Asian Journal of Applied Science and Technology (AJAST)

(Peer Reviewed Quarterly International Journal) Volume 3, Issue 3, Pages 41-52, July -September 2019

Critical Thinking in Information Technology and Management for National Security in Nigeria

Awosusi Oladotun Emmanuel[1] & Ogbuleke Loveday Enyinnaya[2]

[1]*Department of International Relations and Strategic Studies Legacy University, The Gambia. Email: Awosusioladotun@yahoo.com*
[2]*Department of Peace and Conflict Resolution, Legacy University, The Gambia. Email: l.ogbuleke@legacyuniversitygm.org*

Article Received: 23 January 2019 Article Accepted: 09 May 2019 Article Published: 10 July 2019

ABSTRACT

An effective management of information technology is integral to ensuring national security and by extension, national development in this digital age. As useful as information technology is, it also portend harmful effect on the national security if not properly harnessed and managed. Nigeria is today faced with diverse and increasing security issues such as, bloodshed, kidnapping, and terrorism among other social menace which are resultant effects of silent, but salient issue of information technology which has been inadequately harnessed and managed over the years. Although, Nigeria government have taken bold steps to address national security issues through combat approach, there still exist several unresolved issues bordering the country peaceful coexistence on one hand and effective Military operations though uncontrolled information technology on the other hand. The inevitable security issues leading to subsequent destruction of lives, properties and the environment calls for a holistic approach through effective use and control of information technology. In this light, this paper demonstrates the potential value and strength of information technology and management in ensuring sustainable national security with apt demonstration of social, moral, and organizational importance of security and the need to strategically coordinate and manage security efforts in order for security to unfold its beneficial potentials in Nigeria.

Keywords: *Information Technology, Information Management, National Security, Media and Sustainable Development.*

INTRODUCTION

The control and management of information technology is central to a successful warfare or maintaining a condition of peace in this digital age. A sustainable national development is a function of national security which is hinge on who controls and how the information technology is being controlled and managed per time. In the words of an American military strategist and theoretician John Boyd, "Machines do not fight wars". People do, and they use their minds and the destruction and distortion of the enemy's will to win and perception of reality through ambiguous posturing, and severing of the communication and information infrastructure should be the driving force in mental warfare" (Orovwuje, 2014). This, however, underscores the strategic role of the military and information technology and management in the war time. That is, a nation that has effective control and management of its information technology will have a good grip on its national security. This is true in the case of developed countries of the world in the global war against terrorism and its vices. For instance, shortly after the September 11 attack, United States established Homeland Security Institutional framework with its complex, colossal, multidimensional and highly-critical information infrastructure and expansive Database systems on Cyber security and Terrorism (Yakubu, 2006). Also, On April 13, 2013, America strategically deployed its security system to track down the Boston Marathon. Similarly, the ongoing global War on Terror being led by the United States is hinged on effective control of information technology. The world Power, US understood the advantage of having an effective control of information technology within her territory and maximizing it without compromise.

Information technology is a widely defined term that has several meanings across different sectors. Though, essentially, it is used as an umbrella term to refer to the use of communication devices (such as radio and cellular devices, satellite devices and channels, computers, amongst others) and utilities (programs) to manage information (acquisition, dissemination, processing, storage and retrieval). On the other hand, National Security could refer to a state of absence of everything and anything that could be a threat to peace, progress, development and tranquility

within a society (Ajijola, 2012). Information technology is a source and transmitter of information to the diverse society and remains the most essential medium of expression of feelings, ideals and other cultural promotions in the global world. It is on these significance relations and intelligent observers of the effects of the media on the masses have the assumption that it has enormous influence on humans lives, beliefs and opinions and its' critical views shape the national issues and political environment.

The increasing insecurity in Nigeria today which has become a national issue and concern for all is no doubt, a function of chain of factors which the state machinery has left unchecked for a long time. The insecurity posed by Criminals, terrorists, disgruntled employees, technical problems and many other issues are threatening the security and integrity of the nation, Nigeria. The parlance of insecurity in the country today is threatening to tear her apart and requires quick, adequate and a new approach to deal with the security challenges plaguing the nation. Apart from food insecurity, financial insecurity, terrorism, health insecurity and others, security failure has eaten deep into the fabrics of the country. The situation in Nigeria since the beginning of this decade in which dozens of militant groups emerged and challenged in the most violent form the authority of the Government; the growing level of urban crime including armed robbery, kidnappings, ritual killings, and cultism; the continuing erosion of the moral authority of religions in which people engage in acts in open defiance of their religious and moral teachings; the culture of impunity that characterizes public affairs; the corruption that is submerging the average Nigerian; and the collapsing social and political institutions in the country over the last few years, more than anything demand for quick (Mijah, 2007) this acrimonious row is being worsen by the Boko Haram insurgency, militants, Indigenous People of Biafra (IPOB) and the perceived negative reportage of the military engagement strategies with the terrorist, secessionism and also the unfounded notion that information technology is being used by the opposition party to heat up the polity. Given these, it would be observed that the to ensure a sustainable Nigeria there is a prime need to develop condition, create enabling environment, develop institutions and structures with the capacity to ensure economic growth, equitable distribution of national wealth, political stability and accountability. However, there is a daring need to critically rethink especially in this age of digitalization made possible through globalization, and improve on policy and institutional means of dealing with security concerns arising in the country.

It's against this increasing national insecurity that continue to threaten sustainable development in the nation that this paper try demonstrate the value and strength of information technology and management in ensuring sustainable national security. We realize the social, moral, and organizational importance of security and the need to coordinate and manage security efforts in order for security to unfold its beneficial potentials.

Conceptual Clarification

Winter (2000) in his remarks on Information, includes both electronic and physical information. The organizational structure must be capable of managing this information throughout the information lifecycle regardless of source or format (data, paper documents, electronic documents, audio, and video among others) for delivery through multiple channels that may include cell phones and web interfaces

According to Wikipedia, Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences. This sometimes involves those who have a stake in, or a right to that information. Management means the organization of and control over the structure, processing and delivery of information.

Information management embraces all the generic concepts of management, including: planning, organizing, structuring, processing, controlling, evaluation and reporting of information activities, all of which is needed in order to meet the needs of those with organizational roles or functions that depend on information (Bytheway, 2015). These generic concepts allow the information to be presented to the audience or the correct group of people. After individuals are able to put that information to use, it then gains more value. The Concept of National Security

The term "security" may be seen as a state of being protected from danger or anxiety. For a nation, security connotes conditions of peace, stability, order and progress. National security has been construed in different ways, each of which emphasized vital factors underlying ideals. Brennan (1961) holds that national security is the protection of national survival, while Ray (1987) says that national security is to be understood in terms of the desire and capacity for self-defence. Ochoche (1998) holds that national security focuses on the amassment of military armament, personnel and expenditure.

All the above definitions points to the understanding that national security has changed overtime. It was expanded to include international economics, long term goals of national development and reconciliation. They are very important for the security of any nation. With this approach, Asad (2007) says "that national security cannot be narrowed down to exclusively military term. Socio economic and cultural aspects, problems of development and modernization, and national integration should be deemed important in considering". Al-Marshat (1985) suggested that national security is more than territorial defence and should focus on the "Physical, social and psychological equality of life of a society and its members both in the domestic setting and within the large regional and global system".

According to Mathew (1989), Global development now suggests the need for another analogous broadening definition of national security to include resources, environmental and demographic issues. National security question involves a lot of issues. It practically touches on all spheres of human existence. A nation that is capable of protecting herself from harm equally enjoys immense capacity for enviable development. We may therefore posit that national security and national development are complementary and inseparable phenomena. They are mutually related. There can be security without real development and no development without security. It is vice-versa.

Information Technology and Management

In the following section of this paper we will explore how these critical ideas can be brought to bear on information management. This will lay the foundation for our strategic investigation into critical issues in information management. There has been very little, if any, research from a critical position that concentrates on questions of information management and national security. Siponen (2005) mentions crypto inquiry, which may be used to

point out flaws in systems but which, using the current definition of critical research, does not necessarily have a critical angle.

In the Webler, et al (1992) submission, a critical approach to risk management touches on related issues but is not identical to critical work on information technology. At the same veim, Siponen (2005) points out that critical studies of security would be desirable because of their potential to point out weaknesses in current thinking and because they have the greatest potential to take research forward. Backhouse, Hsu and Silva (2006) similarly underline the desirability of a critical approach to security standard development. The current paper fills this void in the information technology and management research literature.

Theoretical Framework

The media for as unit of information management for instance, can be used information to induce panic and reduce tension created by other sources, especially during the periods of insecurity like case of 'Operation Python Dance' by the Nigerian military in the South East Nigeria. The menace of forced inoculation which went through the entire South East and some parts of the South South was preceded by speculations in the social media that the Federal Government was out on a diabolical mission to inject people in some parts of the country with monkey pox in the guise of vaccination. It has been known to play crucial roles in reassuring, calming and in specific instances, directing people to areas of safety. In the light of this, the theoretical foundation of this paper is hinge on the spiral of silence theory. The theory is significant to studies such as it's endowed with the capacity in ensuring a peaceful atmosphere for humanity as both consists in media effects theories of mass communication.

The spiral of silence theory of the mass media was postulated by Elizabeth Noelle –Neumann whose initiative was predicated upon the ability of the mass media to influence public opinions in matters of public interest. According to Aina, the media can shape public opinion distribution by creating the impression that some of the opinions are not good for public consumption since those expressions and activities could lead to conflicts in human society. In order words, the resolve by individuals to comment on certain issues depends largely on the prevailing climate of opinions. The reason is that, in a situation of public interest that affects majority of the citizenry, will be down played and not given importance due to fear of isolation.

The usefulness of this theory is that the mass media criticizes the disdained behaviours which have negative influence on militarization. However, one critical aspect of national security is manifest through social media which tendencies are displayed towards ensuring a politically democratic order in which lives and properties are protected.

This development sometimes make critics say that in developing nations the electronic media are used more for entertainment than for national developmental purposes. For example, radio, which is adjudged the true mass medium in developing nations, is said to attract wide listenership more for its entertainment programmes than for its educative ones. In Nigeria, commercialization of government-owned electronic media has caused wedding and obituary to feature in news bulletins for a fee **(Bright, 2015).**

The Issues and Challenges of National Security and Information Technology Management in Nigeria

The information technology world has grown with its mixed impacts on daily life; its existence has become an integral part of living of the majority of mankind, not only in Nigeria, but also in other nations of the globe. Simply put no information, no knowledge and no knowledge, no power. The breakthrough in technology has created a new microcosmic world order that is highly networked, virtual and powerful; even inescapable by the larger, macrocosmic world. As information technology become more robust, diversified and advanced, the past decade has seen a preponderance of insecurity issues as in hacking,"419" scams, kidnappings and a host of other vices Hack attacks have taken very dynamic trends as the Hackers have assumed very determined skills, all made possible through breakthroughs in information technology. Some examples that stare us in the face include: Prostitution (Adult and Child), Drug Trafficking, Child Trafficking, Child Pornography, Rape, kidnappings and other forms of Sexual Crimes, amongst others.

In the same vein, the recent breakthroughs in Mobile Technology have come with both positive and negative implications for national security. Information, some of which are unverifiable and false, is now placed within reach of the fingers of both those who understand them (or for whom the information is intended) and those who know absolutely nothing about the (usually very potent) information they have access to. The social networking, E-mailing Short Messaging Service (SMS), have become very potent tools, even in the hands of the poor;. These have made the information dissemination to flow without any form of restrictions (Ajijola, 2010). In today Nigeria, geographical difference, distance barrier for criminals and terrorists is a thing of the past. From the comfort of the bed room, criminals can easily network, receive and send signals to any destination in the world. For instance, a recent research showed 2009 bombing of the Superscreen TV station in Lagos; the terrorist-linked bombings in the Northern and other parts of Nigeria in recent years; the bombing of the Twin Towers of the World Trade Centre in 2001 in the U.S.; or the festering sectarian (and religious) violence in various parts of the world and the recent pervasive nature of armed banditry in our societies; these all owe their sophistication and devastation to the unrestrained and negative deployment of both cellular and other communication devices and the Internet (Uwaya, 2011).

Social networking, such as, Whatsapp, Facebook among others has proved very strategically useful over the past decade and criminals and terrorists have found them very useful in perpetrating various dangerous crimes ranging from terrorism to kidnappings, robbery and rape. The social networking or media is widely covered and easily accessible to all: young and old: male and female; rich and poor Political gladiators have used it severally to galvanize supports, and negatively influence the masses writing and posting and sharing negating statements to cause political crises of diverse kinds in the nation Nigeria.. The proliferation of social media (Such as Facebook, Twitter, Whatsapp, et all) for instance, has growing implications for national security. Globally, social media is being used effectively by businesses, individuals, activists, criminals, and terrorists. Governments that harness its potential power can interact better with citizens and anticipate emerging issues (Cited in Drapeau and Wells, 2009).

Since the rise of the Internet in the early 1990s (Shirky, 2011), the world's networked population has grown from the low millions to the low billions. Since then and until now, social media have become a fact of life for civil

society worldwide, involving citizens, activists, nongovernmental organizations, telecommunications firms, software providers, governments et al. As the communications landscape gets denser, more complex, and more participatory, the networked population is gaining greater access to information, more opportunities to engage in public speech, and an enhanced ability to undertake collective action. These increased freedoms can help loosely coordinated public demand change.

Opinions are first transmitted by the media, and then they get echoed by friends, family members, and colleagues. It is in this second social step that political opinions are formed. This is the step in which the Internet in general, and social media in particular, can make a difference. As with the printing press, the Internet spreads not just media consumption but media production as well; it allows people to privately and publicly articulate and debate a lot of conflicting views. For political movements, one of the main forms of coordination is what the military calls "shared awareness," the ability of each member of a group to not only understand the situation at hand but also understand that everyone else does, too. Social media increase shared awareness by propagating messages through social networks (Shirky, 2011) For example, what do we make of organized and well-coordinated events leading to the Obama's electoral victory in 2008; Oscar Morales of Colombia starting a Facebook group against the revolutionary guerrilla group FARC, drawing over 1 million people from over 40 countries; Facebook Vs. Egyptian Government in April, 2008, where through social media a group had a protest of political dissent, and posted photos online of the violence that ensued. State security was taken by surprise by the number of participants. Surely, online social movements have changed the dynamics of political activism. Possibly as a result, Syria has recently blocked use of Facebook by its citizens.

Sadly, the 2008 report of Cyber Crimes Complaints from the Internet Crime Complaint Centre (IC3) – a body setup to investigate internet crimes – revealed that Nigeria is ranked Number Three (3) in the list of countries that have been mostly associated with Reported Cyber Crime Cases(Emmanuel and Ogu, 2014). These increasing cyber atrocities and compromise in National Security using Information technology can be traced and linked directly to unmonitored, poorly administered and unrestricted National Cyberspaces. This negligence has created ambience for criminals to commit cyber-crimes. In Nigeria today, Cyberspace has become a lawless zone where transmissions and communications that explicitly violate constitutional provisions and threaten peace and security are carried out with wanton neglect. With this world's new-age information dynamics, a national government, security agencies and its military authorities should give prominence to national cyberspaces, analyze the balance between security and sharing, and develop strategic method of monitoring the cyberspace as Telecommunication companies which are expected to launch a good cyberspace surveillance strategies are encumbered with profitmaking.

In the contemporary Nigerian state, where conflicts involve non-state actors and governments, experts believe that wars are not won in the field of battle but in the minds of men. Hence, the battle for the minds of the people becomes paramount for both parties to succeed. Non-state actors, which are mostly terrorists, use the media, especially the social media, to spread their ideologies, gain sympathy and acceptance, as well to recruit new members by propagating messages that appeal to the mind of the populace. In order to counter the terrorists

ideologies, states employ the same strategies to win the people to their side. They use trained personnel that are proficient in the use of social media and create messages aimed at winning the mind of the people and de-radicalize terrorists' converts.

In recent times, the Nigerian Military has been involved in internal security operations, primarily because of several security threats across the country, such as Boko Haram insurgency in the North east, Cattle rustling and armed bandits in the North west, secessionist agitation and armed robbery in the South east and militancy and oil bunkering in the south-south, that have overwhelm the Police and other security agencies. Furthermore, the Nigerian Army launched free medical outreach in Ovim, Isiukwuato Local Government Area of Abia State as an integral part of the ongoing Operation Python Dance II exercise in the South-East of the country. This exercise includes vaccination of children at home and in schools, giving out mosquito nets etc.

The Nigerian Army may have started this exercise in good faith but it was not well accepted by most parents in the south-eastern part of Nigeria. This vaccination or inoculation by the Army was perceived by most residents in Imo State, Anambra and some other South-East states as "another" attack by the military. According to George et al (2017), not all schools in Owerri, Imo State was thrown into state of bedlam. Herald News visited schools like Irete Secondary Technical School, Orogwe Secondary School and Ndegwu Secondary School all in Owerri-West LGA Imo State, but they were deserted as at 11am. No single soul was found in Ndegwu Secondary School. We also visited Emmanuel College and found out that they were dispersed. The school blamed their collapsed fence as the reason for their inability to control the students. A different case was witnessed in Holy Ghost College and Alvana Model School where students were relaxed and learnt undisturbed. Although, parents pressured to overpower the staff of the school to take their children away but the school authority stood their ground hoping to only release the students at the normal closing time. School administrators of Holy Ghost College and Alvana Model Secondary School believed that their students were safer in their care within the school hours. They felt uncomfortable releasing the students into the already confused society.

However, the exercise created fear in the minds of people as many parents rushed to schools, agitating for the release of their children and wards to them, to prevent them from receiving the rumored forceful vaccination of children by the military. The parents read negative meaning that the military were with the intention of killing their children. As a result of this, there were lots of scramble in some schools in the South Eastern states as students fled their schools and parents besieged schools demanding to pick their children and wards. Though the Federal Government later re-assured all parents, guardians and care-givers of globally confirmed safety, potency and effectiveness of all antigens in the National Immunization Schedule against vaccines preventable diseases in the country and the vaccination is free in all public health institutions. Overwhelmed by the widespread rumour, the Nigerian army released a statement urging the public to disregard rumours that its ongoing free medical outreach, especially in the South-East, was aimed at de-populating the zone. . He described as "silly and mischievous' publications trending on the social media alleging that the ongoing free medical services given to some communities in the zone were with a sinister motive of depopulating the region through the so-called `monkey pox

vaccination'. However, the damage has been done due to the fact that information is the key just as sensitization is the prime.

Another noticeable challenge that is creating haven for criminals in Nigeria is the lack of adequate, comprehensive record keeping. Nigeria doesn't have a database of her citizens, cannot lay a precise hold on the number of persons that constitute her citizenry. As at the time of this paper, there are no national efforts geared at achieving that. Everyone lives in uncertainty, fear and suspicion. The rate at which this portend harmful effect on national security propelled the Nigerian Communications Commission (NCC) to initiate a compulsory SIM (Subscriber Identity Module) Registration and SIM Verification processes and also by the drafting of the Lawful Interception of Communications Regulations being geared towards regularizing the mobile telephony and telecommunications industry in Nigeria for a better centralized management and efficient administration. Even at this, the true picture of what constitute the national citizenry is not known. In a situation of this nature, the national security is at risk. Thus explain why the nation Nigeria is plagued with diverse security issues and challenges because managing information technology starts with getting accurate number of those who have access to it.

Tackling National Security Issues through Information Technology and Management System in Nigeria

As earlier noted, the most common language that best describes Nigeria over two decades ago is insecurity. There are diverse security issues across the six geopolitical zones that made up the country. Kidnappings, suicide bombings, electoral crises, terrorism are few among the vices that constitute security threat and by implications, impeding sustainable national development. The breakthrough in information technology development which pushes for globalization has created ambience for such vices to thrive in atmosphere where its not effectively harnessed and managed for national security.

However, attempts to ensure a sustainable national security in the face of the growing network of information technology have been flawed with issues and hiccups over the years. Given the range of information management issues and the importance of security, it is not surprising that there are a number of ways in which information management can be integrated and managed in organizations. Information management goes beyond technical computer security (Nissenbaum, 2005). Frequent approaches to information management include the employment of risk management methods (Doherty & Fulford, 2006). It has been pointed out that such approaches lack flexibility required for different types of organizations (Baskerville & Siponen, 2002). The nature of information security threats may have changed significantly over the past thirty years, but the incidence of information security breaches remains stubbornly high (Dhillon, 2004).

In terms of policy, the information security policy is viewed as an increasingly important business document (Doherty and Fulford, 2005), which covers a broad set of security concerns (Rees et al, 2003).. More specifically, this document should 'set out the organization's approach to managing information security. The policy should be a working document that provides guidance on the 'means' of information security management, as well as the desired 'ends '. Moreover, the policy has an important role to play in emphasizing management's commitment to, and support for, information security. Consequently, there is a growing consensus within the literature that the security policy is uniquely well placed to proactively safeguard the availability and integrity of corporate

information resources (David, 2002). As Solms (2004) note, the information security policy is the 'heart and basis' of successful security management. Such documents would therefore lend themselves as suitable sources for empirical research in the area.

Despite these well established procedures, there remain a number of problems associated with current information management approaches. Many of these stem from the difficulty of adequately capturing and defining the concepts. One issue is the problem of inconsistency. Individuals' stated security preferences tend not to translate well into their observed behavior (Nikander & Karvonen, 2000). Users can furthermore be described as acting against their own best interests which renders appropriate provision of security problematic. (Landwehr et al 2001).

As the commonest information unit, the media (Social media and Mass media) is the greatest threat platform used by criminals in Nigeria. In the words of (Mogekwu 2005, p. 30). The media have long been characterized as a social force used either to the benefit or detriment of the society within which they operate. When used to promote justice, moral unity and harmony in society, they can act as facilitators of peace in time of crisis. However, they can also be used as instigators of conflict and destructive purpose. This position is absolutely true in Nigeria. Terrorists and kidnappers use the media to network, recruit members and discuss on any intended operations. Besides, most electoral crises in Nigeria are fueled through the media. It would take a concerted effort among stakeholders, civil society groups, corporate bodies and government institutions to join forces together to rid the country of the increasing terrorism and criminalities by building a controlled information network in the country.

Besides, a recent research on cybercrime conducted revealed that Nigeria is the most internet n fraudulent country in Africa. The same report stated that the giant of Africa is ranked third among others identified with cyber fraud and computer crime in the world (Izizoh, Anaziah, Okide & Okwarada ,2013). Due to the globalization of the world via information technology, access to government classified information has been enhanced, thereby posing great threat to national security. Although this menace is not limited to Nigeria but its increasing rate and disastrous effects on the nation calls for a strategic approach by the government to harness and manage the information technology to national advantage. there is a need to invest in and use intelligence services to detect and defeat or avoid threats and espionage, and to protect classified information that are integral to national security

To ensure a sustainable national security, security agencies must develop workforce and process capabilities that enable efficient, effective and secure information collection, storage, use and sharing. They need to take a collaborative, strategic and enterprise-wide approach to information management. To achieve effective information management, security agencies must develop a consolidated information management architecture—a layer of processes, functions, policies and solutions that ensure the effective and secure creation, collection, storage, communication, valuation, sharing and use of information. Effective information management architectures integrate disparate information, security, and content management capabilities and include law enforcement, administrative and technology work streams. Enterprise information systems are an integral part of effective information management architectures because they provide the IT services, data stores, standards, frameworks and processes required to support secure data and process interoperability across organizational boundaries. Security agencies may implement an information-management framework which provides a complete

model for information management and is designed to help them develop more effective information management architectures. Information management architecture is a layer of processes, functions, policies and solutions that ensure the effective and secure creation, collection, storage, communication, valuation, sharing and use of information. This framework divides information management into five highly-interrelated disciplines and each discipline has multiple components—the most important being processes, functions and technologies required to unlock the value of information. Although information is the first line of defense against crime, sharing it is never easy. Inter-agency or cross-jurisdictional involvement can decentralize critical data, and the lack of standardized technology platforms isolates it further. However, high performance can be achieved with information-sharing strategies that garner immediate results. From intranets, shared databases and call centers to wireless technology and Web-based portals, next-generation technology can be maximized to protect citizens through strong prevention and deterrence practices strong information management system should be able to prevent a devastating event and should be able to give intelligence alerts to security personnel. The coordination between agencies should be backed by a strong culture of information-sharing between central and state-level security agencies along with a robust governance system.

The earlier suggestion that there is a linear relationship between these two is problematic Security considerations can also come into conflict with other important values, such as free speech (Spinello, 2000). The situation is exacerbated by the fact that security measures can introduce new security vulnerabilities (Broucek and Turner, 2004). Furthermore, there are possible contradictions between security measures depending on the level of abstraction one chooses. High levels of individual technical security may translate to decreasing security on a national level.

RECOMMENDATION

- The federal government of Nigeria should gear efforts at initiating a national efforts at creating a database for individuals who constitute her citizenry
- The government should always train personnel, redesign and analyze latest information technology
- The security agencies should rely on effective information technology management strategy and they should be provided with the right technology available for surveillance.
- Devise information strategy for each security unit to enable them to collate, analyze and share data without restrictions
- Government must be true to its people-focused security agenda, seek to implement this agenda in a collective way, involving the public, the media and those other units of the society that have the capacity to provide relevant information for the achievement of national security goals
- Government must also make the legal and political atmosphere friendly to media operations and resist the temptation of making the media a laptop dog instead of a true watchdog.

- The military must also be strategic in their engagement with the media beyond news conferences and releases to more robust techniques of understanding the political slants and media representation in the area of operations and media ownership. The wide variety of non- traditional media should be explored to engage the enemy rather than open confrontation with the media in recent time.
- On its part, the media should avoid getting carried away by overstating negative news while under reporting positive developments.

CONCLUSION

There is a bold and truthful saying on the main page of the Nigerian Army website which says "If you build an Army of 100 lions and their leader is a dog, in any fight, the lions will die like a dog, but if you build an Army of 100 dogs and their leader is a lion, all dogs will fight like a lion." Without mincing words, this points to leadership, styles, approach, quality as well as its infectious effect on the people at large. The increasing menace of insecurity in Nigeria is a resultant effect of poor handling of silent, but salient issues like information technology in the nation. The recurring terrorism attacks and its likes are strengthened by their strong control and hold of good information network, and tackling them requires a strategic control and management of information technology in the nation. This can be achieved through collaborative efforts between the military and the national information unit like the media and others. The media for instance, has increasingly become an important agent in the fight against insurgents in recent years through their grip on the control information both in times of peace and war. Furthermore, the military means and objectives of winning the war against terrorism has changed dramatically, the media itself particularly the press has undergone some transformation in recent years. These developments cannot be under estimated. From 24 – hours rolling news stations, on-line media platforms and websites, the Nigerian discerning public and indeed the world have greater sources of information more than ever before, and the military in my view has a more complex task in information management and intelligence rather than clamping on the press. Therefore the military and the media must build an enduring partnership and consensus to address the new realities of war-reporting in the interest of national security

To achieve this, however, Nigeria government need economic development occasioned by social transformation and made possible through the deployment of all our human resources in order to tackle difficult human problems like threats to national security. We all constitute the human capital of this nation – all of us here present: the military authority, the police authority, the civil authority, the media and others. We've got no place else to call our own but our dear nation Nigeria, and if we can demonstrate sacrificial zeal to calm the tides of some evils in West African sub-region and in Africa as a whole, we can do it more in our home nation.

REFERENCES

Aina, Sina. Anatomy of Communication. Abeokuta: Julian Publishers, 2003.

Ajijola, "The role of ICT Deployment for National Security," in (vol 1). Kaduna, Nigerian Defence Academy Academy Press. 18(2), 39-55

Bright U (2015), "Media Criticism, Culture and Nollywood: Towards Achieving National Security Sustainability in Nigeria" Department of Theatre Arts Faculty of Arts, Niger Delta University (NDU)Wilberforce Island, Bayelsa State, Nigeria

Broucek, V. & Turner, P. 2004 "Intrusion Detection: Issues and Challenges in Evidence Acquisition," International Review of Law, Computers & Technology

Bytheway, A (2015), "Investing in Information: the Information Management Body of Knowledge", Geneva: Springer

Doherty, N. F. & Fulford, H. 2006. "Aligning the Information Security Policy with the Strategic Information Systems Plan," Computers & Security

Dusek, V. 2006. Philosophy of Technology: An Introduction . Oxford: Blackwell EC, Commission of the European Communities 2007. Towards a General Policy on the Fight Against Cyber Crime .

Emmanuel C. Ogu et al (2014), ICT And National Security in Developing and Underdeveloped Countries – The Good, The Bad and The Ugly: A Case Study of Nigeria's Cyberspace, International Journal of Computer Science and Information Technologies, Vol. 5 (4)

George O, Jane N and Felix I (2017), "Panic in South East schools over 'forced' army free Medicare"http://sunnewsonline.com/panic-in-south-east-schools-over-forced-army-free medicare/

Izizoh. A.N, Anaziah A.E, Okide S. O, Okwarada C.AP. (2013) Impacts Of Information And Communication Technology In The Nigerian Economy, International Journal of Engineering Research & Technology Vol. 2 Iss.1.

Mijah E. B (2007). Democracy, Internal Security & Challenges of internal Security in Nigeria

Mubaraka, C., Jirgi, I. M., & Nanyanci, P. L. (2013). Integrating ICT in Traffic Police Department in Uganda;Design and development of traffic case management system. Innovative systems design and engineering

Orovwuje SA (2014), "Military, media and national security" The Nation Newspaper http://thenationonlineng.net/military-media-and-national-security/

Schultze, U. & Leidner, D. 2002 "Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions," MIS Quarterly

Siponen, M. T. 2000a. "A Conceptual Foundation for Organizational Information Security Awareness," Information Management & Computer Security

Uwaya, J "Our National Security and the Raging ICT Revolution"(2011) [Online] Available: http://nigeriavillagesquare.com/articles/guest-articles/our-nationalsecurity-and-theragingict-revolution.html

Webler, T.; Rakel, H. & Ross, R.J.S. 1992. "A Critical Theoretic Look at Technical Risk Analysis," Industrial Crisis Quarterly

Winter, S.G (2000), "The satisficing principle in capability learning" Strategic Management Journal, 21(10-11),

Yakubu., (2006) Kaduna, Nigerian Defence Academy Academy Press. International Association of Emergency Managers, "Principles of Emergency Management," September 11, 2007, 4.