons are not like traditional weapons of warfare because individuals or states that use cyber weapons may choose from variety methods of cyber warfare, such as IP Spoofing, Trojan Horses, DDoS, and Logic Bomb.[7] Through DDoS attacks, like those used against Georgia, the cyber attacker was able to shut down a website by bombarding it with large amounts of traffic. The weapons also target the accuracy of information to which the computer user has access.[8]

Since the enormous attack on Estonian digital networks in 2007, governments around the world have ordered their respective military branches to develop new offensive and defensive cyber capabilities. In same vein, states either united by region or by alliance have developed a common or joint cyber capacity to aid any member in time of military

***Joseph Olajide Italoye LLB (Hons) BL, LLM, is currently a PhD student at the Adekunle Ajasin University, Nigeria. Mail: jideitaloye@gmail.com**

[1] Aleksi Kajander & Agnes Kasper, & Evhen Tsybulenko, 'Making the Cyber Mercenary – Autonomous Weapons Systems and Common Article 1 of the Geneva Conventions' in Taťána Jančárková, Lauri Lindström, Massimiliano Signoretti, Ihsan Tolga & Gábor Visky (eds.), *2020 12th International Conference on Cyber Conflict* (NATO CCDCOE Publications, Tallinn, 2020).

[2] ibid 80.

[3] Yohannes Eneyew., 'The Impact of Cyber Warfare under International Humanitarian Law: A Critical Legal Analysis', (LL.B project, Wollo University, Ethiopia, 2014).

[4] ibid 6.

[5] ibid 6.

[6] Rex Hughes:'Towards a Global Regime for Cyber Warfare' <www.creativete.combr/download/cyberwars> accessed 21 April, 2021.

[7] Susan Brenner & Marc Goodman: *In Defense of Cyber terrorism: An Argument for Anticipating Cyber-Attacks, (*Tech. Poly publishing, United State of America, 2002).

[8] ibid 42.

cyber-attack. An example is the NATO CCD COE in Tallinn, Estonia establishes to defend members against and also countering advanced cyber-attacks.[9] In the same vein, Shanghai Cooperation Organisation (SCO) which was founded in 2001 was initially a Eurasian construct comprising China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan,[10] but also, and more recently, with South Asia, through the incorporation of India and Pakistan.[11] SCO has always recognized –the key role of the UN and the United Nation Security Council (UNSC) in solving major international problems and in the pursuance of a cooperative international security regime.[12] The prime focus has been border stability, counter-terror cooperation, mutual economic interactions, military and joint intelligence exchanges.[13] It is therefore imperative for African states to come up with defensive cooperative alliance that would be readily available in the event of military attack on any African Nations or on African Nations generally.

African States and Cyber Space

The dimensions for the African military have been to maintain and safeguard the territorial sovereignty of the nation state, namely its land, sea, air, space and now (info-sphere) cyber space.[14] The cyber space as a focus would be central to the security of cyber domain in Africa, taking into consideration the technological advancement in the prosecution of war. In addition, a cyber-army will add to the intelligence component by means of collecting relevant information for situational awareness to

[9] NATO 'Opens New Centre of Excellence on Cyber Defense' NATO News (Tallinn, 20 May, 2008) <www.nato.int/docu/update/2008/05-may/e0514a.html> accessed 21 April, 2021; the, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was formally established on the 14 May, 2008 in order to enhance NATO's cyber defence capability. Their mission is, to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation; NATO CCD COE, 2012, <www.ccdcoe.org/> accessed 21 April, 2021.

[10] Shabana Fayyaz , 'Pakistan and the SCO-Aspirations and Challenges!' (2019) 26 Journal of Political Studies 95.

[11] Bruna Toso de Alcântara, 'SCO and Cybersecurity: Eastern Security Vision for Cyberspace' (2018) 6(10) International Relations and Diplomacy <DOI:10.17265/2328-2134/2018.10.003> accessed 22 April, 2021.

[12] cf Fayyaz (n 11) 96.

[13] ibid.

[14] Michael Aschmann, Joey Jansen van Vuuren, & Louise Leenen, 'Cyber Armies: The Unseen Military in the Grid' (2017) <www.researchgate.net/publication/283697882> accessed 22 April, 2021.

decision makers on the battle field.[15]This will serve as a paradigm shift for African military offensive and defensive operations when cyber warfare programme is fully incorporated into her military arrangement like other nations outside Africa.[16] From the foregoing, the general concern is that the rise in cyber conspiracy and conflicts is capable of provoking a full-scale conventional war or cyber war, or a combination of the two.[17] Especially, when African states wholeheartedly embrace cyber space and treat it as fifth zone of war through adequate preparation. However, African states are endeared to conventional/kinetic form of warfare with little or no attention for cyber weaponry in readiness for cyber battle. This is because African states are encumbered by pressing domestic problems and socio-economic challenges.[18] These local issues have, unavoidably, distracted attention from the emerging threats of the digital world.[19]

This requires African leaders to appreciate the urgent requirement to incorporate this domain into their traditional military operations of land, sea, air and space, making cyber conflict strategy an integral part of overall military strategy, with proportionate investment.[20] Whether African leaders consider cyber warfare or not, the African continent will

[15] ibid 7.

[16] There are indications that the US National Security Agency (NSA) conceives the 'US Cyber Command' as early as the year 2000, in order to build the US cyber warfare effort. This is because, the US fears that 'cyber weapons are as crucial to 21st century warfare as nuclear arms were in the 20th'; John Bamford,, *'God of War (The Secret War)'* Wired Magazine, (USA,2013)*;* <www.wired.com/2013/06/general-keith-alexander-cyberwar/all> accessed 22 April, 2021; furthermore, the US is one of those countries that has continued to invest in cyber activities, as it is purported that the US sets aside about USD4.7 billion annually for developing cyber warriors, including expertise development via encouragement of doctoral degree studies in the various fields of cyberspace; Jason Miller, '*Disruptive by design: Breaking Down the Federal Cyber Budget*', (April,2016,).<www.afcea.org/content/?q=Article-disruptive-design-breaking-down-federal-cyber-budget> accessed 22 April, 2021; China, meanwhile, is building its cyber warfare paramilitary forces, understood to be especially targeting US expertise and specialisations in communications, electronic warfare and networking; Anthony Capaccio, *'China Most Threatening Cyberspace Force, US Panel'* Says (2012) <www.bloomberg.com/news/articles/2012-11-05/china-most-threateningcyberspace-force-u-s-panel-says> accessed 22 April, 2021.

[17] Uche Mbanaso 'Cyber Warfare: African Research Must Address Emerging Reality' (2016) 18 The African Journal of Information and Communication 157 <doi.org/10.23962/10539/21789> accessed 22 April, 2021.

[18] ibid 60.

[19] Dmitry Epstein, Erik Nisbet, & Tarleton Gillespie, 'Who's Responsible for the Digital Divide? Public Perceptions and Policy Implications' (2011) 27 the Information Society 92.

[20] cf Mbanaso (n18) 160.

not be immune to cyber conspiracy and conflicts.[21] While cyber warfare could potentially become deeply embedded in contemporary military operations, there is at present no international convention on this matter.[22] This is why military and government information infrastructure should be protected from attacks[23] from within and outside states in Africa. If necessary, adverse state critical infrastructure and information based processes can be attacked by the cyber offensive army,[24] whenever it is established by any African state.[25] To sum up, many of the conspiracies and conflicts seen among states in the offline realm have shifted to cyberspace.[26] This is why the African region cannot afford to occupy a rear position on the issue of cyber space in terms of the formation of cyber-armies for offensive and defensive operations. It is worthy of note that while hacking of networks and information systems is an illegal activity, there is no international law addressing the use of cyber power against a state.[27]

Effective Formation and Management of Cyber Army in Africa

Preparation for war in the 21st century is more of being technological advanced rather than being conventionally strong in terms of defeating enemy. The readiness of African states is attached to how it can skillfully use cyber space and professionally incorporate cyber armies into their military command. In carrying out this military duty, the following are fundamentally inevitable.

[21] ibid.

[22] ibid.

[23] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 7.

[24] ibid.

[25] For example, Russia has been observed using massive cyber offensives to threaten its former allies, especially the Ukraine and Estonia; Scott Applegate : 'Cyber Militias and Political Hackers: Use of Irregular Forces in Cyber Warfare' (2011) 9 Institute of Electrical and Electronic Engineer Security & Privacy 16; North Korea is constantly using cyber offensives against South Korea; Reuters :North Korea mounts long-running hack of South Korea computers (13 June, 2016) <www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE>accessed 22 April, 2021.

[26] cf Mbanaso (n 18) 161.

[27] cf Applegate, *op.cit.* at 20.

a. Creation of Offensive and Defensive Cyber Capacities

When offence holds the advance, it is relatively easier to move forward, destroy and conquer territory than to protect and defend it.[28] This is why there is a growing interest in the use of Offensive Cyber Capabilities (OCC) among states.[29] A diverse group of states across the world including Columbia[30], Germany[31], Finland[32], India[33], the United Arab Emirates (UAE)[34] and Vietnam[35] have all said they are exploring options for cyber warfare. In turn, states such as the United States[36], Russia[37], Iran[38] and North Korea[39] continue to further develop their OCC.[40]

[28] Charles Glaser & Chaim Kaufmann, 'What is the Offence-Defence Balance and can We Measure it?'(1998) 22 International Security 44.

[29] Max Smeets & Herbert Lin, 'Offensive Cyber Capabilities: To What Ends?' in Tomáš Minárik, Raik Jakschis & Lauri Lindström (eds.) *2018 10th International Conference on Cyber Conflict* (NATO CCDCOE Publications, Tallinn, 2018).

[30] Christoffer Frendesen, 'Colombia Sends Officials to Estonia for Cyber Defence Training' Columbia Reports (2 September, 2014) <colombiareports.com/colombias-govt-sends-security-forces-estonia-cyber-defense-training/> accessed 22 April, 2021.

[31] Nina Werkhäuser : 'German Army Launches New Cyber Command', Defence World (1 April, 2017) <www.dw.com/en/germanarmy-launches-new-cyber-command/a-38246517> accessed 22 April, 2021.

[32] Secretariat of the Security Committee, *Finland's Cyber Security Strategy* (2013) <www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.> accessed 22 April, 2021.

[33] Vivek Raghuvanshi, 'New Indian Cyber Command Urged Following Recent Attacks', Defense News,(6 June,2016) <www.defensenews.com/2016/06/06/new-indian-cyber-command-urged-following-recent-attacks> accessed 22 April, 2021.

[34] Thomas Bindiya, 'UAE Military to Set up Cyber Command' Defence World, (30 September, 2014) <www.defenseworld.net/news/11185/UAE_Military_To_Set_Up_Cyber_Command#.WW4nJYjyiUk> accessed 22 April, 2021.

[35] Jim, Giang Tran, & Tu Ngoc Trinh, 'New Law on Cyber Security in Vietnam' Tilleke & Gibbins 3 June,2016) <www.tilleke.com/resources/new-law-cyber-security-vietnam> accessed 22 April, 2021.

[36] Sean Lyngaas, 'Pentagon Chief: 2017 Budget Includes $7Bn for Cyber', FCW (2 February, 2016) <fcw.com/articles/2016/02/02/dod-budget-cyber.aspx> accessed 22 April, 2021.

[37] Eugene Gerden, 'Russia to Spend $250m Strengthening Cyber-Offensive Capabilities' SC Magazine UK, (4 February,2016)<www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive- capabilities/article/470733> accessed 22 April, 2021.

[38] Bozorgmehr Sharafedin, 'Iran to expand military spending, develop missiles', Reuters, (9 January, 2017)<www.reuters.com/article/us-iran-military-plan/iran-to-expand-military-spending-develop-missiles idUSKBN14T15L> accessed 22 April, 2021.

[39] David Sanger, David Kirkpatrick & Nicole Perlroth, 'The World Once Laughed at North Korean Cyber Power. No More', The New York Times (15 October, 2017) <www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html> accessed 22 April, 2021.

[40] cf Smeets & Lin (n 30) 56.

Concurrently, many states have adopted cyberspace as a new operational domain of warfare, alongside land, air, space and sea.[41] This shows that OCC can alter the manner in which states use their military power.[42] Unlike conventional capabilities, the effects of OCC do not necessarily have to be exposed publicly, which means the compelled party can back down post-action without losing face thus deescalating conflict.[43]

There are reasons why offensive strategies have an upper hand in cyberspace. Firstly, attacks in cyberspace occur at great speed, putting defenses under immense pressure, as an attacker has to be successful only once, whereas the defender has to be successful all of the time.[44] Secondly, the prospect of launching attacks with relative anonymity (and therefore impunity) lowers the expected cost of offensive strategies in cyberspace.[45] Furthermore, physical distance is relatively inconsequential in the virtual world.[46] Cyber-attacks can emerge practically from anywhere, providing significant latitude for attackers to seize the initiative and catch defenders by surprise.[47] It is therefore worthy of note that cyber technologies lead to great improvements in the mobility and reach of force, to which there is an increase in offensive advantage.[48] It is therefore imperative for African nations to create cyber space unit in their respective military formation in order to strengthen their offensive capability. This is in the light of the facts that nations from other continents are advancing daily on the unit of OCC. In another vein, effective defensive operations begin with an understanding of the value of the information system and the databases within the total information system.[49] African states need to carefully concentrate on

[41] Chris McGuffin & Paul Mitchell, 'On Domains: Cyber and the Practice of Warfare' (2014) 69 International Journal 394.
[42] cf Smeets & Lin (n 30) 57.
[43] ibid.
[44] John Sheldon, 'Deciphering Cyber Power Strategic Purpose in Peace and War' (2011) 98 Strategic Studies Quarterly 75.
[45] ibid.
[46] Joseph Nye, 'Cyber power' Belfer Center for Science and International Affairs, Harvard Kennedy School, (2010) <belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html> accessed 22 April, 2021.
[47] cf Sheldon (n 45) 98.
[48] cf Glaser, & Kaufmann (n 29) 62.
[49] Thomas Johnson 'Cyber Intelligence, Cyber Conflicts, and Cyber Warfare' in Thomas Johnson (ed.) *Cyber-Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (Taylor & Francis Group Publishing, United State, 2015).

strategic aspect of information buffer their military capacity. It would therefore create an effective operational cyber defensive value for African nations in their preparation for cyber space domination. It is noteworthy that Defensive Operation on Cyber Warfare which is also known as Computer Network Defense (CND).[50] In the military sense, CND may very well parallel the strategies and tactics that are used for conventional defence,[51] which African states need to appreciate and inculcate in the formation and management of cyber armies. It is however, important to put effective counter measure in place to reduce or prevent unnecessary military cyber-attack.[52]

b. Cyber Sovereignty and Obligation

States are entitled to, where applicable, the rights of sovereignty in cyberspace,[53] which African States must make use in the formation and management of its cyber armies. This includes sovereignty rights over cyber infrastructure, online data, cyber activities and public cyber management in its territory.[54] Extra-territorial jurisdiction under international law over cyber activities outside its territory; the right of self-defence against armed attacks; the right to invoke counter-measures against international wrongful acts; and the right to equally participate in global cyber governance and the international law-making process.[55]

[50] Computer Network Defence (CND) is defined by the US Department of Defense (DoD) as 'Actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorised activity within Department of Defence information systems and computer networks'; Cyberspace and information operations study center, *Cyberspace & Information Operations Study Center. What are information operations?* (24 July, 2010) <http://www.au.af.mil/info-ops/what.htm> accessed 22 April, 2021.

[51] Steve Winterfeld & Jason Handress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice* (Elsevier, Inc, United State, 2013).

[52] The ICJ in *Gabcikovo-Nagymaros Case* (Hungary/*Slovakia*), 25 September 1997, [1997] I.C.J. Report. 7, paras. 52, 82–85 has elaborated three conditions for a justifiable countermeasure: (a) it must be taken in response to a previous international wrongful act of another State and must be directed against that State; (b) the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it; and (c) the effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question.

[53] Ma Xinmin, 'Key Issues and Future Development of International Cyberspace Law (2016) 2 China Quarterly of International Strategic Studies 119.

[54] ibid.

[55] ibid.

State sovereignty in cyberspace also implies that a state is to fulfill its obligation in respect for the sovereignty of other states, ensuring that it shall not knowingly allow cyber infrastructure located in its territories to be used for acts that adversely and unlawfully affect other states.[56] Maintaining peaceful use of cyberspace and refraining from the threat or use of force; non-intervention of internal affairs of other states by cyber means; and finally, respect and protection of basic human rights and freedoms including the freedom of speech and expression.[57] In the formation of African cyber-armies, both intra-territorial jurisdiction and extra-territorial jurisdiction must be carefully considered in line with articles 2(4) and 51 of UN Charter.

c. Cyber Weapons Manufacturing Guidance

Cyber weapons by their nature require constant modifications to overcome the active defences of the target.[58] It means, for the formation and management of cyber army, cyber weapon designers for African states must first understand the dynamism of cyber defence generally in the African context. As a result, those designing weapons may be called upon to operationalise their weapon, using intelligence about the target to do so.[59] The ICRC's *Interpretive Guidance* categorises those whose 'continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation' as combatants.[60] It would distinguish these individuals from 'recruiters, trainers, financiers and propagandists,' who contribute to the war effort, but in a manner more akin to civilian supporters than combatants.[61] It is therefore, imperative for African states to note that an effective formation and management of a cyber-army must show a clear demarcation between active cyber participants and perceive cyber war participants. In the context of cyber operations the *Guidance* considers the purchase; manufacturing and maintenance of weapons out-side of a specific military operation.[62] In the same vein, the collection of intelligence that

[56] ibid.

[57] ibid.

[58] Vijay Padmanabhan 'Cyber Warriors and the Jus in Bello' (2013) 89 International Law Studies 288.

[59] Sean Watts 'Combatant Status and Computer Network Attack (2010) 50 Virginia Journal of International Law 392.

[60] Nils Melzer, *International Committee of the Red Cross, Interpretive Guidance on the Notion of Direct Participation in Hostilities* (ICRC, Switzerland,2009).

[61] ibid 34.

[62] cf Padmanabhan (n 59) 302.

is not tactical in nature, to be civilian functions.[63] In all, civilians must be well considered before the formation and management of cyber weapons to prevent or reduce to the barest minimum, injury to civilians.

Cyber Sovereign Protection of African States

The role of the cyber-army for African states will be the protection of her cyber sovereignty, specifically in safeguarding military equipment, government information and civilian cyber infrastructures.[64] In order to effectively actualise cyber sovereignty protection for African states, the following are of great importance.

a. Formation of Military Cyber Commands Capacity

Cyber command formation is a combination of military formations in one unit for adequate cyber military power of offensive and defensive operations. Advanced nations like United State of America through it United State Cyber Command (USCYCOM),[65] China Cyber Operation,[66] United Kingdom Cyber Security Strategy,[67] Russia Cyber Defence,[68] North Korea Cyber Warfare,[69] and most recently Nigeria Cyber Command[70] have created cyber command capacities. African states can protect both military and civilian cyber infrastructures through cyber capacity by carefully observing and adopting these five 'strategic initiatives'[71] with the peculiar variations. First, cyberspace is to be considered a distinct domain, allowing the 'Department of Defence (DoD) to organise, train, and equip for cyberspace.[72] African nations must

[63] ibid.

[64] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 8.

[65] Julie Lowrie, 'Cyber Security A Primer of U.S. and International Legal Aspects" in Thomas Johnson (ed.),*Cyber Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (Taylor & Francis Group, LLC, New York, 2015).

[66] Dean Cheng, *Cyber Dragon Inside China's Information Warfare and Cyber Operations* (Praeger Publishing, United State, 2017).

[67] Paul Cornish, David Livingstone, Dave Clemente & Claire Yorke *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House, London, 2010).

[68] Igor Bernik, *Cyber Crime and Cyber Warfare*, (John Wiley & Sons, Inc, London, 2014).

[69] ibid 122.

[70] Kate O'Flaherty, 'The Nigerian Cyber Warfare Command: Waging War in Cyberspace' (2018) < forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in cyberspace/#1e48436b2fba> accessed 23 April, 2021.

[71] Gary Solis, 'Cyber Warfare' (2014) 219 Military Law Review 1.

[72] *United State Department of Defence Strategy for Operating in Cyberspace* (2019) <www.slideshare.net/DepartmentofDefence/department-of-defencestrategy-for-operating-in-cyberspace>accessed 23 April, 2021.

therefore, begin to move from dissipating strength on kinetic warfare to cyber building capacity. In the same vein, African states must do it in air, land, maritime, and space to support national security interests.'[73] Second, the DoD will employ new defence operating concepts to protect networks and systems, including sensor, software, and intelligence defences against insider threats.[74] This will requires African nations using trained cyber personnel to muster defensive capacity for a nation to prevent military cyber-attack. Third strategic initiative requires the DoD to act with other government departments and agencies, and the private (i.e., defence contractor) sector, to generate an overarching government-wide cyber security.[75] This will facilitate harnessing cyber-technology like the United States Cyber Command (USCYCOM),[76] for the purpose of protecting government and civilian infrastructure from cyber-attack. Furthermore, the DoD is directed to partner with allies and international partners to strengthen cyber security.[77] Formation of cyber warfare partnership among African states like NATO CCD COE will facilitate exchange of timely and relevant cyber knowledge and threat signals of malicious code. Finally, a high quality cyber workforce, capable of rapid technological advancement, is mandated.[78] This is pointing to the activities of highly sophisticated cyber warriors which African nations must understand and form to swiftly respond to cyber-attack and can lunch cyber-attack.[79]

b. Activities of Cyber Warriors

Cyber warriors could be a state's cyber warriors or non-state cyber warriors. Cyber warriors involved in the design and launch of cyber weapons, as well as quasi-independent groups used to launch cyber operations, could conceivably meet these requirements.[80] Therefore, for

[73] ibid.

[74] cf Solis (n 72) 38.

[75] ibid.

[76] cf Lowrie(n 66) 199-54.

[77] cf Solis (n 72) 39.

[78] United State Department of Defence Strategy for Operating in Cyberspace ibid 10.

[79] Russia was allegedly said to have used *www.xakep.ru* and *www.stopgeorgian.ru* to carry out cyber-attack on Georgia in 2008; Jon Swaine '*Georgia: Russia "Conducting Cyber War'* The Telegraph (2008), <telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russiaconducting-cyber-war.html> accessed 23 April, 2021.

[80] cf Padmanabhan (n 59) 294.

African states to adequately protect their cyber sovereignty in the 21st century, formation and maintenance of cyber warriors is inevitable.[81] For example, Chinese People's Liberation Army's strategic cyber command is located in the 3rd General Staff Department, whose estimated 130,000 personnel man signals intelligence and defence information systems.[82] In the same vein, an African state must also prepare to defend it cyber territory from the activities of non-state cyber warriors. For example, members of Al Qaeda have admitted to engaging in "low level and disruptive" cyber operations and denial of service attacks as part of their organization's war with the United States.[83] This is because, as it stands, such individuals, even if part of the armed wing of Al Qaeda, would not qualify for lawful combatant status.[84] African states must as a matter of importance include in their preparation, ways of defending their cyber territory from non-state cyber warriors. However, discrete use of non-state cyber warriors by African nations for military cyber-attack may also be adopted, since attribution is a major challenge.[85] This can be possible so far African states can manage to evade responsibility and liability.[86] It is worthy of note that non-state actors launch cyber offence and defensive actions.[87]

[81] Pakistan Cyber Army (PCA): A small but very talented army, Bangladesh Cyber Army: An army that hacked the Central Bureau of Investigation of India and several websites from schools and the media, Indishell: India has also developed its own cyber army (non-state actors) to counteract the numerous attacks by Pakistan and Bangladesh. It is a collection of the best hackers, using ordinary IT equipment. They are the most secretive cyber gangs ever formed in the history of the internet; Israeli hack teams: They were on the news for hacking anonymous websites and hurting members of Anonymous. Hackers operating under the name of 'Israeli Elite' broke into websites in Pakistan and installed images of Israeli Defence Force soldiers and the Israeli flag; Siddiqui, Sadiquik, *'Most Dangerous Cyber Armies and Their Attacks.: Real Hackers Point'* (2013) <realhackerspoint.blogspot.in/2013/04/most-dangerous-cyber-armies-and-their.html> accessed 23 April, 2021.

[82] cf Solis (n 72) 4.

[83] cf Padmanabhan (n 59) 296.

[84] ibid.

[85] The attacks on Estonia and Georgia demonstrate how attribution can fit in the peculiar environment of cyber warfare, but in a less distinct way than in traditional warfare settings; cf Cornish, Livingstone, Clemente, & Yorke, (n 68) 13.

[86] In *Prosecutor v Tadic* Case No. IT-94-1-A, Appeals Chamber Judgment*,* 137 (Appeals Chamber, ICTY, 15 July,1999) 'Under international law it is by no means necessary that the controlling authorities should plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations and any violations of international humanitarian law. The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group.'

[87] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 4.

They are hired by governments, military forces, or the private sector for such actions and receive a financial fee.[88] African states cannot therefore, afford to continually prosecute war in a kinetic/conventional way, when the activities of non-state warriors (cyber armies of non-state actors) are prominent across the globe. Cyber armies of non-state actors include[89]:

i. 3xp1r3 Cyber Army: A Bangladeshi group focusing on the United States (US) defaced websites by including the following message: 'Protest against the Shit Movie 'Innocence of Muslims' created by U.S. agencies';
ii. K9 Network Cyber Army: This is one of the smallest but most dangerous cyber-armies. It focuses on defacing USA websites;
iii. MI6 Hackers Team: A United Kingdom (UK) based team that has some of the best hackers in the world. They hacked the Al-Qaeda website and replaced the bomb-making recipe with cupcake recipes;
iv. Team Poison: The Child of Z Company Hacking Crew, a gang consisting of less than 10 people was founded in 2008 by a 16 year old hacker. This cyber gang is one of the most notorious gangs in the history of internet;
v. Anonymous: They originated from the 4chan image board website and describe themselves as 'an internet gathering' with 'a very loose and decentralized command structure that operates on ideas rather than directives'. Anonymous has member who strongly oppose Internet censorship and surveillance. The DDoS attacks by Anonymous are performed by using Low Orbit Ion Cannon software, which users willingly download. This download sends stress signals to the destination directed by Anonymous. One of their biggest attacks is 'OpIsrael'. Anonymous protested what they called the 'barbaric, brutal and despicable treatment of the Palestinian people by the Israel'.

[88] James Jay Carafano, *'Fighting on the cyber battlefield: Weak states and non-state actors pose threats: The Heritage Foundation'* (2013) <www.heritage.org/research/commentary/2013/11/fighting-on-the-cyber-battlefield-weak-states-and-nonstate-actors-pose-threats> accessed 23 April, 2021.

[89] cf Siddiqui (n 82) 23.

Non-state actors fight for their beliefs or financial gain and execute attacks independently against nations or private organisations as a cyber-army outside of the military or government's authority.[90]

c. Cyber Intelligence Collection and Analysis

The cyber intelligence component is vital for the collection and analysis of the cyber space to provide a view on the cyber threats and vulnerabilities,[91] which is important for an African state. This can be achieved adequately with a meaningful alliance with an advance nation on cyber domain. Intelligence analysis will help an Africa-nation to reduce vulnerability to military cyber-attack. A state left vulnerable after each attack also recognises that it would be at a disadvantage if it does not begin to include strategic cyber offensive and defensive operations into its national defence blueprint.[92] In achieving this, professionalism in the collection and analysis of cyber intelligence by the ICT Experts, otherwise known as digital literate is significant to African states' military cyber domain. Digital literacy refers to the skill-set necessary to participate in the digital era.[93] These skills are more than the ability to use digital devices.[94] It also includes for example, reading instructions from graphical displays in user interfaces; using digital reproduction to create new meaningful materials from existing ones.[95] Therefore, having a pragmatic understanding of the rules that prevail in the cyberspace[96] in terms of cyber intelligence collection and analysis will help African nations' cyber domain. However, instead of channeling the digital skill towards building a formidable cyber power in Africa, cyber-crime is what is gaining grounds. For example, internet use and development in developing nations of the world like Nigeria, South Africa, Togo, Ghana, and Cameroon have witnessed whirling incidences of cyber-

[90] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 4.

[91] *ibid.*

[92] Denise Baken, *'Cyber Warfare and Nigeria's Vulnerability'* (2013) <www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability> accessed 23 April, 2021.

[93] Elvira Libaba Paraiso, 'Towards a Cyber Safety Information Framework for South African Parents' in Van Niekerk, (ed.) *Proceedings Of The African Cyber Citizenship Conference 2016* (Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, 2016).

[94] ibid 87.

[95] ibid.

[96] Yoram Eshet-Alkalai, 'Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era' (2004) 13 *Journal of Educational Multimedia and Hypermedia* 93.

crimes.[97] This rarely received governmental attention consequent on the technical nature of these crimes.[98]

d. Cooperation with Cyber Power for Assistance on Cyber Command

Cyber army (cyber command) for African states will be an extension of military power to close the gap of the fifth dimension info-sphere.[99] Therefore, collaborating with states that have developed cyber commands will be of an immense cyber benefit.[100] It will enhance the defending and protection of the technological realm and the cyber space of African nations and be able to offensively fend off a cyber-onslaught from adversaries. [101] In the same vein, sharing of military cyber information among African states will rapidly develop cyber commands of African states. African states can take a clue from NATO CCD COE which holds yearly Cyber Conference (Cy-Con) which is now an internationally-acclaimed conference addressing cyber conflict and security from the perspectives of technology, strategy, operations, law, and policy.[102] Therefore, cooperation can be facilitated through the establishment of an annual conference that would serve as an avenue to exchange cyber space information or knowledge.

e. Funding of Cyber Programme

African nations must be prepared to finance the formation and maintenance of cyber programmes. For example, US cyber budget under the Obama administration was estimated at 4.7 billion USD, and it spent 358 million USD on the headquarters in which its new

[97] Emmanuel Adu & Adedayo Ige 'Secondary School Teachers' Perceptions of Incidences of Cyber Crimes Among School-Aged Children in Lagos State, Nigeria' in Van Niekerk (ed.) *Proceedings Of The African Cyber Citizenship Conference 2016* (Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, 2016).

[98] ibid 62.

[99] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 9.

[100] Apart from the United States, the most powerful country in the field of cyber warfare is China, since cyber warfare is of critical and vital importance to the country; cf Bernik (n 69) 113.

[101] ibid.

[102] Tomáš Minárik, Raik Jakschis, Lauri Lindström & Ann Väljataga 'Introduction' in Tomáš Minárik, Raik Jakschis & Lauri Lindström (eds.) *2018 10th International Conference on Cyber Conflict* (NATO CCDCOE Publications, Tallinn, 2018).

cyber command was housed.[103] It is therefore imperative for an Africa state to include cyber budget in its fiscal financial budget and remain consistent about it. The United States as one of the most powerful cyber actor has a comprehensive cyber funding programme which an Africa states can take clue from. The Fiscal Year (FY) 2020 Cyberspace Activities budget ($9.6 billion) focuses on implementing the DoD Cyber Strategy with renewed emphasis on: [104]

i. Reducing risk to DoD networks, systems, and information by investing in more cyber security capabilities (FY 2020, $5.4 billion);
ii. Supporting Combatant Commander cyber operations by providing integrated cyber capabilities to support military operations and contingencies (FY 2020, $3.7 billion);
iii. Focusing on research and development to support Defensive Cyber Effects Operations (DCEO), Offensive Cyber Effects Operations (OCEO), and Defense of the DoD Information Network (DODIN) (FY 2020, $0.5 billion);
iv. The $3.7 billion cyber operations budget includes $2.0 billion to continue support for Cyber Mission Forces (CMF).

In the same vein, the UK effectively manages its exposure to cyber risks,[105] The UK National Cyber Security Strategy (the Strategy) runs from 2016 to 2021 and it has a £1.9 billion budget.[106] Russia is committing more than 100 million dollars yearly to the training of cyber weapon developers in order to remain as one of the strongest nations on the cyber scene.[107] It is therefore important for an Africa state to carefully count the cost before embarking on cyber programmes, due to financial implication.

Conclusion

The African cyber armies will be able to defend and attack adversaries from the tactical level right through to the national strategically

[103] Warren Strobel, & Deborah Charles, *'With troops and techies, US prepares for cyber warfare'* (2013) <www.reuters.com/article/2013/06/07/ususa-cyberwar-idUSBRE95608D20130607> accessed 23 April, 2021.

[104] Secretary of Defense (Comptroller) *Defence Budget Overview: United State Department of Defence Fiscal Year 2020 Budget Request* (2019) <comptroller.defense.gov> accessed 23 April, 2021.

[105] House of Commons Committee on Public Accounts *Cyber Security in the UK* (2019) <www.parliament.uk/copyright/> accessed 23 April, 2021.

[106] ibid.

[107] cf Minárik, Jakschis, Lindström & Väljataga (103) 138.

level.[108] If it is carefully and strategically put in place, a cyber-command that will be handled by cyber experts/cyber weapon developers. However, international cyber law is also to be kept in mind when launching offensive cyber-attacks.[109] Nations need to come to a resolution in which there should be a cyber-treaty signed in order to pursue cyber peace globally.[110] In order to be relevant in the making of cyber-treaty when the time comes, African cyber-armies must not only be formed, it must also continuously be managed by cyber experts. This will enhance cyber sovereignty protection of the African nations and make them ready for military cyber warfare.

[108] cf Aschmann, Jansen van Vuuren & Leenen (n 15) 10.

[109] ibid.

[110] ibid.