Global Journal of Politics and Law Research

Vol.4, No.2, pp.43-54, March 2016

Published by European Centre for Research Training and Development UK (www.eajournals.org)

CYBER SECURITY, SOVEREIGNTY AND DEMOCRATIC GOVERNANCE IN AFRICA, CHALLENGES

Paschal Oguno Ph.D

Anambra State University, Now Chukwuemeka Odumegwu Ojukwu University, Igbariam Campus, Anambra State Nigeria.

ABSTRACT: *Much of Africa is presently firmly committed to advancing the standards of democracy and human rights that has become topical over the past two decades. Priority reforms to forge a non formidable democratic rule that will secure and maintain the sovereignty of the African nation include the need to improve on both the information society and knowledge economy. This shades light on one of the key phenomenon in the digital age which is our strong dependence on information systems in our life styles, living conditions and our security. Cyber security is a phenomenon which is closely tied to the rapid expansion of information and communication technologies. It has taken a global proportion and occurs across Africa as well as the world in general such that no individual society can disregard it. But Africa has a huge challenge on the face of high rate of cyber crime, cyber terrorism, cyber fraud, cyber attacks and cyber warfare. These cyber threats do not only constitute challenges to humanity and its governance mechanism but they also show us beyond doubt that our policies, institutions, infrastructure and our defense and security systems are not only unprotected but are fragile in nature. The cyber criminals used these threats to continue their malicious pursuit for spying, destabilizing people, organizations and governance perpetrating sabotage or destroying information systems thereby provoking fear psychosis. This highlights the shortcomings and weaknesses of security, governance systems and sovereignty in general. In this environment of growing insecurity, the digital divide is widening to Africa's detriment and getting trivialized in the same way as poverty that ravages Africa. The continent is still not enjoying all the dividend of digital technology and yet it suffers all the disadvantages more than any other. This work is set to anticipate and analyse governance trend in the face of Africa's cyber security and sovereignty issues and challenges. To do so we shall identify the barriers to digital sovereignty by securing the digital and technological sovereignty of states in Africa by proposing ways and means of achieving this digital sovereignty. Again, we shall suggest ways of promoting democracy by preserving fundamental rights and civil liberties especially by protecting personal data and to propose the areas where Africa needs to refine its cyber legislation so as to deepen trust in the information society. This is what this work is set to achieve.*

KEYWORDS: Cyber Security, Governance, Sovereignty, Democratic, Africa

INTRODUCTION

Globally sensitive information is now being stored on computers. These computers are often attached to the internet. The information include information on governance which border on the sovereignty and democracy of the state in issue. Presently, Africa is strongly committed to

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

improving the standard of democracy and human right and this has become topical over the past two decades.[1]

To achieve a strong democratic rule that will secure and maintain the sovereignty of the African nations, priority reforms are required to be put in place and include the need to improve on both the information society and the knowledge economy. This shades light on one of the key phenomenon in the digital age, which is our strong dependence on information systems in our lifestyles, living conditions and security.

The African community as a whole has huge challenges on the face of high rate of cyber terrorism, cyber fraud, cyber attacks and cyber warfare. These cyber threats do not only constitute challenges to humanity and its governance mechanisms but they also show us beyond doubt that our policies, institutions, infrastructure and our defense and security systems are not only unprotected but are fragile in nature.[2]

Cyber security is therefore inevitable at this time in order to protect the sovereignty and democratic governance of the nation of the world particularly African nations. Cyber security itself is a phenomenon which is closely tied to the rapid expansion of information and communication technology.[3] It has taken a global proportion and occurs across Africa as well as the world in general such that no individual society or nation can disregard it. This work is therefore apt at this time to elicit some of the challenges of achieving cyber security in Africa of which lack of good democratic governance, violation of sovereignty and lack of good cyber security standards are chief. Possible means of eliminating these challenges shall also be marshaled out.

DEFINITIONS AND EXPLANATIONS OF KEY TERMS:

Democratic Governance: This means the government by the people, exercised either directly or through elected representatives. It could also be said to be a political or social unit that has such a government. Again it could be said to be the common people considered as the primary source of political power or it could be referred to as the majority rule. *Demos* means "people" from Greek Demokratia. In sociology it connotes the practice or spirit of social equality or a social condition of classlessness and equality under government, policies and diplomacy. It connotes also the common people, especially as a political force. Democracy or democratic governance can be said therefore to be a form of government in which sovereign power resides in the people and is exercised by them or by officers they elect to represent them. It is the doctrine that the numerical majority of an organized group can make decisions binding on the whole group. Democratic governance in a nut-shell is the capacity of the society to define and establish policies and resolve their conflicts peacefully within the existing legal order. This is a necessary condition for the rule of law in addition to the separation of powers and a legal system that ensures the enjoyment of individual freedoms and rights-civil, social, political and cultural. This in turn requires institutions based on the principles of equity, freedom,

[1] Dominique Djindjere, Cybersecurity, Sovereignty and Democratic Governance in Africa, http://en.wikipedia.org/wiki/cyber_security_standards#standard_of Assessed on 15/12/2015
[2] Ibid.
[3] Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

participation in decision making, accountability; and promoting the inclusion of the most vulnerable sectors of a society. [4]

There was massive movement towards multiparty elections across the African continent in the 1990s, giving the expectations of democracy to millions of voters after long periods of dictatorship.[5] Democracy, having been given at the very minimum, denotes the right of the people to choose their own government through an institutionalized multiparty system and periodic secret ballots. Democracy in the main includes the struggle for recognition which was first recognized by **Plato** in the republic. According to **Fukuyama**, humans crave personal self esteem, the desire for recognition, and the accompanying emotions of anger, shame and pride, which are so critical political life and which have fostered the need for democratization in different societies.[6]

Again five cultural factors that inhibit the establishment of sustainable liberal democracy were outlined by Adedeji.[7] These are nationalism, ethnicity, religious fundamentalism, high socio-economic inequalities, the absence of a healthy civil society, and the absence of effective honest and moral leadership. In the demand for democratic change by the people, poverty and economic crisis seem to provide a basis and indeed a common platform. Thus, the struggle for democratization in Africa has relevance not only in liberalizing the political arena and achieving civil and political liberties, but also to ensure better living standards and social welfare for the African people in other words achieving the object of good governance.[8]

The culture of democratic governance moves beyond the mere procedures of democracy and the establishment of democratic institutions. It involves promoting the sustainability of democracy which includes an enduring capacity for: the separation of powers and independence of the branches of government; the exercise of power in accordance with the rule of Law; the respect for human rights and fundamental freedoms; and the transparency and accountability of a responsible civil service, functioning at both the national and local levels. A state which identifies with the culture of democratic governance is one which welcomes a wide scope of political participation embracing a pluralistic system of political parties, a vibrant civil society and media. Further, strong democratic institutions promote and integrate women and minorities in all levels of the government and the society as a whole. Also, a state which embodies the culture of democratic governance is one which protects the right and dignity of children. Therefore the promotion of the culture of democratic governance involves an integrated approach to sustainable governance for and by all the people.[9]

---

[4] Neil Brenner; Democratic Governance, http://www.regionalcentrelac-undo.org/en/democratic-gove. Assessed n 23/4/2015

[5] Ibid.

[6] Fukuyama F, The End of History and the Last Man. London: Hamish Hamilton, 1992 in www.academia.edu/12062304/Cybersecurity_Sovereignty_and_Democratic_Governance_in_Africa_What_are_the_challenges. Assessed on 1/12/2015

[7] Tumusime Isaac: http://www.content.eisa.org.za/pdf/sym06cp.pdf in www.academia.edu/12062304/Cybersecurity_Sovereignty_and_Democratic_Governance_in_Africa_What_are_the_challenges. Assessed on 1/12/2015

[8] Ibidi., Adejumobi 1996, Mamdani 1987, Lisulo 1991

[9] Opcit., http://www.unmit.unmissions.org/Default.aspx?tabid=12071&language=en.US. In www.academia.edu/12062304/Cybersecurity_Sovereignty_and_Democratic_Governance_in_Africa_What_are_the_challenges. Assessed on 1/11/2015

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

Cyber Security: The word cyber relates to, or involves computers or computer network (as the internet).[10] It is a prefix that means "computer" or "computer network" as in cyber space, the electronic medium in which online communication takes place or it could be said to be a virtual reality. This is the use the word cyber is put in science. The word cyber originally is from Cybernetics. Cyber Security therefore is the body of technologies processes and practices designed to protect networks, computers, programs and data from attack, damages or unauthorized access. In a computing context, the term security implies cyber security. The choice between writing cyber security as two words (cyber security) or one (cybersecurity) depends on the institution, and there have been discrepancies on documents in the United States.[11] However, since the United States Federal Executive Order (EO) 13636 on the subject was spelled "Improving Critical Infrastructure Cybersecurity", most media and forums have embraced spelling "cybersecurity" as a single word.[12]

Sovereignty: Sovereignty on the other hand means supreme authority or power.[13] It also means the quality or state of being sovereign or of having supreme power or authority. It also connotes the status, dominium, power or authority of a sovereign, royal rank or position or royalty. Sovereignty could also mean supreme and independent power or authority in government as possessed or claimed by a state or community. It could be said to be rightful status, independence, or prerogative. It could also be said to be a sovereign or independent state, community, or political unit. It therefore could be said to be the supreme and unrestricted power, as of a state or the position, dominion, or authority of a sovereign especially of an independent state. We also have sovereignty in the bible of God, the absolute right to do all things according to his own good. [14]

Sovereignty of African nations and cyber security: We have about 54 sovereign states and 10 non-sovereign territories in Africa.[15] The 54 fully recognized states are all members of the **United Nations** and all except Morocco are members of the **African Union**.[16]

The notion of sovereignty presupposes that every independent state and community has supreme and unrestricted, independent and prerogative power or authority in governing the people within its community or political unit. Such power or authority ought not to be violated by any act of interference except with the concession of the state. This heralded the principle of territorial integrity which is of great essence in international law. The General Assembly Resolution[17] underlines simplicita that any attempt at the partial or total disruption of the national unity and the territorial integrity of a country is incompatible with the purpose and principles of the **United Nations**. Another Resolution[18] also buttresses this point under the Declaration on Principles of International Law Concerning Friendly Relations. It emphatically stated that nothing in the declaration shall be construed as authorized or encouraging any action

[10] Ibid.

[11] Elliot Grauds; Deparment of Homeland Security, A Comparison of Cyber Security Standards Developed by the Oil and Gas Segment. (November , 2004) in www.en.m.wikipedia.org/wiki/list_of_sovereignty_states_and_dependent_territories_in_Africa. Assessed on 18/12/2015

[12] Ibid.

[13] Bryan Garner; Black's Law Dictionary, 7th Ed., St Paul Minn. 1979

[14] Dan Chapter 4, verses 25 and 35, Romans Chapter 9 verses 15 to 23, 1st Timothy Chapter 6 verse 15, Revelation Chapter 4 verse 11.

[15] Member States United Nations. www.en.m.wikipedia.org/wiki/list_of_sovereignty_states_and_dependent_territories_in_Africa. Assessed on 16/11/2015

[16] Ibid.

[17] General Assembly Resolution 1514 (xv) 1960.

[18] Ibid., Resolution 2625 (xxx), 1970.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

which would dismember or impair totally or in part, the territorial integrity or political unity of sovereign or independent states. The territorial frame work of independent states is further encapsulated in the doctrine of *uti possidetis juris*. Under this doctrine, it is possible that boundaries established and existing at the moment of independence cannot be altered unless the relevant parties consent to the change. The International Court of Justice Report has it that the *uti possidetis juris* constituted a general principle whose purpose was to prevent the independence and stability of new states from being endangered by fratricidal struggles provoked by the challenging of frontiers. And that this essential requirement of stability had induced newly independent states to consent to the respecting of colonial borders and to take account of it in the interpretation of the principles of self determination of peoples.[19] This decision of the International Court of Justice shows that the doctrine of *uti possidetis juris* finds acceptance in both international instruments and in judicial pronouncements.[20]

Again, it was established as a principle that whatever the circumstances, the right to self-determination must not invoke changes to existing frontiers at the time of independent except where the states concerned agree otherwise.[21] The organization of African Unity, now African Union had earlier in a conference of its Heads of State in 1963 at Addis Ababa held that the rights of all peoples to control their destiny is inalienable.[22] The violation of the sovereignty of African Nations can easily be dictated when it relates to its geographical territory that it would when its digital technology is being violated. This is because there is growing environment of insecurity in the digital divide which is widening to Africa's detriment and yet like poverty it is getting trivialized.[23] In Africa generally, she is lagging behind in technology. Africa could be said to be consumers rather than producers of technology and content. Some African countries and organizations are excluded from information society which they ought to be an integral part of. They also participate only marginally in the knowledge economy which ought not to be so.

Clearly, there exists what is called cyber space which the principle of territorial integrity and sovereignty ought to protect. The state of governance in Africa in the face of cyber security leaves much to be desired. Cyber-attacks affect the digital sovereignty of African organizations not only in the public operations but also in the private or social spheres. The question is whether Africa is in a position to develop the capacity for response and resilience to cyber threats. Poverty, underdevelopment and lack of capacity to contribute to the world's wealth of cyber knowledge have deprived Africa the position to develop the capacity for response in that direction. Africa also lacks the resources to frame its own vision of cyber security and sustenance of the tenets of the much desired vision in cyber space. There are challenges posed by an attempt to anticipate and analyze governance trends in the face of Africa's cybersecurity and sovereignty issues. Such challenges in the main include as follows:

[19] Burkina Faso v Mali ICJ Reports, 1986 p. 554.
[20] General Assemblies Resolution 15(xv) and 1541(xv), OAU (non AU) Resolution. 16(i), 1964.
[21] Opinion NO. 2 of the Arbitration Commission of the European Conference on Yugoslava.
[22] African Report (1963) pp 9-10 in www.en.m.wikipedia.org/wiki/list_of_sovereignty_states_and_dependent_territories_in_Africa. Assessed on 17/12/2015
[23] Adriane Fugh; Cybersecurity, Sovereignty and Democratic Governance in African, A Publication of the Africa Center For Strategic Studies, www.en.m.wikipedia.org/wiki/list_of_sovereignty_states_and_dependent_territories_in_Africa. Assessed on 16/11/2015

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

1. The ability of Africa to identify the areas where she needs to refine its Cyber Legislation which includes the areas of freedom of speech, intellectual property, child protection and security to mention but a few. This will help deepen trust in the information society.

2. The ability to identify the barriers to digital sovereignty by securing the digital and technological sovereignty of states, individuals and organizations through eradication of economic dependence, lack of national initiatives, lack of national infrastructure *etcetera* and by proposing ways and means to achieve this digital sovereignty.

3. Capacity to raise awareness on the need to preserve fundamental rights and civil liberties especially by protecting personal data. This can easily be achieved by defining an appropriate legal framework, promoting social and state-run initiatives to achieve this, *etcetera.*[24]

Cyber security Standards: Cybersecurity standards are security standards which enables organizations to practice safe security techniques to stop cybersecurity attacks.[25] These guides provide general outlines as well as specific techniques for implementing cybersecurity. For certain standards, cybersecurity certification by an accredited body can be obtained. There are many advantages to obtaining certification including the ability to get cyber security insurance.

By way of history, cybersecurity standards have been created recently because sensitive information is now being stored on computers that are attached to the internet. Also many tasks that were once carried out by hands are now being carried out by computers; therefore there is a need for information assurance (IA) and security. Cybersecurity standards were designed and had continued to develop over time. An information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) called **ISO/IEC 27001:2005** is part of the growing ISO/IEC 27000 family of standards. Its full name is ISO/IEC27001:2005-International Technology-Security Techniques-Information security management systems-Requirements.[26] This standard was developed to formally specify a management system that is intended to bring information security under explicit management control.

ISO/IEC 27002 was later developed to incorporate in the main part 1 of the BS779 good security management practice standard. The latest version of BS7799 is BS7799-3. ISO/IEC27002 is sometimes referred to as ISO 17799 or BS7799 part 1 and could either be referred to as part 1 and part 7. Notably, BS 7799 part provides an outline or good practice guide for cybersecurity management; whereas BS7799 part 2 and ISO270011 are said to be normative and therefore provides a framework for certification. Importantly ISO/IEC 27002 is a high level guide to cybersecurity. It is most beneficial as explanatory guide for the management of an organization to obtain certification to the ISO27001 standard. Once the certification is obtained, it lasts for three years. Although it depends on the auditing organization, some intermediate audits may be carried out during the three years.

[24] Ibid.

[25] Guttman, M., Swanson, M., National Institute of Standards and Technology; Technology Administration; U. S. Department of Commerce; Generally Accepted Principles and Practices for Securing Information Technology System (800-14). (September 1996) in http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 16/12/2015.

[26] National Institute of Standards and Technology; Technology Administration; U.S. Department of Commerce., An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 in http://en.wikipedia.org/wiki/cyber_security_stanards#standard_of... Assessed on 18/12/2015

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

ISO 27001 (ISMS) replaced BS7799 part 2, but it is said to be hackward and any organization working towards BS7799 part 2 can easily transit to the ISO 27001 certification process. There is also a transitional audit available to make it easier once an organization is BS7799 part 2-certified for the organization to become ISO 27001-certified. ISO/IEC 27002 provides best practice recommendation on information security management for use by those responsible for initiating, implementing or maintaining information security management system (ISMS). It states the information security system required to implement ISO 27002 control objectives. Without ISO 27001, ISO 27002 control objectives are ineffective. ISO 27002 controls objectives are incorporated into ISO 27001. It is worthy of note, that ISO/IEC 21827 (SSE-CMM-ISO/IEC 21827) is an International Standard based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) that can measure the maturity of ISO control objectives.

Standard of Good Practice

Standard of Good practice refers to best practices for information security. The Information Security Forum (ISF) was established in 1990 and it published a comprehensive list of best practices for information security, published as the Standard of Good Practice (SoGP).[27] The ISF continues to update the SoGP every two years; and the latest version was published in 2013.

Originally, the standard of good practice was a private document available only to ISF members, but the ISF has since made the full document available for sell to the general public. Among other programs, the ISF offers its member organizations a comprehensive benchmarking program based on the SoGP. Furthermore, it is important for those in charge of security management to understand and adhere the NERC CIP compliance requirement.

The North American Electric Reliability Cooperation (NERC) has created many standards.[28] The most widely recognized is NERC 1300 which is a modification update of NERC 1200. The newest version of NERC 1300 is called CIP/002/3 through CIP/009/3 (CIP=Critical Infrastructure Protection). These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best practice industry processes. Standard of good practice includes other special publications like NIST 800-12 which provide a broad over view of computer security and control areas also implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. More especially, it was written for those people in the federal government responsible for handling sensitive systems.

We also have ISO 15408 which developed what is called the common criteria and also many different software applications to be integrated and tested in a secure way. Others include RFC (Request For Comment) 2196 which is a memorandum published by internet engineering task

[27] Swanson, M., National Institute of Standards and Technology; Technology Administration; U. S. Department of Commerce; Generally Accepted Principles and Practices for Securing Self-Assessment Guide for Information Technology System (800-14). (September 1996) in http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 16/12/2015.

[28] The North American Electric Reliability Council (NERC). http://www.nerc.com. Retrieved November 12, 2005 in http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 29/12/2015.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

force for developing security policies and procedures for information systems connected on the internet.[29] It provides also a general and broad overview of information security including network security, incident response, or security policies. The document is very practical and focuses on day to day operations. This is to mention but a few.

DEMOCRATIC GOVERNANCE IN AFRICA AND CYBER SECURITY

In Africa today, senior defense and security officials must adopt higher standards of leadership to reshape Africa's security forces into professional bodies capable of handling contemporary security threats and earning the respect of civilian populations.

There is need for politicians to adhere to constitutional limits on power in order to avoid placing military officers in the position of choosing between respecting civilian authority and upholding democracy. Security cooperation and assistance from international partners should favour African states with a track record of responsible governance within the security sector as an incentive.

In Niger, Honduras, Turkey, Bangladesh, Guinea, Madagascar, Thailand and Mauritania in recent years there is serious political crises which illustrates the continuing influence of security forces on the political trajectories of countries around the world.[30] Examples of such instability are particularly recurrent in Africa. When Africa's political crises turn into coups, armed insurrections, or tragic confrontations the defense and security forces (DSF) are invariably key players. For many years, such military actions were justified as an established right of state sovereignty over domestic issues. Often, they were even recognized as such on the international level.

This state of affairs is no longer acceptable. Most African countries are presently firmly committed to furthering the standards of democracy and human rights that have advanced over the past two decades. Nonetheless, the path towards democracy, stability and development is long and has many blind alleys. If Africa is to stay on this path, its defense and security forces must resolutely fulfill the role assigned to them by the nations they serve with dedicated and consistent adherence to constitutional rule and a republican outlook.

Cyber security no doubt can be said to be the emerging face of security both in the information society and the knowledge economy. As such, it sheds light on one of the major phenomena in the digital age, which is our strong dependence on information systems in our lifestyles, living conditions and security. Cybersecurity is a phenomenon tied closely to the rapid expansion of information and communication technologies and the blurring lines between the public and private spheres. It has taken global proportions and occurs across the world such that no society, organization and individual can disregard it. This need for security is not only geographical but is inherent in cyberspace. The environment for communication formed thanks to the global interconnectivity of digital data processing equipment cannot be underrated. But apart from its

[29] Ibid.
[30] Dominique Djindjere, Cybersecurity, Sovereignty and Democratic Governance in Africa, http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 18/12/2015.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

technological component, cybersecurity also dovetails permanently with our reality, both in its material and virtual forms.[31]

Today, cybersecurity places us before a huge challenge that analysts have termed "the horsemen of the apocalypse" in the digital era: cybercrime, cyber terrorism, cyber fraud, cyber attacks and cyber warfare.[32] It is said that these cyber threats do not only constitute challenges to humanity and its governance mechanisms, but they also show us beyond doubt that our policies, institutions, infrastructure and our defense and security systems are all insecure and fragile in nature. Those who use these threats can continue their mischievous pursuits for spying, destabilizing people and organizations, perpetrating sabotage or destroying information systems, and provoking fear psychosis. We therefore use information and communication technologies to communicate, explore, learn, play or do business. The year 2015 kicked off with news of cyber-attacks and acts of terrorism perpetrated with information and communication technologies, thereby highlighting the shortcomings and weaknesses of security governance system.[33]

In this environment of growing insecurity, the digital divide is widening to Africa's detriment and getting trivialized in the same way as poverty. The continent is still not enjoying all the dividends of digital technology, yet it suffers all the disadvantages more than any other. As consumers and not producers of technology and content, some African countries and organizations are excluded from the information society that is supposed to be inclusive and participate only marginally in the knowledge economy.

It comes therefore as no surprise that Africa is experiencing a dearth of adequate solutions for its cyber security needs, this places a considerable part of the continent in what is termed criminal havens or cyber crime zones. However, although Africa is lagging behind in technology, efforts are being made to pave new in roads to the digital world, as well as to define an intervention framework for all stake holders. It is in this respect that a convention in cyber crime and the protection of personal data was adopted on 27 June 2014 in Malabo.

Without disputing the utility and need for a legal framework in this area, more has to be done to compliment this instrument with strategic thinking and forward planning so that it comes into force (after fifteen state parties have signed it) and is operationalized effectively, efficiently and sustainably.

RECOMMENDATIONS

Necessary Reforms

From the foregoing, it has been said that proper definition of a nation's cyber space, geographic territory and sovereignty is much desired to secure its cybersecurity. Proper application of the tenets of democracy is required to be put in place also for good governance. How can the defense and security forces be refashioned to support democracy is a question confronting us at this stage. Ultimately, this is dependent on deep respect for the rule of law by all stakeholders,

[31] Ibid.
[32] Ibid.
[33] Alan. R. Gaaby; Cybersecurity, Sovereignty and Democratic Governance in Africa, http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 27/12/2015.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

whether civilian or military, governmental or non-governmental. The caliber of command and leadership exercised by a country's senior officers, accordingly, will determine the defense and security forces (DSF) ability to effectively support democratic government. To this end, defense and security sector leaders and security sector leaders should focus on five priority reforms to forge a new military government in Africa.[34]

Reform No. 1: Building Institutions of Professional Defence and Security Forces (DSF)

Order, discipline, know-how, and rigorous standards have always been the main stays of effective defense and security forces. Scenes of mutiny, looting, and violence by troops are setbacks which are all too familiar in Africa and are the antithesis of professional DSF. It is recommended that reforms that enhance ethics improves training and provide adequate means to support well being of troops will institute and sustain professionalism.

The foundation of a professional defense and security force is reflected by basic ethical value typically formalized in an official code of conduct meant to guide the thoughts and actions of troops. Such values include loyalty to the nation and to the armed forces, a sense of duty, selfless service, and integrity. While some security forces in Africa wholly lack codes of ethics, others in countries such as Mali, Senegal, Zambia, Ghana, Tanzania and Malawi have made great strive to inculcate these norms into their day to day operations. A code of conduct, however, is only valuable in so far as it is known and respected. A successful effort in Mali have shown, such codes must be instilled in new recruits as well as seasoned officers and modeled by commanders if they are to be absorbed.

Ethical values must also be reinforced by a senior command that scrupulously reward troops on merit and performance and strictly prohibit favouritism and arbitrary decision making. Moreover, leadership by example is a fundamental quality of a disciplined and ethical DSF. Senior officers must know how to listen and advocate for their troops, exercise authority fairly, and emphasis professional development.

Reform No. 2: Establish National, Threats-Based DSF

Some African defense and security forces continue to operate without any constitute document that clearly sets forth their missions or defines their rules of deployment. This perpetuates many problems and causes great confusion in defining their purposes, their configurations, and the resources and the task assigned to them. Some nations of Africa are now firmly committed to furthering the standards of democracy and human rights.

In the field, this often results in forces that are insufficiently organized and poorly equipped with lopsided troop numbers that are difficult to manage and control. Roles and responsibilities of the military and police in some instances are unclear and overlap, leading to inadequate budgetary support, improper and counterproductive deployments. To remedy these structural and organizational weaknesses, it is incumbent on the senior chain of command to do the following:

1. Define a clear and pertinent inter-services national security strategy.

[34] Dominique Djindjere; Democracy and the Chain of Command: A New Governance of Africa's Security Sector, A Publication of the Africa Center for Strategic Studies. http://en.wikipedia.org/wiki/cyber_security_standards#standard_of... Assessed on 18/12/2015.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

2. Establish suitable doctrines for the use of force.
3. Opt rational organizational structures.
4. Establish and maintain appropriate human and material resource management practices.[35]

Well conceived National security plans are signs of military professionalism that enable proactive, flexible and rapid responses to threats. Ghana, Senegal, Sierra Leone and Burkina Faso among others, have made note worthy progress towards making such comprehensive plans. A coherent national security strategy provides a systematic basis to restructure a nations defense and security forces. This is a top priority given that force structures for many African countries are misaligned with today's threats.

A rational defense structure provides commanders and oversight authorities the ability to better balance the mission to be filled with available resources. It also fosters a more outcome based means to create by gets, recruit, train, procure assets, maintain equipment, and reliably track troop compensation. As a result, even in a context of limited budget resources, overall efficiency and readiness can improve. Additionally, these tools help prevent embezzlement and corruption, a frequent affliction within African DSF. For example, public submission of the defence budget to parliament was reinstituted in Zambia in 1990 and has continuously led to adjustment that produce new efficiencies, review poor management and rectify the misallocation of funds within the DSF. Restructuring defense and security forces must involve key societal stakeholders. This approach underscores that DSF are from and for the brother society not distinct from it.

Sierra Leone, which continues to consolidate reforms made during a comprehensive DSF restructuring, provides a model of productive, consultative defense review. Citizens group, civilian agencies, and senior officers collaborated to design new policies that streamlined the DSF command structures, elevated training and personnel priorities and enhance accountability and transparency. Other reforms include inspiring of complexity of non military factors. These will help to enhance good governance, democracy and sovereignty required for cybersecurity.

Cybersecurity has been shown to be guaranteed when cybersecurity standards are adopted and put in use. Africa therefore needs to be abreast with current cybersecurity standards. Their cyberspace too is required to be well defined and well secured. They should ensure that they participate as an integral member of the information society in the technological divide particularly in computer design.

CONCLUSION

In conclusion therefore, the degree to which democracy is consolidated in Africa is contingent on defense and security forces that are well structured, professionally based on republican values, and subordinate to civilian political authority. Across the continent, then, all societal and governmental leaders, including top military officials must acknowledge the need to reserve outdated mindset that stymie necessary reforms and adjustments. Additionally,

[35] Ibid.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)

international partners must work to consistently encourage good governance and unequivocally denounce the interference of defense and security forces in politics, politicians who seek to skirt constitutional checks and balances and the use of armed militias and mercenaries as an instrument of contestation and conquest. Sustained support to committed reformers as they seek to implement sound, consensus-based plans is equally critical. With professional defense and security forces fully dedicated to these reforms, Africa will be able to sustain the momentum now under way and steadily expand the number of countries on the continent respectful of democracy and human rights.

When this is achieved, defining each of Africa nations cyberspace will be paid attention to. Again, designing its cybersecurity and adopting internationally accepted cybersecurity standards will be in the limelight. There is therefore a correlation between cybersecurity, democracy (good governance), and sovereignty.

ISSN 2053-6321(Print), ISSN 2053-6593(Online)