THEME:

THE ROLES OF INFORMATION AND COMMUNICATION TECHNOLOGY MANAGEMENT IN NATIONAL SECURITY AND SOCIO ECONMIC DEVELOPMENT IN NIGERIA

Abstract

Information and Communication Technologies (ICT) introduced in the second half of the last century have shaped substantially the mode of peoples' interaction, business process, entertainment and learning. ICT are encouraging globalization, exchange of information and the proliferation of cyber space. The benefits of using these technologies are immense and they are here to stay. Today, Information and Communication Technology (ICT) acquisition and implementation are facing a lot of problems. Considering the enormous benefits that are experienced in the impact of ICT in Nigeria Security and Civil Defence Corps (NSCDC), NSCDC still experience some obstacles or hindrances in the effective and efficient use of the ICT resources in combating crime. This includes the problem of insufficient data, due to lack of strategic use of ICT as resources tools in combating crime. Secondly, inadequate government funding of the NSCDC leading to lack of relevant materials and equipment needed in cyber threat combating. Additionally, the lacks of competent ICT personnel or technical team engaged in such critical and sensitive operations seem to be another threat to the security or crime combat mission. This research has been conducted to expose some of the inhibiting factors, and to ascertain the impact of ICT on national security with special focus on the Nigeria Security and Civil Defence Corps (NSCDC's) case. A hypothetic deductive methodology (quantitative approach) involving survey design, distribution, collation and computational analysis using, frequency distribution and percentage method, and Chi-Square; Discriminant Analyses using statistical packages such as SPSS. The results of such analysis would be discussed and interpreted in relation to the key issue of the research. The results of the analysis of the responses from the field work conducted reveal that the NSCDC do have the required ICT tools in combating crime, and that information gatherings do help the Corps in the actualization of their technological goals. The outcome of the research suggests from all indications, that using Nigeria Security Civil Defence Corp, FCT Command, Abuja as a study, ICT has tremendous impacts on security and fight against cybercrime. ICT has roles in the security of any nation. Impacts can be direct, through growth of the ICT sector and ICT-using industries, and indirect through multiplier effects.

Keywords: *Information and Communication Technology, Information Security, Cyber Security Issues, National Security*

INTRODUCTION

The development of any society to a large extent depends on the extent of the security of lives and properties of the citizens. A secured atmosphere will encourage intellectual minds who will be a great asset to Nation building; it will also guarantee an environment for the growth of infrastructural development. The growing erosion of internal security and responses from the populace and the Nigerian state raises some serious questions such as; can the security agencies and their strategy guarantee internal security? Do these agencies have proper Information Technology Infrastructure in place for the purpose of information gathering, sharing and dissemination? Do they have adequate surveillance equipment? These are some of the questions central to the issues addressed in this paper. Nigeria Security Challenges National security is important not only to the government, but to the nation as a whole. National security serves many purposes. First of all, the armed forces are a very important aspect of national security. The Federal Republic of Nigeria has a very strong military to help ensure that the nation stays safe, however Nigeria's security concerns and threat perceptions emanated from many quarters, these includes the threat of extreme Islamic sects like Boko Haram, high level of unemployed youths, Militia from the oil rich Niger delta, ritual killings, the widening economic gap between the poor and the rich, influx of illegal migrants from the neighboring countries, emergence of political and regional thugs, and the collapse of the justice system . In addition, when threats are directed at the country there is an attempt to keep these threats isolated. National security is also concerned with emergency preparedness among many other things.

Background of the Study

Information and Communication Technology (ICT) 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).

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.

Approach to emergency management: These include:

Preparedness: Mobilizing and preparing the campus response to emergencies, from the development of emergency response plans and the procurement of supplies to educating the campus community about procedures for disaster response

Mitigation and prevention: Taking steps to reduce or prevent the possibility of disaster on campus, from identifying and assessing risk to putting preventative measures in place to reduce the risk occurrence

Response: The way that a campus reacts to disaster, including crisis communication and the treatment and protection of key assets, from university students and personnel to critical information systems and university property

Recovery: The timely resumption of standard operating procedures on campus, moving from "disaster" mode to "normal" mode through treatment, rebuilding, reorganization, and recovery.

All the above measures must be employed in addressing security issues in most public places. All emergency management, as defined by IAEM, must be applied by the Nigerian security authorities:

Comprehensive: Taking into account the full range of hazards and societies vulnerabilities while preparing a response that encompasses all assets (cyber, human, and physical) and members of the society / community.

Progressive: Anticipating new and emerging threats and securing the society and community against them.

Risk-driven: Rooted in sound principles of risk and impact assessment and identification

Integrated: Considering all members society and surrounding communities, from federal response agencies and local law enforcement to society police and IT

Collaborative: Cultivating a sense of trust, respect, and responsibility among all parties

Coordinated: Providing a safe, efficient, and well-maneuvered response to disaster and recovery.

Flexible: Allowing for creativity and innovation when established responses may fail or fall short of needs and expectations

Professional: Relying on a knowledge-based approach to research and planning.

Effective Emergency Management are:

1. Relevant players understand their roles in advance and execute accordingly.
2. Crisis communications are clear, consistent, and well received.
3. Life and property are preserved to the greatest extent possible.
4. Response plans are easily accessible, appropriate, and updated.
5. Critical technologies work without delay or interruption.
6. Society transitions from "crisis" to "normal" in a timely fashion.

The Country image is maintained in the eyes of internal and external communities.

Emerging Opportunities for Security Management

The integration of information technology and emergency management presents significant opportunities for innovation in the way to assess, manage, and respond to security challenges. Most technologies today are increasingly mobile, highly integrated, and inherently flexible. From social networking sites to geospatial imaging, the society today can take advantage of emerging tools to address critical security needs. (An EDUCAUSE White Paper, 2008)

Emergency Communication Systems

Emergency notification systems are Vendor applications that offer a plethora of opt-in services that can push emergency messages to cell phones via text messages, e-mail accounts, instant message accounts, or college or university voicemail systems. This system can help the Nigeria Security system respond to distress call from citizens. The most frequently cited technological answers to emergency notification system according to (Young, 2008), are Sirens, digital signage in common spaces and classroom buildings, notification systems that include both emails and text messages, and automatic messaging to classroom projectors and alarm systems.

GPS Technology

GPS-enabled devices can also help citizens signal for help when emergency situations arise. For example cell phones with Rave Guardian software, can activate a timer on their device when they would like surveillance from the police. On a University campus for example "student stepping outside the library at night, might activate the system while crossing campus. If the timer is not deactivated within a given time frame, authorities can use GPS technology to track

the student's location. Students can also press a panic button, alerting officials that they may be in trouble and broadcasting the specific coordinates of their position" (An EDUCAUSE White Paper; 2008).

Social Networking

Tools To reach members of the society who are constantly connected to the Web and actively creating and sharing content in their own time, security agencies should be turning to familiar social networking tools to share news and strategies for community security. Social networking sites like Facebook and MySpace will usually allow communities to create pages that store information about security plans, emergency procedures, and community events. The widespread popularity of networks like YouTube and iTunes can create opportunities for security agencies to educate through quick, entertaining videos and podcasts; these can easily be shared and stored.

Virtual Emergency Operations Centers

Physical emergency-operation centers (EOCs) can be used as a hub of community response in times of emergency. Communities can consider supplementing physical locations with virtual EOCs, these can coordinate response teams across geographic areas. It is noted that a virtual EOC dashboard can store and integrate unit response plans, incident reports, and operational reports from a variety of community agencies. A single user can access the virtual EOC to send communications through various channels to relevant players. In cases when the physical communities are unreachable or unsafe, the virtual EOC provides a safe and accessible alternative to coordinate groups across the wider community (An EDUCAUSE White Paper; 2008).

Intelligent Monitoring

Important buildings and business areas in Nigeria must turn to using new advances in intelligent monitoring, from biometrics and speech-recognition software to intelligent video and swipe-card access to such buildings. These must be done by striking a balance between security and openness, personal freedoms and reasonable expectations of privacy must be maintained.

Data Mining and Database Tracking

Weeks after the shootings at Virginia Tech, It is noted that " campus administrators were criticized for failing to heed potential warning signs during Seung-Hui Cho's time at the university, particularly a history of mental illness and a faculty member's request that Cho seek counseling." One of the issues that came up after the shootings is whether predictive modeling, aided through data mining software and other actuarial tools, offers some promise for preventing campus violence or suicide in colleges and universities. Many believe that the ability to predict violence is a nebulous process. Being able to turn to databases to share information between institutions will also be very helpful. The report by EDUCAUSE White Paper (2008), also indicated that "After two separate incidents in 2004 at the University of North Carolina Wilmington in which students were murdered by other students, officials at the UNC system's 16 campuses began feeding suspension and expulsion data into a shared database, allowing schools to check to see if a potential applicant had a violent history at another university. The 2004 murders were not connected, but both assailants concealed past offenses from school officials." (Cox, 2007)

Information Sharing

One of the most frequent barriers to effective emergency management generally is a lack of communication between security agencies. Greater communication might include sharing case studies that showcase best practices or offering open solutions to the society needs on security issues. The government must encourage information sharing and open dialogue between all the security agencies in the society. For example all personnel in the agencies must have e-mail addresses and subscribe to a discussion group where they can chat and share ideas real time online.

Information Technology and National Security

Information technology (IT), as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer based information systems, particularly software applications and computer hardware." (enotes.com, 2011). IT deals with the use of electronic computers and computer software to convert, store, protect process, transmit, and securely retrieve information. Today, the term

information has ballooned to encompass many aspects of computing and technology, and the term has become very recognizable. IT professionals perform a variety of duties that range from installing applications to designing complex computer networks and information databases. A few of the duties that IT professionals perform may include data management, networking, engineering computer hardware, database and software design, as well as the management and administration of entire systems. Information technology (IT) will play a critical role in strengthening Nigeria's National security against potential future attacks. 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.

Statement of Problem

Since the advent of Information Technology, it is assumed to have been of greater advantages than the disadvantages most especially in the area of Security, even at that the Security situation of Nigeria is getting deteriorated and more complicated by the day. The major challenges of security in Nigeria include: Terrorism by the boko haram in the Northern Nigeria, Kidnapping in the Southern part of Nigeria, armed robbery, the most recent pipeline vandalisation caused by some Militant group known as the Niger Delta Avengers in the South-South region of the country and Herdsmen killings in some part of the country. Therefore, the question this AIMP research is out to answer is: how can Information technology impact positively on National Security in Nigeria?

Objectives of the Study

1. To determine the relationship between Information Technology and National Security;
2. To find out the various ways in which Information Technology can impact positively on National security.
3. To find out reasons why Information Technology has not been able to help in achieving full National Security in Nigeria; and
4. To determine how National Security can be achieved through Information Technology and Communication Technology Management

Scope of Study

The essence of this research work is to primarily study the role of Information Technology in National Security and Socio Economic Development. The research intends to focus on Nigeria's security situation and how AIMP can help.

Conceptual Clarifications and Literature Review

We shall clarify some concepts and review some literature with regards to developing the subject in Nigeria:

National Security

National security, means "security from threats or attacks from people, organizations or countries that are impact the wellbeing of a nation and its citizen as a whole rather than of any specific individuals or within the nation. Such threats and attacks are usually directed at harming the lives of people and property. However, this does not rule out other illegal acts. National security is a concept that a government, along with its parliaments, should protect the state and its citizens against all kind of "national" crises through a variety of power projections, such as political power, diplomacy, economic power, military might, and so on.

Information technology

This is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

Nigeria Security Challenges

National security is important not only to the government, but to the nation as a whole. National security serves many purposes. First of all, the armed forces are a very important aspect of national security. The Federal Republic of Nigeria has a very strong military to help ensure that the nation stays safe and the citizens well secured, however Nigeria's security concerns and threat perceptions emanated from many quarters, these includes the threat of sects like Boko Haram, high level of unemployed youths, Militant from the oil rich Niger delta, ritual killings and kidnappings, the high rate of inequality, influx of illegal migrants from the neighboring

countries, emergence of political and regional thugs, and the collapse of the justice system . In addition, when threats are directed at the country there is an attempt to keep these threats isolated.

Some Security Challenges in Nigeria

• Poverty and unemployment • Insurgences – Boko haram, militants, religious or ethnic wars • Insecurity of lives – kidnapping, armed robbery, ritual killings • Corruption – Rigging of election, fake licenses, etc. • Theft – Oil pipeline, public funds or piracy • Information security – defacing government websites, theft of critical data, Denial of Service attacks • Insider threats - Moles within security agencies, disgruntled employees • Over-reliance on foreign technology • Inadequate regulations: e.g. cyber security and the most recent • Farmers/Herdsmen clashes.

Emerging Opportunities for Security Management

The integration of information technology and emergency management presents significant opportunities for innovation in the way to assess, manage, and respond to security challenges. Most technologies today are increasingly mobile, highly integrated, and inherently flexible. From social networking sites to geospatial imaging, the society today can take advantage of emerging tools to address critical security needs.

GPS technology

GPS-enabled devices can also help citizens signal for help when emergency situations arise. For example cell phones with Rave Guardian software, can activate a timer on their device when they would like surveillance from the police.

Social Networking Tools

To reach members of the society who are constantly connected to the Web and actively creating and sharing content in their own time, security agencies should be turning to familiar social networking tools to share news and strategies for community security. opportunities for security

agencies to educate through quick, entertaining videos and podcasts, these can easily be shared and stored. Members of the society are encouraged to become "friends" with security agents on Facebook and MySpace, this can create an alternate pathway for pushing information to the wider community. Facebook and MySpace Allow members of the community to add their own commentary through "on the scene" reporting, sharing messages with security agents.

Data Mining and Database Tracking

One of the most frequent barriers to effective emergency management generally is a lack of communication between security agencies. Greater communication might include sharing case studies that showcase best practices or offering open solutions to the society needs on security issues. The government must encourage information sharing and open dialogue between all the security agencies in the society. For example all personnel in the agencies must have e-mail addresses and subscribe to a discussion group where they can chat and share ideas real time online.

Social Networking Tools

To reach members of the society who are constantly connected to the Web and actively creating and sharing content in their own time, security agencies should be turning to familiar social networking tools to share news and strategies for community security. Social networking sites like Facebook and MySpace will usually allow communities to create pages that store information about security plans, emergency procedures, and community events. The widespread popularity of networks like YouTube can create opportunities for security agencies to educate through quick, entertaining videos and podcasts, these can easily be shared and stored. Members of the society are encouraged to become "friends" with security agents on Facebook and MySpace, this can create an alternate pathway for pushing information to the wider community. Facebook and MySpace Allow members of the community to add their own commentary through "on the scene" reporting, sharing messages with security agents.

Methodology

There are diverse set of people in Nigeria both the Young and old, unemployed and employed, students and so also different states and geopolitical zones Using the simple random sampling

technique, six different offices were visited which include Federal Ministry of Defense, Federal Ministry of Science and Technology, National Defense College, Defense Headquarters, the Police Force headquarters and National Information Technology Development Agency (NITDA). Using the purposive sampling technique, the researcher purposively selected a sample size of 120 respondents from the five offices. Each offices contributed 20 sample sizes Therefore, the sample size for the study were 120 respondents study were 120 respondents. Data was collected using the questionnaire which the researcher administered face to face to the respondents. Out of 150 copies of questionnaire distributed to the respondents, 120 copies were retrieved. This represented a response rate of 80%.

Summary of Findings

The findings showed that:

1. A great number of the officers in the Nigerian military and other security agencies believe IT can be of great impact in National Security so therefore there is a great relationship between Information technology and National security.
2. The reasons why IT has not really been able to impact in National security include: Corruption. Inadequate research, lack of technological knowhow, inadequate fund and political instability.
3. IT has been of 97.5% impact on Nigeria's National Security.
4. IT can improve National security through the use of GPS Technology, CCTV, Social networks, intelligent gathering, Smart weapons, Data mining and data base tracking.

Recommendation

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. • Hence, some recommendations were derived from this study: • Government should invest more in the defense sector • Government and individual should focus more in Science and Technology related research • Military officers and other security agents should be adequately involved in Capacity building • The Government of Nigeria should continue in the fight against corruption • There should be proper collaboration between the information technology sector and the defense and security sector.

CONCLUSION

To adequately address Nigerian security challenges, modern intelligence gathering devices must be acquired and deployed by security services, like the police, the SSS, the Army, the Navy, the Air Force and other Para - military . 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

References

1. Ajijola, "The role of ICT Deployment for National Security," in (vol 1). Kaduna, Nigerian Defense Academy Press. 18(2), 39-55. Accessed 10/10/2012.
2. Anyu, J.N. (2007) The International Court of Justice and Border-Conflict Resolution in Africa: The Bakassi Peninsula Conflict. Mediterranean Quarterly.
3. Blakes, G. (1989) Conference on International Boundaries and Boundary Conflict Resolution, University of Durham, 15-17 July, 1989. http://searchcio-mid market.techtarget.com/ definition/ICT.
4. E-Note.com (2011). Understand what "national security" is and the importance of it in American government http://www.enotes.com Retrieved on 13/9/2011.
5. Abu. S. (2011). Anarchy in the Land. Today's Challenge. Vol 6 No. 8. and Sustainable Development in Africa
6. Elaigwu. J. I (2005). Crisis and Conflict Management in Nigeria Since 1980.
7. The Library of Congress (2011) Nigeria National Security Issues and Perceptions: The a Library of Congress Country Studies; CIA World Factbook. Retrieved on 13/9/2011.
8. An EDUCAUSE White Paper. (2008). The Role of IT in Campus Security and Emergency Management. Retrieve from http://creativecommons.org/licenses/ by-nc-sa/3.0/.
9. Cox J. (2007). After Virginia Tech, Security Firms Ramp Up. CNN.com, April 26, 2007,
10. Imobhege T A (1992). Doctrines for the threats of Internal in security. In A. Ekoko and M Vogt (Eds). Nigerian Defence Policy: Issue and Problems. Lagos, Malthouse Press. The Role of Information Technology in National Security: "A Case Study of Nigeria"
11. Mijah E. B (2007). Democracy, Internal Security & Challenges of internal Security in Nigeria.