**APPLICATION OF ICT IN MILITARY**

**BY**

**IDRIS DALHATU**

**ST/CS/ND/19/304**

**BEING A SEMINAR PAPER**

**PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE**

**SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC, MUBI ADAMAWA STATE, NIGERIA**

**NOVEMBER, 2021**

**ABSTRACT**

*Information and communication technology became the all-round program that is applicable in all our day to day activities across the world. Basically, ICT is a phenomenal service that can lead to the enhancement of high multimedia services such as video, text, images and audio files. This paper will give rise to how ICT tools can be used to combat insecurity in Nigeria where a lot of application will be used in order to achieve the aims of this research. Insecurity is one of the biggest problems that a lot of countries are suffering from such as Nigeria. Specifically, IT will help enable the nation to identify potential threats, share information more readily, provide mechanisms to protect the Nation, and develop response capabilities.*

**INTRODUCTION**

ICT (Information and Communication Technology) is a widely defined term that has several meanings across umbrella term to refer to the use of communication different sectors. Though, essentially, it is used as an 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). In lay terms, 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).

Thus, ICT has consistently been proven a powerful double-edged sword with a capability for both overwhelming good and devastating evil, all depending on the skills and values of the user(s) in harnessing its powers in either or both directions. There is general agreement among historians that insecurity have been the core cause of bloodshed in Nigeria and the world at large (Anyu, 2007).

The inevitable security issues leading to subsequent destruction of lives, properties and the environment calls for a holistic approach through effective use of information technology (Anyu, 2007). Although Nigeria have taken bold steps to settle their insecurity issues through combat approach, there still exist several unresolved issues bordering the country peaceful coexistence on one hand and accurate mapping of contiguous areas using geospatial science and technology such as satellite Remote Sensing (RS), Geographic information Systems (GIS) and Global Navigational Satellite Systems (GNSS) on the other hand. In this paper, we trace the evolution of Nigeria security challenges possible causes of insecurity and methods of solving the challenges through using Information technology and compliance with laid down rules/treaties and the possible areas of collaborations in the areas of space science and technology (with reference to Nigeria space programme), culture and Politics (Imobhege, 2007).

Abu (2011), stated that “One of the most important features of the digital age is the use of new communications technologies to build digital citizen ships.

The state of insecurity in Nigeria today is no news to anyone and although it can have blamed on some factors that have been left unchecked for a long time by both the Government and people of Nigeria but the level 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 and lasting solutions that will at least reduce the security threats facing Nigeria today (Mijah, 2007).

National security threat has been a major issue for the government of Nigeria in recent years. Recently, Nigeria has been characterized with different turmoil ranging from human abduction, political mayhem, terrorism and bomb attacks. Governments have tried several methods in order to curb these menaces but all of them have been proved abortive. According to Philip Zelikow Executive Director of 9/11 Commission and now a Professor at the University of Virginia, USA, the most significant lessons learned from the 9/11 catastrophe is: “The United States of America would have done, before the 9/11 saga, most of the things (i.e.: reactionary measures taken) that we did post 9/11!” A valid example is the establishment of the Homeland Security Institutional framework with its complex, colossal, multidimensional and highly-critical information infrastructure and expansive Database systems on Cyber security and Terrorism. It is all foe public safety (Gale, 2001).

Nigeria is currently faced with a similar challenge –informed by the magnitude and complexities of the several bomb blast in various parts of Northern Nigeria. Would we have done some of the things we now intend to do – about 10 years ago?Would we have created a National Security Intelligence Database, adequately prepared with disaster recovery plans and mastered the related operational complexities before they stuck? 21st century Information clusters are dyna- mic knowledge architecture for developing Intelligent and security systems (Blakes, 2009).

The role of Technology and in particular, software systems in National Security Database Intelligence dynamics has therefore become a critical and significant component as well as a fundamental necessity for understanding e-security life-cycle. Also, it amplifies the needs and accelerated urgency for deploying strategies capable of protecting Critical National Information Infrastructure (CNII) with result-oriented and sustainable implementation process (Jeffrey, 2008).

**ADVANTAGES OF ICT IN MILITARY**

The following are the various advantages of using information technology in the military sector.

1. **Use of Smart weapons:** Looking into smart weapons, ICT has changed the way of entire defense industry in grand manner. Industry has produced dumb bombs previously and with the help of ICT defense industry produced smart weapons. These are very efficient and accuracy is very high. With the help of this the individuals are able to communicate much frequent and inform their weapon status to their commanders. If they require weapons very urgently based on situation in battlefield they can seek them very comfort to target their enemies and accurately destroy the target without creating any damages to surroundings (Imobhege, 2007). Examples of smart weapons are like air-to-air missiles that can target enemy’s aircrafts with speed. Another one is used in sea to find and identify whether enemy ship is can be destroyed with the help of vibrations like targeted one is military ship or civilian ship.



Figure 1: Smart weapons.

1. **Use of Robots:** Present, robots are being produced to replace human individuals in battlefield. These all are possible by the ICT and advancements taken place in that by artificial intelligence system for defense industry.



Figure 2: Military Robot for tactical operation

1. **When we observe network centric battlefield management**: This is a new approach and with the help of this, military can able to manage their battlefield with the use of ICT advantages. Using this, a military commander can monitor his army and decide whether he is stronger than the enemy’s line. The benefits from network-centric battlefield management are like observing military force position in battlefield and force of causalities and ammunition supply level (Mijah, 2007). Network-centric devices help in intra-troop communication improvement and a leader for his squad can identify and classify friendly armed forces and hostile enemy forces. These are possible with the advancements by ICT and wireless devices.
2. **Surveillance for real time combat**: Surveillance for real time combat is the extension for the previously discussed network centric battlefield management. In this the details will be sent to command center as feeds. Military forces are with well-equipped electronic devices to follow their commander orders. Superiority in air as well outer space is the greater advancement from ICT for defense industry and this facilitated defense industry to produce very high-end military equipment which are used by air forces across the world. There are lot of electronic devices exist in market with advancements in ICT components like interceptor jets, UAV’s and satellites for military to monitor targets continuously.
3. **Force multipliers**: The software is one which has greater advantages for defense industry. The above discussed equipment are nothing if there is no brain to control and think about it. Due to these army forces reached their capability optimally. To say in other way, with the introduction of ICT era in defense industry the focus of industry moved from hardware base force multipliers to software based force multipliers (Elaigwu, 2005). Most of defense industry companies have dedicated separate departments which are specialized in military for software development. This software involves in many hardware equipment like battlefield management system, long range radar and GPS and missile active guidance system etc.

In fact, if any company wants to enter in global defense industry, software development is the best option because of the scope that has by ICT. The contribution from them in military software development is very high.

**DISADVANTAGES OF ICT IN MILITARY**

The following are the various disadvantages of using information technology in the military sector.

1. Sharing of data
2. Global Position System (GPS)
3. Smart weapon
4. Bomb disposal

**CONCLUSION**

Some issues that are central to information technology and national security include Corruption, Inadequate research, lack of technological knowhow, inadequate fund and political instability. All these constitute a major source of insecurity in Nigeria.

It is quite glaring that information technology has a great role to play on national security in Nigeria.The growing importance of information technology presents not only new opportunities to benefit modern society, but also brings challenges to the approach and methodology of securing that society from outside attack.

To adequately address Nigerian security challenges, modern intelligence gathering devices mustbe acquired and deployed by security services, like the police, the SSS, the Army, the Navy, the Air Force andother Paramilitary. Surveillance system that can monitor most sensitive equipment and public places must be put in place.

Real time communication systems that will enable information sharing must be installed. Adequate scanning of imported goods using modern scanners that can detect weapons and other materials used in making bombs and explosives must be put in place. There is need for adequate border patrol and use of GIS and surveillance equipment to monitor people and weapon proliferations. There is need to ensure the loyalty of security agents because lack of loyalty can cause the leak of security information to agents of destabilization in the Country.

**RecomendationS**

The problem of insecurity in Nigeria has been further compounded by lack of technological knowhow majorly in the aspect of using information technology as a tool in tackling insecurity in Nigeria.

1. Government should invest more in the defence sector
2. Government and individual should focus more in Science and Technology related research
3. Military officers and other security agents should be adequately involved in Capacity building
4. The Government of Nigeria should continue in the fight against corruption
5. There should be proper collaboration between the information technology sector and the Defence and security sector.

**References**

Abu, S. (2011). *Understand what "national security" is and the importance of it in American government* retrieved November 13, 2021 from <http://www.enotes.com>

Ajijola, H. (2012). *The role of ICT Deployment for National Security*, Nigerian Defence Academy Press, Kaduna.

Anyu, J. (2007) *The International Court of Justice and Border-Conflict Resolution in Africa*: The Bakassi Peninsula Conflict. Mediterranean Quarterly.

Blakes, G. (2009*). Conference on International Boundaries and Boundary Conflict Resolutoon*, University of Durham, retrieved January 18, 2021 from <http://searchcio-midmarket.techtarget.com/definition/ICT>

Elaigwu. J. (2005). Crisis and Conflict Management in Nigeria, *International Journal of information technology, 2 (12),* 44-53.

Gale, C. (2001). New technologies for teaching and learning; challenges for higher learning institutions in developing counties”. *International Journal of Education and development using information and communication technology. 3(2),* 57-67.

Imobhege, A. (2007). *Doctrines for the threats of Internal in security*. Issue and Problems. Malthouse Press, Lagos.

Jeffrey, R. (2008). *War and anti-War: Survival at the Dawn of the 21st Century*, Warner Books, New York.

Mijah, E. (2007). Democracy, Internal Security & Challenges of internal Security in Nigeria. *International Journal of Computer Science Information Security, 9(9),* 812.