International and Public Affairs
2018; 2(3): 48-61
http://www.sciencepublishinggroup.com/j/ipa
doi: 10.11648/j.ipa.20180203.11
ISSN: 2640-4184 (Print); ISSN: 2640-4192 (Online)

The Impact of ICT on National Security: A Case of Nigeria Security and Civil Defence Corps

Chinedu Paschal Uchenna, Okeke Chukwuemeka, Onyeukwu Chukwuka

School of Science and Technology, National Open University of Nigeria (NOUN), Abuja Model Study Centre, Abuja, Nigeria

Email address:

puchinedu@yahoo.com (C. P. Uchenna), emeka5638@gmail.com (O. Chukwuemeka), emmanuelpeter8@gmail.com (O. Chukwuka)

To cite this article:

Chinedu Paschal Uchenna, Okeke Chukwuemeka, Onyeukwu Chukwuka. The Impact of ICT on National Security: A Case of Nigeria Security and Civil Defence Corps. *International and Public Affairs*. Vol. 2, No. 3, 2018, pp. 48-61. doi: 10.11648/j.ipa.20180203.11

Received: October 2, 2018; **Accepted**: October 18, 2018; **Published**: November 9, 2018

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

1. Introduction

Globally, internet and computer-based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activities, and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. The new boundaries, which are manifested in the monitor screens, firewalls, passwords, intruder detection, and virus busters, have created new personalities, groups, organizations, and other new forms of social, economic, and political groupings in the cyber world of bits. Traditional border-based law making and law enforcing authorities find this new environment of cyber boundaries very challenging [1].

The use or misuse of the internet as a medium of communication may in some situations lead to direct damage to real physical society. Non-imposition of taxes on online transactions may have its destructive effect on physical businesses, and also government revenues. Terrorists may also make use of the web to create conspiracies and violence. Wide and free sharing of ideologies, beliefs, convictions, and opinions between different cultures might cause physical and

emotional stress and confusion that might lead to physical violence.

1.1. Statement of Problem

Information technology is impacting all walks of life all over the world. ICT developments have made possible a transition in information storage, processing, and dissemination, from paper to virtual and from atoms to bits, which are now setting new standards of speed, efficiency, and accuracy in human activities. Computerized databases are extensively used to store all sorts of confidential data of political, social, economic or personal nature to support human activities and bringing various benefits to the society. However, the rapid development of ICT globally also has led to the growth of new forms of national and transnational crimes. These crimes have virtually no boundaries and may affect any country across the globe. Thus, there is a need for awareness, policy formation, and enactment of necessary legislation in all countries for the prevention of computer related crime. This research his been conducted to expose some of the inhibiting factors that are hindering the impact of ICT on national security using Nigeria Security and Civil Defence Corps as a case study. Till date, the security organization has been plagued with problem of insufficient data, as the Nigeria Security and Civil Defence Corps have not yet grasped the idea of using information resources tools in combating. Coupled to this, inadequate funding by the government nationwide has further given room for inadequate materials and equipment used by the NSCDC in combating crime. Further to this, include the lacks of competent ICT personnel or technical team engaged in the security or crime combat mission. To this end, the research is concern to ascertain the impact of ICT on national security, and as such quarries on the level of computerization in Nigeria Security and Civil Defence Corps; the skillfulness and knowledgeability of the NSCDC staff in the use of ICT resources; the usefulness of Information gathering, and the challenges associated with the application of ICT to combat crime by NSCDC.

1.2. Aim and Objectives

The aim of the study is to investigate into the Impact of Information and Communication Technology (ICT) on national security using Nigeria Security and Civil Defence Corps, FCT Command as a case study.

Supposedly, the study will seek to know the followings:

1. To examine the level of computerization in Nigeria Security and Civil Defence Corps.
2. To determine how skillful and knowledgeable the staff are in the use of Information and Communication Technology resources.
3. To ascertain the usefulness of Information gathering to Nigeria Security and Civil Defence Corps.
4. To determine the challenges associated with the application of Information and Communication Technology to combat crime by Nigeria Security and Civil Defence Corps.

1.3. Research Questions

As a research question, the research seeks to answer what the impacts of information and communication technology on security at the Nigeria Security and Civil Defence Corps (NSCDC) are. The study will answer the following research questions:

1. Does NSCDC have the Information and Communication Technology tools in combating crime?
2. What is the usefulness of information gathering to NSCDC?
3. Does the staff of NSCDC FCT Command have the required knowledge and skills in using ICT resources?
4. What are the factors militating against the application of ICT in NSCDCs?

1.4. Hypotheses

The following hypotheses have been formulated for testing:

1.4.1. Hypotheses 1

H^0: NSCDC does not have the required ICT tools in combating crime

H^1: NSCDC do have the required ICT tools in combating crime

1.4.2. Hypotheses 2

H^0: Information gathering does not help NSCDC

H^1: Information gathering do help NSCDC

1.5. Brief History of Nigeria Security and Civil Defence Corps

The Nigeria Security and Civil Defence Corps (NSCDC) is a Para-military agency of the Federal Republic of Nigeria that is commissioned to provide measures against threat and any form of attack or disaster against the nation and its citizenry. The Corps is statutorily empowered by lay Act No. of 2003 and amended by Act 6 of 4th June 2007.

The Corps is empowered to institute legal proceedings by or in the name of the Attorney General of the Federation in accordance with provision of the constitution of the Federal Republic of Nigeria against any person or persons suspected to have committed an offence, maintain an armed squad in order to bear fire arms among others to strengthen the corps in the discharge of its statutory duties.

The Nigeria Security and Civil Defence was first introduced in May 1967 during the Nigerian Civil War within the then Federal Capital Territory of Lagos for the purpose of sensitization and protection of the civil populace. It was then known as Lagos Civil Defence Committee.

It later metamorphosed into the present-day Nigeria Security and Civil Defence Corps in 1970. On inception the Corps had the objective of carrying out some educational and enlightenment campaigns in and around the Federal Capital Territory of Lagos to sensitize members of the civil populace on enemy attacks and how to save them from danger as most

Nigerian living in and around Lagos territory had little or no knowledge about war and its implications. This was done through electronic and print media on how to guide themselves during air raids, bomb attacks, identify bomb and how to dive into trenches during bomb blast.

In 1984, the Corps was transformed into a National security outfit and the addition of special functions by the Federal Government and on the 28th of June 2003, an Act to give statutory backing to the NSCDC passed by the National Assembly was signed into law by Chief Olusegun Obasanjo, GCFR, the former president and commander in chief of the Armed Forces, Federal Republic of Nigeria. These functions include: have power to arrest with or without a warrant, detain, investigate and institute legal proceedings by or in the name of the power of the Attorney General of the Federation, monitor the activities of religious bodies and trade union, monitor, investigate and take every necessary step to forestall any planned act of terrorism, provide intelligence information to the ministry on matters relating to crime control generally, riot, disorder etc. [2].

The following are the NSCDC Technology Goals:

1. Use technology to facilitate access to Corp's commercial and non-commercial information to authorized persons. Legitimate access.
2. To increase NSCDC revenue via ICT
3. The Corps to ensure regular training of ICT professionals
4. Provide support for CNS/ATM operations
5. Co-ordinate information communications technology at both the headquarters and outstations
6. Virtual community: Use technology to foster improved communication and information dissemination.
7. Staff will be efficient and effective in the use of all Agency-supplied information technology.
8. NSCDC information shall be secure and accurate and Data is collected and entered once
9. Timely and accurate communication between HQ, departments, outstations and personnel.
10. The Corps will use technology for Just –in- Time service delivery
11. Develop both knowledge and information workers
12. Use technology to automate its various processes
13. Gain appropriate returns on investment from its technology investment.
14. Use web-based technologies and processes for its security operations
15. Reduce Total Cost of Ownership
16. Provision of more Personnel's for ICT department.
17. Technical Support: Provide high quality technology support for all ICT based/driven CNS/ATM systems and management/financial services
18. Make optimum use of the infrastructure to achieve desired result.
19. Computer centre: Provide and support computer centre to meet personnel and other training user needs.
20. Corporate social responsibility via information communications technology.

The deployment of information communications technology is characterized by both a strong service orientation and a readiness to respond to a rapidly changing security environment.

2. ICT and Security

Information and Communication Technologies (ICT) introduced in the second half of the last century have shaped substantially the human interact with one another, business activities, 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. This has become obvious in this era of digital revolution when every of man's day to day activities are more dependent on such technologies and their by-products. Furthermore, these technologies have matured developing into a range of dedicated niche domains such as, networking, mobile communications, wireless communications and satellite broadcasting and so on. However, alongside benefits and opportunities a broad range of issues and drawbacks have limited to some extent full extraction of benefits from ICT use.

One of the main issues with ICT today is security. The last twenty years have witnessed the flourishing of a myriad of electronic attacks, malware, vulnerabilities and intrusions in the domain of information and communication technologies. According to Bruce Schneier, a well-known cryptographer, this is mainly due to the availability of attacking tools, automation and action at distance [3]. It is worth mentioning also that ICT security issues are not encountered only in the cyber space, but their impact is more noticeable and considerable in this domain. There are at least five distinct problem areas where security related issues are currently impacting in a negative way in ICT. These areas are: lack of security awareness and training, operating system design and security, open source issues, design complexity and multiple layer approach [4].

2.1. Lack of Security Awareness and Training

This is perhaps the most concerning and often overlooked issue, with serious implications on ICT infrastructures. In December 2007, a government wide data security review revealed nine NHS trusts in England had lost the medical records of hundreds of thousands of patients [5]. Also, in 2007 twelve British banks (including HBOS, Alliance & Leicester, Royal Bank of Scotland, Natwest, Barclays, and Nationwide) were named and shamed for failing to dispose electronic data regarding their customers properly [5]. Other episodes include the disappearance of top-secret electronic information, by Home Office or security services officials in Britain. CD, USB or Laptops containing very sensitive data were stolen, jeopardizing the lives of thousands of people. These facts demonstrate the lack of security awareness and training by some of the top governmental organizations or financial operators in the country. If this is the situation with top government bodies, then imagine what is happening with

the private sector, small enterprises or individuals.

Likewise, training is another pungent issue amongst network administrators and technical staff that are in charge of ICT infrastructure and security. Because of a variety of factors, including lack of funding, awareness or support from top management, these people lack training and often fail to deal adequately with security issues. On the other hand, the situation gets worst by the fact that ICT is evolving very fast and in different directions. It is difficult to keep up to date with these changes; therefore, a certain degree of commitment and dedication is required to follow the progress. It is relatively easily to demonstrate with facts the above statements above the lack of training and awareness by the above-mentioned professionals. Let us examine the case of zone transfers in some of UK academic institutions.

Lack of Security awareness and training is likely to influence ICT in the future due to a variety of reasons. First of all, the impact of digital security compromises and vulnerabilities will influence financially ICT used in businesses, government or other enterprises. Secondly, reputation damages will discourage customers to use ICT based businesses. On-line shopping for instance will not flourish in the future if the problem of card fraud or other e-commerce security issues are not dealt with. Besides, training staff responsible for security will prove to be a difficult task, simply because technology is changing so fast in many directions.

2.2. Operating System Design and Security

An operating system is a program or set of programs that serve as an intermediate layer between computer hardware and software applications. Various operating systems are in use today to satisfy the ever-changing customer demands; nevertheless, the most widespread operating systems are: Microsoft Windows, Linux/Unix and Macintosh.

Windows are mostly used as personal computers, Linux/Unix are mainly open source while Apple Macs are often used for graphic designs or other specialist applications. Irrespective of their application or use all operating systems up to date have been subject to security compromises or likewise failures. It is a fact that the majority of hacking tools, viruses, worms or Trojan horses are written for Windows, but this is merely due to the fact that Windows occupy almost 90% of the global market. Gantz et al [6] argued that Microsoft plan to release a new operating system in October 2009 called Windows 7. It was estimated that only within the period 2009-2010, 177 million units was to be shipped; while 7 million people employed in ICT around the world were anticipated to be using it. For this reason, Microsoft Windows OS will be the main focus of study.

Security is the main problem that Windows operating systems are facing since their introduction. Lack of vision from its developers regarding security is probably the main reason behind this issue. The first windows were designed to be simple and productive but not very secure. Although new operating systems version were introduced almost 5-10 years the same issues with security persisted. In my opinion, because of market pressure and product development circles it was almost impossible for Microsoft to totally change their operating system approach; instead they continued to build on top of each previous model. Unfortunately, their operating systems are still vulnerable affecting significantly ICT applications worldwide.

To understand the impact of operating system vulnerabilities on ICT suffice to look at the case of "SQL slammer', a worm released on the web in 2003 (Forte, 2003). Slammer, also known as "SQL hell", is a worm that affected Microsoft Windows operating systems in January 2003 affecting within ten minutes 75 thousand machines worldwide. Slammer exploited vulnerability in SQL server and desktop engine slowing down communications and affecting businesses financially worldwide. Following this incident several modified slammer versions were released online. This is not an isolated episode that demonstrates the lack of security vision and poor operating system design. Viruses and worms like Melissa, code red, sasser, nimda, donut, spida or slapper have also impacted information communication telecommunications globally. In 2007 Computer Economics, a well-known research company conducted a research on the impact of the malware globally estimating a $ 13 billion in financial losses in 2006 only [7]. It is quite obvious how ICT and global communications are affected by malware which attributes its success to operating system vulnerabilities.

How Microsoft reacts to malware threats? The magic word is releasing patches or services packs. Although, it looks like this is the right approach to this problem it does eradicate the problem and provide temporarily relief from threats. A holistic approach to deal with the root of the problem not with-it consequences is needed. As a matter of fact, operating system patches manage to avoid the threat temporarily, since what they usually do is a mere change of names or locations of important operating system files used by malware. In other occasions Microsoft has even discontinued shipping certain programs with its operating systems as a security measure against malware, therefore not dealing with the main problems: design and security.

A quick assessment of the most commonly used versions of the Microsoft Windows: In 2007, Microsoft released officially to the public Windows Vista and also the later release of Window seven in October 2009. Although, the graphical user interfaces look impressive, both operating systems are still vulnerable to malware or system hacking. A very simple example is the 'the sticky key backdoor', one of Vista's vulnerabilities. Vinoo Thomas, a McAfee researcher, in 2007 released a blog online informing the public about the Sticky Keys vulnerability. Vista apparently does allow the modification of sethc.exe file (located at: C:/windows/system32/sethc.exe) and no integrity checks are performed before execution. Authentication can simply be bypassed by replacing this file with cmd.exe using a live CD like Backtrack or direct logging and entering windows explorer [8]. Moreover, Vista activation mechanism has been broken almost one year after its official release. The same

security scenario applies to Windows seven. This operating system can be bypassed in the same way as Windows Vista (using the installation disk and entering recovery mode); furthermore, online news of a zero-day attack are spreading around. Certainly, this poor security performance of Microsoft Windows, the most used operating system worldwide, does not sound promising for ICT and its future.

Operating system design is a factor that will influence ICT in the times to come. The main reason is security. Considering the fact that digital globalization is facilitating the distribution of malware and the number of internet users are rising exponentially, it is worthwhile to expect more sophisticated attacks on operating systems and ICT. Under these circumstances, a review of the existing operating system design strategy, focusing on security and build reliable OS.

2.3. Open Source Issues

While companies like Microsoft, Apple or Sun de facto own the commercial software market, a variety of nonprofit organisations or savvy individuals contribute constantly to the proliferation of the open source software. In terms of operating systems, Linux is the example par excellence of all free open source systems. Introduced by Linus Torvalds, at the time a student, Linux was the first fully functional operating system that was offered for free under the open source agreement to the public [9]. Following this event, with the participation of thousands of admirers across the globe a myriad of open source Linux based operation systems flooded the cyber world.

The same phenomenon accompanied the development and release of various application programs. Nowadays it is quite likely to find online the open source counterpart of each of commercial software packages that are use every day (operation system or application software). Richard Stallman created in 1985 the Free Software foundation, aiming to help diffuse and make available free open source; later on, this event led to the development of General Public License (GPL), a license that allows use of software at no cost [10].

There are different pushing forces or reasons that motivate thousands of people around the globe to participate in open source projects and release software to the public. Intellectual gratification, pleasure of creativity or of solving complex and challenging tasks, are of some the driving forces in this domain [11]. Whatever the reasons, the benefits of using open source are manifold. Open-source software powers many of the web sites on the Internet, corporate computer, servers used for research and development, and a plethora of new gadgets that have broad appeal; it can be found in digital video recorders, telephones, personal digital assistants (PDAs) watches, networking hardware, MP3 players and automobiles [12].

Nevertheless, open source software does not come without issues or disadvantages. Even though the codes are available to thousands of eyes for scrutiny, there is no guarantee for security or optimal performance. Although that is ok for simple home applications it is not the case for enterprise, commercial or critical applications. Also because of lack of standardization and complex licensing issues, open source software is prone to misuse or abuse [12].

Standardization is hard to achieve in this domain because open source creators are completely free in their choice of design, implementation or adherence to existing standards. Usually standardization is enforced by market forces and industry regulators; however, in the case of open source software both these factors do not exercise enough pressure to drive the process.

Version proliferation is another major open source issue according to Waring and Maddocks [13]. As a matter of fact, this matter does not concern only open source software but commercial software as well. Nevertheless, the effect on the open source software is more evident. Developing many versions of a program in a short period not only confuses users but also requires a steep learning curve. This is true in particular in the case of constant changes of graphical user interfaces and navigation concepts from one version to the next one. At the sometime, constant introductions of new versions of a software package do not affect in positive way its reputation since the user might believe this is a sign of instability.

Another issue that affects ICT today is that of the implementation of open source software [13]. Because, open source is developed by the co-operation of different individuals, it is hard to establish a proper working relationship with the person in charge (if there is any). Furthermore, technical support, documentation issues, no access to advice, are some of the problems that a company or individual that uses open source software might face. Hardware and software compatibilities influence also the processes ever since most of hardware manufacturers do not expose their trade secrets, therefore not allowing access to their codes to open source developers. Open source developers have no other choice but to design and release their own code (hardware drivers) therefore contributing to the complexity and lack of standardization.

The open source phenomenon is definitely influencing in a positive way ICT and probably the trend will not change in the future. Open source projects are available to “millions of eyes” for scrutiny, improvement or testing. Nevertheless, it is likely that in the future will continue to experience the same issues mentioned above with some improvements in the area of standardization. Some open source will definitely transform into commercial software provided that they have matured enough and captured a significant market share. Red Hat Linux for example, is a typical example of how open source software becomes commercial under the right circumstances.

2.4. Design Complexity

The advances in information communication technologies are quite impressive and beneficial. Quite often new models of laptops, computers, phones or satellite navigators are released to the public. Certainly, while the benefits of such technology are enjoyed by users, another problem arises in

the background. It is the problem of the complexity of digital systems and technologies that are already believe to be un-replaceable. Let's take the case of the development of Microsoft operating systems. Microsoft employs thousands of programmers to develop its products, which are divided in teams with separate developing tasks. An operating system like Windows probably counts millions of lines of code; therefore, no individuals or even teams can really understand how the whole system works, or other individuals' parts of it interact in detail. These layers of complexity influence further performance and security merely because of the impossible task to understand the whole system. No wonder why several bug or operating system vulnerabilities are discovered on regular basis.

The same situation applies to application programs or hardware components. It is quite a common practice today to simply replace digital components and not repair them (memory slots, hard disk, processors). It is often convenient and financially less expensive to do so, however likely one of the reasons is the complexity of the components and the difficulty in understanding internal mechanisms. With the advances in technology users are reaching a stage when they are totally relying on components they do not understand although they have to trust. It is a well-known fact that the human brain does have limits as far as the memory and learning processes are concerned. Certainly, the level of complexity of systems and pace of change, do not contribute constructively to succeed at this endeavor.

The OSI layer is a theoretical model taught in almost any networking class to explain how digital information is exchanges locally or on the internet. There are currently seven layers in this model that make possible data delivery. For each layer, various protocols have been developed in the past with new ones added frequently. Each of these protocols are also very complex and difficult to understand; besides this, another layer of complexity is added to the process since various protocols interact together. This degree of complexity is one of the reasons behind the predominate issues with network programming and security.

Design complexity will be present in the future and more complex and sophisticated products will be seen. At the present, very complex products (hardware and software) are already being worked on and used, and the trend for the future is not going to change direction. ICT will suffer at a certain degree in the future because of complex designs and difficulty in troubleshooting or supporting systems. Furthermore, the core of Internet technology TCP/IP protocol stack must be redesigned to reduce complexity or deal better with security. The OSI model (which is an abstract model) currently relies on seven layers or communication. Each layer supports several individual protocols, which in their turn are very complex and add another layer to the complexity of the main systems. Maybe, design complexity is a price to be played in order to further the development of ICT and technological improvements.

2.5. Multiple Layer Approach

The proliferation of ICT technologies did have a positive impact on various research domains such as medicine, sociology, mathematics, business, research and development. In the same time, armed with these technological advances, many software developers developed countless number of applications that would satisfy market demand. For example, the great choice of web browsers (Mozilla Firefox, Internet Explorer, Opera, and Goggle Chrome) makes the experience of using the web enjoyable. On the other hand, other software package such as Adobe or Flash allows developers to create in their turn very useful applications. In addition, very small applications known as plug-ins or addins are randomly used to help users interact with web browsers or other software applications.

There is a problem though simply related to the fact that these programs interact with each in a multiple layer approach. For example, Internet Explorer is one of the web browsers shipped with Windows operating systems and used by millions of people around the world. For this web browser, a user needs several plug-ins so that can view different websites, videos or applications. Typical ad-ins for IE include: Java, Shockwave, Flash, ActiveX, Vivo Active or Windows Media Player plug-in. These applications are used on top of Internet Explorer adding another layer of complexity to system. In addition, the multiple layer approach deteriorates the security of ICT systems for a variety of reasons. One of them is interaction between plug-ins. In the modern times live product life cycles are very short due to the fact that competition is fierce and quick market releases are needed. In this condition, developers are in a lot of pressure and do not have the luxury of testing the interaction with other available plug-ins. The end result or this cycle are unforeseen interactions between applications, leading to vulnerabilities and probably ICT infrastructure breaching.

Multiple layer approach will affect ICT in the future. A multiple layer approach cannot be completely simplified; however, attempts can be made to achieve a reasonable degree of complexity. It will impact the future ICT regarding the security aspect of it because of the variety of applications and plug-ins that are likely to be developed and released for use. Even today, it is quite difficult to test and assess the interaction of these applications with each other, because of several factors including developer's time, pressure, financial costs and considerable application numbers. The same prognosis is reserved for the future.

3. ICT and Information Security Issues in Nigeria

Cybersecurity has grown to become a national issue as risk about it now requires to be taken more seriously. The big question is "How ready is Nigeria to tackle the challenges of cyber securities and fight cybercrime [14]. Section 3.1 highlights the operational definition of ICT and an overview

of Internet use in Nigeria, then section 3.2 examines briefly ICT and the menace of Cyber Crime in Nigeria, while section 3.3 considers the impacts of ICT on Privacy and Security.

3.1. Operational Definition of ICT and an Overview of Internet Use in Nigeria

The term "information and communication technology" (ICT), describes the integration of two previously existing disciplines: computing and telecommunications. ICT therefore refers to the convergence of audio-visual and telephone networks with computer networks, and the technology encompasses a wide range of activities, ranging from office data processing to remote control and monitoring of manufacturing robots. It also covers the cabling infrastructure e.g. fibre optic cables, which carry voice, data and video communications. A major offshoot of the convergence of information and communication technology is the emergence of the internet, which is a content distribution network comprising of a global system of interconnected computer networks through which data is interchanged. The technology consists of millions of private and public academic, business and government networks of both local and global scope which facilitates the dissemination and exchange of information and makes diverse other forms of non-physical interaction the new reality [15].

3.2. ICT and the Menace of Cyber Crime in Nigeria

In a paper, Oforji, Udensi, and Ibegbu [14] submitted that Africa is going through numerous Internet-related challenges in the areas of security risk, intellectual property breach and security of personal data in which it was maintained that Nigeria as a country is not an exception. Cybercriminals aim at people within and outside their national borders, and various African governments who lack the technical and the financial capability to tackle and supervise electronic communications believed to be sensitive for national security.

As argued by Oyewunmi [15], ICT access and uses began to grow, so also did the menace of cyber-crime. Cyber-crime consists of a variety of criminal acts perpetrated through the Internet, and includes e-mail scams, child pornography, hacking, theft of data, identity theft, extortion and a wide array of other nefarious activities. Other ICT–related crimes include the counterfeit cashier's cheque scheme, which relies on the issuance of fraudulent cheques, and targets individuals that use Internet advertisements to sell merchandise. Another is the advance fee fraud, also known as the "419 scam", after the section of the Nigerian Criminal Code dealing with the crime of obtaining property by false presences. The 419 scam combines impersonation fraud with a variation of an advance fee scheme, and relies on letters, emails, or faxes to potential victims from individuals representing themselves as government officials, offering the recipient the "opportunity" to share in a percentage of millions of dollars, while soliciting for help in placing large sums of money in overseas bank accounts. Therefore, these reports are consistent with recent submission in Ekoa and Mungwe [16], that Nigeria cybercrime has evolved from silly spray-and-spray email spam campaigns to refined con games that target large business organizations. According to the report, it is noteworthy that over 8,400 malwares sample was derived from Nigeria's scam emails from July 2014 to June 2016.

The problem of cybercrime is a global one whose extent, magnitude and impact reverberate throughout various walks of life, leaving hitherto unimaginable damage in its wake. Popularly referred to as the "yahoo yahoo syndrome" in Nigeria, these fraudulent activities are carried on by a recalcitrant few, but the impact is far reaching due to the world-wide reach of the Internet. Cybercrime is not only an embarrassment; it also has negative implications for the positive deployment of ICT for socio-economic growth and development.

With a view to dealing with some of the problems occasioned by cybercrime, the Nigerian government has deployed some legal and enforcement tools, including the enlistment of the Economic and Financial Crimes Commission (EFCC), the Nigerian Police Force, and other crime fighting bodies to tackle the problem. Unfortunately, however, initial attempts to deal with the problem did not utilize a refined and technology savvy approach to detect and arrest perpetrators. Rather, law enforcement officers largely descended on cyber cafes, carrying out frequent raids, arrests, ban of overnight browsing and other activities. However, resort to cyber cafes for internet access has waned considerably, with more possibilities to access the internet through mobile phones and personal computers. This may be attributed to the deregulation of the telecommunications sector, which has afforded the public the benefit of competitive internet access options by telecommunications companies, thus making private internet more accessible and affordable. This modification in the location of use from cyber cafes to private offices and homes means that physical raids of cyber cafes and other public venues for internet access can no longer constitute a valid approach to tackling online criminal activities. Rather, use of technological means and seeking of relevant information from, and collaboration with Internet Service Providers (ISPs) have become inevitable. This on its part raises the need for proper training and adequate deployment of specialized police and other enforcement authorities. Additionally, there is the issue of the security of stored customer data, which has been a concern in many developed countries, where servers holding millions of customer data have been hacked, and storage media such as compact discs holding data on millions of customers have been carelessly misplaced or lost in the post [15].

Beyond these however, more effort should be made to refocus on the promotion of positive uses of ICT. In this regard, it is encouraging that Microsoft has partnered with an NGO (Paradigm Initiative Nigeria (PIN)) to tackle cyber-crime through its Internet Safety, Security and Privacy Initiative for Nigeria (ISSPIN). The programme essentially focuses on redirecting the energy of young Nigerians away from cyber-crime and towards positive utilization of cyber

space for legitimate purposes. Microsoft also aims at addressing the need for adequate training in information technology among young Nigerians by distributing free compact discs containing Microsoft's Digital Literacy Curriculum. There is also the practical aspect of empowerment through training programmes designed to arm youths with marketable skills for legitimate business activities in the online environment. As awareness continues to rise about the potentials of the technology, there is a corresponding need for the creation of local content online, establishment of websites for businesses, as well as online advertisements and marketing. Expertise and skills in these areas are therefore increasingly becoming more valuable, and a legal framework that deals with protection of creativity, prevention of misrepresentations and fraudulent acts become relevant. Hopefully, skill acquisition in these areas will not only reduce the tendency towards commission of cyber-crimes, but also contribute to a reduction in the number of the unemployed in the country.

3.3. Impacts of ICT on Privacy and Security

There are a number of adverse impacts of ICT on the privacy and security of individuals and organizations. They include commercial losses from denial of service attacks, data loss through theft or corruption and disclosure of confidential data. The OECD model business and household surveys OECD [17] and Eurostat [18] model community surveys of enterprises and households included questions on the incidence of harmful security incidents. Such questions do not quantify the extent of impact, although they are useful in measuring how widespread the problems are. Far more serious potential negative impacts could arise because of the increasing reliance of critical infrastructure on ICT and the serious consequences of failure. Such impacts can affect societies and economies, as well as individual businesses [19].

4. Methodology

The research conducts a quantitative research. The research method utilized for this study is the survey method which involves the use of questionnaire instrument. The research used questionnaire in collecting the raw data from the respondents easily, and co-ordinate them in a more concise manner. Closed - ended questions were asked to enable the respondents -personnel of Nigeria Security and Civil Defence Corps (NSCDC), the opportunity to give their suggestions by answering the question in objective format. The sampling techniques used in analyzing the data obtained from the questionnaire answering the research question is Yaro Yemen's formula, as a sampling technique and chi-square has been used to test the formulated hypotheses. For easy analysis and interpretation of the result, a sample of one hundred and fifty (150) members of staff of Nigeria Security and Civil Defence Corps (NSCDC) is chosen from the population using the simple random technique.

In order to achieve accuracy and true representative of the study population, the stratified random sampling techniques was used to select 5 respondent each from the superintendent cadre, inspectorate cadre and other rank and file from the selected Departments/Units and Area Councils under the Federal Capital Territory (F. C. T) Command. However, the entire staff of a selected department/unit whose staff strength is less than or not more than five was sampled.

Table 1. *Breakdown of sample size.*

S/No	Departments/Units/Area Councils	Superintendent Cadre	Inspectorate Cadre	Other Rank & File	Total
1	Admin & personnel staff	5	5	0	10
2	Planning research & statistics staff	5	5	0	10
3	Operations staff	5	5	5	15
4	Private guard company staff	5	5	0	10
5	Intelligence & investigation staff	5	5	5	15
6	Gwagwalada staff	5	5	5	15
7	Kuje staff	5	5	5	15
8	Amac staff	5	5	0	10
9	Counter terrorism unit staff	5	5	5	15
10	Special duties staff	5	5	0	10
11	Account staff	5	5	0	10
12	Disaster management unit staff	5	5	5	15
	Total	60	60	30	150

Source: Field Work, 2014

The quantitative data were analyzed logically using the Statistical Package for Social Sciences (SPSS) which is a descriptive statistics of frequency analysis for quantitative data. This help to ensure completeness, legibility and constituency. The chi – square statistical technique which is a non – parametric test was employed to test the formulated hypotheses. The chi-square is used to test hypotheses about the distribution of observations into categories. It shows the relationship between the expected frequencies and observed frequencies. It is computed by this formula:

$$X^2 = \sum \frac{(Oi - Ei)^2}{Ei}$$

5. Results and Discussions

This section presents the results and discussion for the

study. It includes the results of quantitative data which were derived from descriptive statistics such as frequency distribution and chi – square. The results are integrated to harmonize different views on the subject – matter under investigation. In attempt to carry out a meaningful study, the research distributed a total of one hundred and fifty (150) questionnaires using simple random technique to gather information for this study; one hundred and forty-six (146) questionnaires were returned.

5.1. Presentation and Analysis of Data According to Research Questions

5.1.1. Research Question One

Does NSCDC have the Information and Communication Technology tools in combating crime?

Questionnaire No 1, 2 and 3 were used to answer research question one. This is expected to examine the level of computerization in Nigeria Security and Civil Defence Corps, FCT command.

Table 2. *Responses to research question one.*

		Frequency	Percent	Valid Percent	Cumulative Percent
NSCDC As An Establishment Undertake Computer Training Programme For Its Personnel					
	STRONGLY AGREE (SA)	8	5.5	5.5	5.5
	AGREE (A)	17	11.6	11.6	17.1
Valid	DISAGREE (D)	60	41.1	41.1	58.2
	STRONGLY DISAGREE (SD)	61	41.8	41.8	100.0
	Total	146	100.0	100.0	
Combating Crime Can Be Achieved Greatly with The Use Of ICT					
	STRONGLY AGREE (SA)	49	33.6	33.6	33.6
	AGREE (A)	68	46.6	46.6	80.1
Valid	DISAGREE (D)	25	17.1	17.1	97.3
	STRONGLY DISAGREE (SD)	4	2.7	2.7	100.0
	Total	146	100.0	100.0	
Does NSCDC Have The Information and Communication Technology Tools in Combating Crime					
	STRONGLY AGREE (SA)	5	3.4	3.4	3.4
	AGREE (A)	37	25.3	25.3	28.8
Valid	DISAGREE (D)	40	27.4	27.4	56.2
	STRONGLY DISAGREE (SD)	64	43.8	43.8	100.0
	Total	146	100.0	100.0	

Source: Field Survey, 2014

Based on "NSCDC as an Establishment Undertake Computer Training Programme for Its Personnel", it indicated that 5.5% of the respondents strongly agree, 11.6% of the respondents agrees, 41.6% of the respondents disagree and 41.8% of the respondents strongly disagree. This implies that majority of the respondents strongly disagree that NSCDC as an establishment undertake in-service training for its staffs.

Based on "Combating Crime Can Be Achieved Greatly With the Use of ICT", this implied that 33.6% of the respondents strongly agree, 46.6% of the respondents agrees, 17.1% of the respondents disagrees while 2.7% of the respondents strongly disagrees. It indicates that majority of the respondents agrees that combating crime can be achieved greatly with the use of ICT.

Based on "Does NSCDC Have the Information and Communication Technology Tools in Combating Crime", 3.4% of the respondents strongly agree, 25.3% of the respondents agrees, 27.4% of the respondents disagrees, while 43.8% of the respondents strongly disagree. This implied that majority of the respondents strongly disagree that NSCDC have required Information and Communication Technology tools in combating crime.

5.1.2. Research Question Two

What is the usefulness of information gathering to NSCDC?

Question No 4, 5, 6, and 7 are used to answer research question two. This is poised to ascertain the usefulness of Information gathering to Nigeria Security and Civil Defence Corps.

Table 3. *Responses to research question two.*

		Frequency	Percent	Valid Percent	Cumulative Percent
Information Management Department/Unit Would Play a Great Role in Information Gathering					
	STRONGLY AGREE (SA)	24	16.4	16.4	16.4
	AGREE (A)	95	65.1	65.1	81.5
Valid	DISAGREE (D)	21	14.4	14.4	95.9
	STRONGLY DISAGREE (SD)	6	4.1	4.1	100.0
	Total	146	100.0	100.0	
The Wrong Criteria For Staff Deployment to Information Management Department/Unit Hinder Information Gathering					
	STRONGLY AGREE (SA)	31	21.2	21.2	21.2
Valid	AGREE (A)	75	51.4	51.4	72.6
	DISAGREE (D)	29	19.9	19.9	92.5

		Frequency	Percent	Valid Percent	Cumulative Percent
	STRONGLY DISAGREE (SD)	11	7.5	7.5	100.0
	Total	146	100.0	100.0	
Every Information Gathering Should Be Treated as Valid and Important.					
Valid	STRONGLY AGREE (SA)	36	24.7	24.7	24.7
	AGREE (A)	96	65.8	65.8	90.4
	DISAGREE (D)	14	9.6	9.6	100.0
	Total	146	100.0	100.0	
The Usefulness of Information Gathering to NSCDC is Vital Through ICT.					
Valid	STRONGLY AGREE (SA)	30	20.5	20.5	20.5
	AGREE (A)	98	67.1	67.1	87.7
	DISAGREE (D)	18	12.3	12.3	100.0
	Total	146	100.0	100.0	

Source: Field Survey, 2014

Based on "Information Management Department/Unit Would Play a Great Role in Information Gathering", 16.4% of the respondents strongly agree, 65.1% of the respondents agreed, 14.4% of the respondents disagreed, in addition only 4.1% of the respondents strongly disagree. This implied that majority of the respondents agrees that Information management department/unit/councils play a great role in information gathering in the security agencies.

Based on "The Wrong Criteria for Staff Deployment to Information Management Department/Unit Hinder Information Gathering", Majority of the respondents (51.4%) agree, 21.2% of the respondents strongly agrees, 19.9% of the respondents disagrees, while only 7.5% of the respondents strongly disagree. This implied that when staffs with the right skills are deployed to Information Management Department/Unit, it would help in information gathering in NSCDC.

Based on the "Every Information Gathering Should Be Treated as Valid and Important", 24.7% of the respondents strongly agree, 65.8% of the respondents agreed, 9.6% of the respondents disagreed. This implied that majority of the respondents agreed that every information gathering should be treated as valid and important.

Based on "The Usefulness of Information Gathering to NSCDC is Vital through ICT", 20.5% of the respondents strongly agreed, 67.1% of the respondents agreed, while 12.3% of the respondents disagreed. It shows that majority of the respondents agreed that the usefulness of informational gathering to NSCDC is vital through ICT.

5.1.3. Research Question Three

Does the staff of NSCDC FCT Command have the required knowledge and skills in using ICT resources?

Question No's 11, 12, 13, and 14 were used to answer research question three. This tends to determine how skillful and knowledgeable the staffs are in the use of Information and Communication Technology resources.

Table 4. *Responses to research question three.*

		Frequency	Percent	Valid Percent	Cumulative Percent
Application of Information Gathering is Important to Crime Management					
Valid	STRONGLY AGREE (SA)	78	53.4	53.4	53.4
	AGREE (A)	37	25.3	25.3	78.8
	DISAGREE (D)	26	17.8	17.8	96.6
	STRONGLY DISAGREE (SD)	5	3.4	3.4	100.0
	Total	146	100.0	100.0	
ICT Equipment is Useful for Information Storage and Dissemination					
Valid	STRONGLY AGREE (SA)	81	55.5	55.5	55.5
	AGREE (A)	55	37.7	37.7	93.2
	DISAGREE (D)	10	6.8	6.8	100.0
	Total	146	100.0	100.0	
NSCDC Undergo In-Service Training on Information Management					
Valid	AGREE (A)	27	18.5	18.5	18.5
	DISAGREE (D)	94	64.4	64.4	82.9
	STRONGLY DISAGREE (SD)	25	17.1	17.1	100.0
	Total	146	100.0	100.0	
The Staff of NSCDC FCT Command Has The Required Knowledge and Skills In Using ICT Resources.					
Valid	AGREE (A)	21	14.4	14.4	14.4
	DISAGREE (D)	99	67.8	67.8	82.2
	STRONGLY DISAGREE (SD)	26	17.8	17.8	100.0
	Total	146	100.0	100.0	

Source: Field Survey, 2014

Based on "Application of Information gathering is important to Crime Management", indicates that 53.4% of the respondents strongly agrees, 25.3% of the respondents agrees, 17.8% of the respondents disagrees while 3.4% of the

respondents strongly disagree. This implied that majority of the respondents strongly agreed that application of information gathering is important to crime management.

Based on "ICT Equipment is useful for Information Storage and Dissemination", majority of the respondents (55.5%) strongly agrees, 37.7% of the respondents agrees while only 6.8% disagree. It shows that majority of the respondents strongly agrees that ICT equipment is useful for information storage and dissemination.

Based on "NSCDC undergo In-Service training on Information Management", Table 4 indicates that 18.5% of the respondents agrees, 64.4% of the respondents disagrees, while 17.8% of the respondents strongly disagree. This implied that majority of the respondents disagrees that NSCDC undergo in-service training on information management.

Based on "The Staff of NSCDC FCT Command has the required Knowledge and Skills in using ICT Resources", indicates that 14.4% of the respondents agrees, 67.8% of the respondents disagrees, while 17.1% of the respondents strongly disagree. This implied that majority of the respondents disagrees that the staff of NSCDC FCT command has the required knowledge and skills in using ICT resources.

5.1.4. Research Question Four

What are the factors militating against the application of ICT in NSCDCs?

Question No 15 is used to answer research question four. This seeks to determine the challenges associated with the application of Information and Communication Technology to combat crime in Nigeria Security and Civil Defence Corps.

Table 5. *Responses to research question four.*

		Frequency	Percent	Valid Percent	Cumulative Percent
Lack of Finance is One of The Factors Militating Against The Application of ICT in NSCDCs					
Valid	STRONGLY AGREE (SA)	130	89.0	89.0	89.0
	AGREE (A)	16	11.0	11.0	100.0
	Total	146	100.0	100.0	

Source: Field Survey, 2014

Based on "Lack of Finance is one of the Factors Militating Against the Application of ICT in NSCDCs", Table 5 indicates that (89.0%) of the respondents strongly agrees, while (11.0%) of the respondents agrees. This implied that majority of the respondents strongly agrees that lack of finance is one of the factors militating against the application of ICT in NSCDCs.

5.2. Test of Hypotheses

Two hypotheses formulated in the section one of this study are tested using chi - square statistical method.

5.2.1. Test of Hypotheses 1

H^0: NSCDC does not have the required ICT tools in combating crime

H^1: NSCDC do have the required ICT tools in combating crime

The Table 6 following will be relevant for the test of hypotheses 1:

Table 6. *NPar Tests, Chi-Square Test and Frequencies for Hypotheses 1.*

	Observed N	Expected N	Residual
NSCDC As An Establishment Undertake Computer Training Programme For Its Personnel			
STRONGLY AGREE (SA)	8	36.5	-28.5
AGREE (A)	17	36.5	-19.5
DISAGREE (D)	60	36.5	23.5
STRONGLY DISAGREE (SD)	61	36.5	24.5
Total	146		
Combating Crime can be achieved Greatly with the Use Of ICT			
STRONGLY AGREE (SA)	49	36.5	12.5
AGREE (A)	68	36.5	31.5
DISAGREE (D)	25	36.5	-11.5
STRONGLY DISAGREE (SD)	4	36.5	-32.5
Total	146		
Does NSCDC have the Information and Communication Technology Tools in Combating Crime			
STRONGLY AGREE (SA)	5	36.5	-31.5
AGREE (A)	37	36.5	.5
DISAGREE (D)	40	36.5	3.5
STRONGLY DISAGREE (SD)	64	36.5	27.5
Total	146		

Test Statistics			
	NSCDC as an Establishment Undertake Computer Training Programme for its Personnel	Combating Crime can be Achieved Greatly with the use of ICT	Does NSCDC have the Information and Communication Technology tools in combating Crime

Test Statistics			
Chi-Square	64.247[a]	64.027[a]	48.247[a]
Df	3	3	3
Asymp. Sig.	.000	.000	.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 36.5.

Interpretation of Result

Calculated value (X_{Calc}) = 64.247, 64.027 and 48.247, tabulated value (X_{tab}) = 7.81, 7.81, and 7.81, degree of freedom (df) = 3, 3 and 3. Hence, the calculated value is greater than the tabulated value; Consequently, the alternate hypothesis (H^1) is accept and the null hypothesis (H^0) is reject. The alternate hypothesis states that NSCDC do have the required ICT tools in combating crime. The findings in hypothesis two is similar to the strategic intent as stated in the website of NSCDC, The Nigerian Security and Civil Defence Corps "will use proven information technologies to deliver the best possible service to all its Directorates, Units, Zones, Commands and the public. Systems will be selected and deployed based on their effectiveness in improving the access to and exchange of information as well as the productivity of staff in furtherance of the Corp's objective. Systems should be intuitive, easy to use, and integrated with other systems to eliminate duplication and redundant data entry. The Corps will commit the necessary resources to support these systems and ensure their security, reliability and accuracy. There will be appropriate backup and disaster recovery".

5.2.2. Test of Hypotheses 2

H^0: Information gathering does not help NSCDC

H^1: Information gathering do help NSCDC

The Table 7 following will be relevant for the test of hypotheses 2:

Table 7. *NPar Tests, Chi-Square Test and Frequencies for Hypotheses 2.*

	Observed N	Expected N	Residual
Information Management Department/Unit Would Play a Great Role in Information Gathering			
STRONGLY AGREE (SA)	24	36.5	-12.5
AGREE (A)	95	36.5	58.5
DISAGREE (D)	21	36.5	-15.5
STRONGLY DISAGREE (SD)	6	36.5	-30.5
Total	146		
The Wrong Criteria For Staff Deployment to Information Management Department/Unit Hinder Information Gathering			
STRONGLY AGREE (SA)	31	36.5	-5.5
AGREE (A)	75	36.5	38.5
DISAGREE (D)	29	36.5	-7.5
STRONGLY DISAGREE (SD)	11	36.5	-25.5
Total	146		
Every Information Gathering Should Be Treated as Valid and Important			
STRONGLY AGREE (SA)	36	48.7	-12.7
AGREE (A)	96	48.7	47.3
DISAGREE (D)	14	48.7	-34.7
Total	146		
The Usefulness of Information Gathering to NSCDC is Vital Through ICT			
STRONGLY AGREE (SA)	30	48.7	-18.7
AGREE (A)	98	48.7	49.3
DISAGREE (D)	18	48.7	-30.7
Total	146		

Test Statistics				
	Information Management Department/Unit Would Play a Great Role in Information Gathering	**The Wrong Criteria For Staff Deployment to Information Management Department/Unit Hinder Information Gathering**	**Every Information Gathering Should Be Treated as Valid and Important.**	**The Usefulness of Information Gathering to NSCDC is Vital Through ICT.**
Chi-Square	130.110[a]	60.795[a]	74.027[b]	76.493[b]
Df	3	3	2	2
Asymp. Sig.	.000	.000	.000	.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 36.5.
b. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 48.7.

Interpretation of Result

Calculated value (X_{Calc}) = 130.110, 60.795, 74.027 and 76.493, tabulated value (X_{tab}) = 7.81, 7.81 5.99 and 5.99, degree of freedom (df) = 3, 3, 2, and 2. Hence, the calculated value is greater than the tabulated value; Consequently the alternate hypothesis (H^1) is accept and the null hypothesis (H^0) is reject. The alternate hypothesis states that Information gatherings do help NSCDC. The findings in hypothesis two is similar to the technical goals of NSCDC as stated in the website of NSCDC which has been clearly highlighted under

section 1.5.1 of the report.

5.3. Further Discussions

The critical presentation and analysis of data in this section provides various facts as regard the impact of information and communication technology toward security. Various questions were asked in this section of this study which indicates that majority of respondents strongly believe and accepts that the impact of ICT plays a great role toward security.

The following represents the findings from the study. Considering the research study which focuses on table 4.8, test of hypothesis one. It was tested using chi-square analysis and revealed that the NSCDC do have the required ICT tools in combating crime. The Nigerian Security and Civil Defence Corps "will use proven information technologies to deliver the best possible service to all its Directorates, Units, Zones, Commands and the public. Systems will be selected and deployed based on their effectiveness in improving the access to and exchange of information as well as the productivity of staff in furtherance of the Corp's objective. Systems should be intuitive, easy to use, and integrated with other systems to eliminate duplication and redundant data entry. The Corps will commit the necessary resources to support these systems and ensure their security, reliability and accuracy. There will be appropriate backup and disaster recovery".

Table 7, test of hypothesis two shows that Information gatherings do help NSCDC. Several studies have identified that the deployment of ICT is characterized by both a strong service orientation and a readiness to respond to a rapidly changing security environment.

6. Conclusion

6.1. Summary of Findings

This study examined the Impact of Information and Communication Technology on Security using Nigeria Security and Civil Defence Corps (NSCDC) as case study. Information and Communication Technologies (ICT) introduced in the second half of the last century have shaped substantially the way people interact with each other, do business, entertain and learn. ICT are encouraging globalization, exchange of information and the proliferation of cyber space. In this era of digital revolution when humans have become more dependent on such technologies and their by-products, the benefits of using these technologies are immense and globally visible and here to stay. Furthermore, these technologies have matured developing into a range of dedicated niche domains such networking, mobile communications, wireless communications, satellite broadcasting and so on.

The result had shown in hypotheses one that NSCDC do have the required ICT tools in combating crime, with p-value = 64.247, 64.027 and 48.247 which is greater than significant level of 0.05 ($p>0.05$). These hypotheses supported with various studies and research finding. The finding is consistent with strategic intent as stated in the website of NSCDC [2]. The Nigerian Security and Civil Defence Corps "will use proven information technologies to deliver the best possible service to all its Directorates, Units, Zones, Commands and the public. Systems will be selected and deployed based on their effectiveness in improving the access to and exchange of information as well as the productivity of staff in furtherance of the Corp's objective. Systems should be intuitive, easy to use, and integrated with other systems to eliminate duplication and redundant data entry. The Corps will commit the necessary resources to support these systems and ensure their security, reliability and accuracy. There will be appropriate backup and disaster recovery".

The result shown in hypotheses two that Information gathering does help NSCDC, with p-value = 130.110, 60.795, 74.027 and 76.493 which is greater than significant level of 0.05 ($p>0.05$). The findings in hypothesis three is similar to the technical goals of NSCDC as stated in the website of NSCDC which is as follows: Use technology to facilitate access to Corp's commercial and non-commercial information to authorized persons legitimate access, To increase NSCDC revenue via ICT, The Corps to ensure regular training of ICT professionals, Provide support for CNS/ATM operations, Co-ordinate information communications technology at both the headquarters and outstations, Virtual community: Use technology to foster improved communication and information dissemination.

6.2. Concluding Statements

ICT will provide great benefits especially in security to the society for years to come. The proliferation of these technologies or their decline will be affected amongst all by security issues on these areas: lack of security awareness and training, operating system design and security, open source issues, design complexity and multiple layer approach. Therefore, designing better operating systems, improving on security awareness, training and multiple layer complexity are some of the challenges for the future to contain as a sovereign nation.

Obviously, using Nigeria Security Civil Defence Corp, FCT Command, Abuja as a study, this research work has revealed that ICT has tremendous impacts on security and fight against cybercrime. The findings in this study correspond with the theoretical postulations established under the literature review of this study. ICT has roles in the security of any nation; the impacts of which can be direct, through its sectoral and industries' growth, and indirect through some multiplier effects.

6.3. Recommendations

In line with the findings and conclusions reached, the following recommendations are suggested:

i. NSCDC as an establishment should undertake computer training for all its personnel's as a way of equipping them with the necessary ICT skills.
ii. Constantly equipping NSCDC personnel with the

required ICT skills would help in combating crimes with the use of ICT tools.

iii. Various Information Management Departments/Units in the NSCDC should be well equipped with the right ICT tools which would help in information gathering.

iv. ICT equipment should be encouraged and fully enforced for information storage and dissemination.

v. Government should provide adequate fund towards the application of ICT in NSCDC.

References

[1] Tengku, Mohd T. S. (2003). Ethics of Information Communication Technololgy. A Paper presented at.

[2] NSCDC (2014). Information and Communication Technology Unit. Retrieved from http://www.nscdc.gov.ng/index.php/unitss/ict.

[3] Schneier, B. (2004). Secrets and Lies: Digital security in a networked world, John Wiley and Sons Inc., USA.

[4] Elidon, B. (2011). Information and Communication Technology security issues. School of Computing, Information Technology and Engineering, University of East London, Docklands Campus, University Way.

[5] Turle, M. (2009). Data security: Past, present and future, Science Direct, Computer Law & Security Report, Volume 25, Issue 1, Pages 51-58.

[6] Gantz, J., Gillen, A., & White, A. (2009). The economic impact of Microsoft's Windows 7, Worldwide, Retrieved from http://www.microsoft.com/about/corporatecitizenship/us/economicgrowth.mspx.

[7] CE (2007), Computer Economics, Annual Worldwide Economic Damages from Malware Exceed $13 Billion, Retrieved from http://www.computereconomics.com/article.cfm?id=1225.

[8] Vinoo, T. (2007). Windows Vista Vulnerable to StickyKeys Backdoor. Retrieved from http://www.avertlabs.com/research/blog/index.php/2007/03/12/windows-vistavulnerable-to-stickykeys-backdoor/.

[9] Wikipedia, (2009). History of Linux, Accessed from http://en.wikipedia.org/wiki/History_of_Linux Cyber Security Future Issues.

[10] Krogh, G. & Hippel, E. (2003). Special issues on open source software, Science Direct, Research Policy, Volume 32, Issue 7, July, Pages 1149-1157.

[11] Bonnacorsi, A. and Rossi, C. (2003). Why Open Source software can succeed, Science Direct Research Policy Volume 32, Issue 7, July, Pages 1243-1258.

[12] Stahl, M. (2005). Open-source software: not quite endsville, Science Direct, Drug Discovery Today, Volume 10, Issue 3, 1 February, Pages 219-222.

[13] Waring, T. and Maddocks, P. (2005). Open Source Software implementation in the UK public sector: Evidence from the field and implications for the future, Science Direct, International Journal of Information management, Volume 25, Issue 5, October, Pages 411-428.

[14] Oforji, J. C., Udensi, E. J. & Ibegbu, K. C. (2017) Cybersecurity Challenges in Nigeria: The Way Forward, Sos Poly Journal of Science & Agriculture, V ol. 2, (Dec., 2017) ISSN: 2536 - 71 61.

[15] Oyewunmi, A. O., (2012). The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions. British Journal of Arts and Social Sciences ISSN: 2046-9578, Vol. 5 No. 2. Retrieved from http://www.bjournal.co.uk/BJASS.aspx.

[16] Ekoa, R. & Mungwe, M. (2018). A review of Cybercrime in Sub-Saharan Africa: A Study Cameroon and Nigeria. International Journal of Scientific & Engineering Research Volume 9, Issue 5, May 2018 211 ISSN 2229-5518. Retrieved from https://www.ijser.org/researchpaper/A-review-of-Cybercrime-in-Sub-Saharan-Africa-A-Study-Cameroon-and-Nigeria.pdf (Accessed: 12/10/2018).

[17] OECD (2009a). Guide to Measuring the Information Society, 2009.Available from www.oecd.org/sti/measuring-infoeconomy/guide.

[18] Eurostat (2010). Model ICT use questionnaires, years 2002-2011.

[19] OECD (2008c). Shaping Policies for the Future of the Internet Economy. OECD Ministerial Meeting on the of the Internet Economy, Seoul, 2008. Retrieved from http://www.oecd.org/dataoecd/1/29/40821707.pdf.