CYBERWARFARE & NATIONAL SECURITY:

AN IMPERATIVE OF NIGERIAN ARMY PREPAREDNESS

"The supreme art of war is to subdue the enemy without fighting"
- Sun Tzu's *The Art of War*

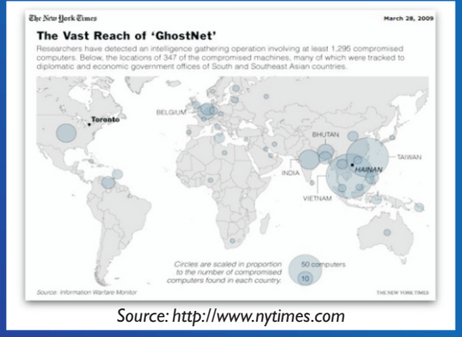
By: Ikerionwu Fredrick
Web Developer
Twitter@Fredwave

INTRODUCTION

Information and Communications Technologies (ICTs) have drastically increased the porosity between national borders. The increased porosity and anonymity of the Internet superimposed in a complex interaction that enables criminal and violent groups, transnational terrorist organizations and companies engaged in espionage to expand their operations globally. The tempo of our lives is being increased due to the compression of time and the shrinking of distances across the world. Given the dynamics of international power play, including changes in war fighting methods, with the blurred nature of the cyberspace there is no doubt that the terrestrial distance between adversaries becomes irrelevant making everyone a next-door neighbor in cyberspace. This development in cyberspace cannot be ignored by any military in the quest for improving its national security.

The most powerful weapons in cyber terrorism are not based on physical strength but logic and innovation in cyberspace, hence, a threat to national security. Computer hardware, software, and bandwidth forms the wherewithal for implementing a robust cyberwarfare for individual organization and state and also to transnational criminal organizations thereby posing a threat to national security.

Countries across the world are experiencing different levels of cyber attacks. The Russian Federation's cyber attacks against Estonia in 2007, Israeli cyber attacks on Syria in 2007 and Georgia in 2008 are typical examples of cyberwarfare application to undermine national security. Also the cyber spy network called "GhostNet" in 2009 that accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world cannot be over ruled. GhostNet was reported to originate from China, although the country denied responsibility**.** According to the Imperial War Museum (IWM) research, wide-range cyber-exploitation network GhostNet, contaminated minimum of 1,295 computers in 103 countries and 30% of the targeted objects are to be evaluated as high value, as far as the political, diplomatic, economic, and military criteria are concerned.

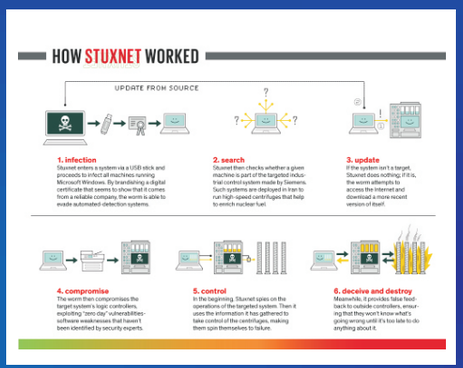


Source: http://www.nytimes.com

According to Forbs, the Stuxnet worm invasion of Iranian nuclear facilities in June 2010 is a typical case of cyberwarfare application, suspected to be fashioned by either the U.S. or Israei government designed to attack the Bushehr nuclear power plant in Iran. The following spots fall into range of the high-value targets' list;

- Ministries of foreign affairs of Bangladesh, Brunei, Indonesia, Iran, Philippines Embassies of Cyprus, Germany, India, Indonesia, Pakistan, Portugal, South Korea, Thailand.
- The Asian Development Bank, Association of Southeast Asian Nations Secretariat (ASEAN) and South Asian Association for Regional Cooperation (SAARC).
- An unclassified NATO headquarters

Stuxnet is an Internet worm that infects Windows computers, which is been spread via USB sticks, once inside a network, it uses a variety of mechanisms to propagate to other machines within that network and gain privilege once it has infected those machines, placing the host in total control of the network and it's allied infrastructures. Stuxnet has already infected more than 70,000 Windows computers, and Siemens has reported more than 50 infected control

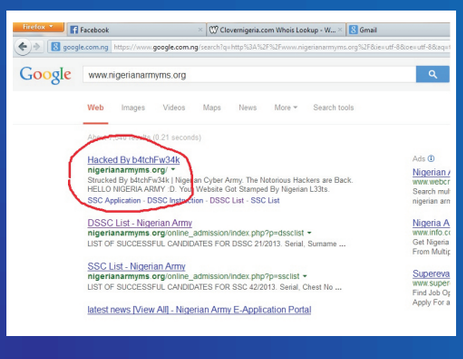


systems, many in Germany as this number increase even at the time of filing this report. There has not been any official record of any physical damage Stuxnet has caused, although there are rumors that it was responsible for the failure of India's National Satellite System (INSAT-4B) in July 2010. In Nigeria, the increasing prevalence on acts of terrorism is a contemporary security issue that demands swift reaction. The tendency for the terrorist to resort to cyberwarfare to undermine the nation's infrastructure as well as national security cannot be over ruled. Currently, terrorism has become the most widespread form of violence for expressing public discontent. Thus, in Nigeria so far, terrorism has remained within its traditional form of violence, but it has the potential of migrating into the use of computer technology and network to lunch such attacks. The illustration bellow is a google footage of the Nigerian military website belonging to the department of Military Secretary used for the purpose of online application of Nigerians into the Direct Short Service and Short Service Commission was hacked on 10th Mar 14.

More worrisome is the level of preparedness of Nigeria's security agencies and stakeholders especially the Nigerian Army towards containing this emerging threat. The foregoing motivated the writer to undertake this study. The purpose of this paper is to appraise cyberwarfare in a contemporary Nigerian national security with a view to drawing lessons to the NA.

CONCEPTUAL DEFINITION

Cyberwarfare.JA. Lewis in his study ***Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats***, denotes that



Cyberwarfare conjures up images of information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations. This can also be defined as activities which involve units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. The in cooperation of Cyberwarfare in a military doctrine can support military operations and also enhance state's national security. They can disrupt the target's command, control, and communications. They can support covert actions to influence governments, events, organizations, or persons, often disguising whoever is launching those actions. Valuable information and state secrets can be obtained through cyber espionage.

Twitter@Fredwave

CYBERWARFARE & NATIONAL SECURITY:

AN IMPERATIVE OF NIGERIAN ARMY PREPAREDNESS

"The supreme art of war is to subdue the enemy without fighting"
- Sun Tzu's *The Art of War*

By: Ikerionwu Fredrick
Web Developer

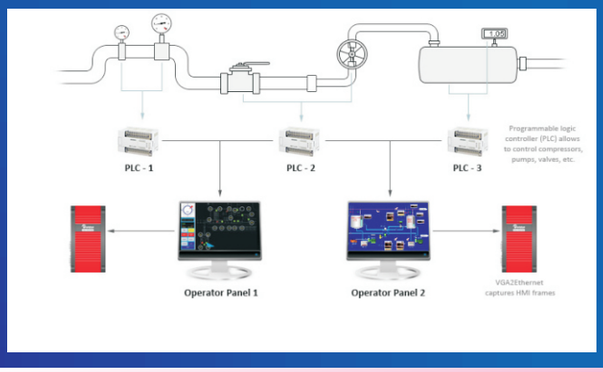
Cyberwarfare can be carried out in a number of ways. Among them:
a. Computer-network attacks
b. Social-networking-led attacks
c. Attacks on radio networks for GPS and wireless networks
d. Radio frequencies with sufficiently high power to disrupt all unprotected electronics in a given geographical area

Cyber Terrorism.

ED Dorothy, defines cyber terrorism as Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Furthermore, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions or severe economic and destruction of critical infrastructure would be examples provided it was carried out with the aid of a computer mechanism. Cyber terrorism can be launched against the critical infrastructure of nations that includes telecommunications, energy, financial networks, transportation systems, and water distribution, among others. In many countries, such infrastructure is owned and operated by the private sector. Much of it depends on Supervisory Control and Data Acquisition (SCADA) systems, which are computer-controlled in a networked environment.

Illustration of SCADA controlled Power plant

Taking advantage of vulnerabilities in these systems, terrorist can disable them and disrupt essential services. An attack on the air traffic control system could not just wreak havoc with flight schedules but also, in the worst case, cause crashes. The effects are the same as if the infrastructure were bombed or attacked by some other physical measure, without the enemy coming in by air, sea, or land. Likewise, financial networks can be targeted to disrupt a nation's economy. Banks, stock exchanges, trading, online payment systems, and other transactions of all kinds can be brought to a grinding halt as if these were physically bombed. The effects are similar to what would be achieved by Weapons of Mass Destruction (WMD). The convergence of terrorism and cyberspace is referred to as cyber terrorism. An attack on ICT infrastructure can lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic losses. All such attacks against critical infrastructures would qualify as acts of cyber terrorism. In spite of a lack of an operational definition, cyber terrorism is real and it has become the new tool of terrorists, jihadists, and transnational criminal organizations (TCOs) worldwide.



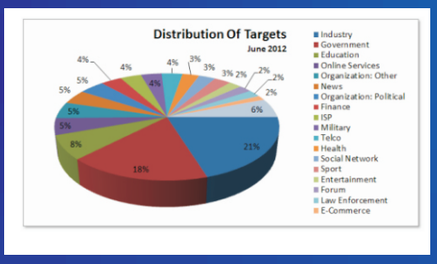
Cyberspace. Dr Dan Kuehl defines Cyberspace as an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected ICT based systems and their associated infrastructures. It comprises of IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. They are connected through undersea cables, satellites in outer space, land lines, and radio links. A nation's cyberspace is part of global cyberspace; it cannot be isolated to define its boundaries since cyberspace is borderless. This is what makes cyberspace unique. Unlike the physical world that is limited by geographical boundaries—land, sea, river waters and air—cyberspace can and is continuing to expand. Technology innovations are pushing the speeds of communication and computing to new limits; quantum computers promise to far exceed Moore's Law, which predicts that the processing power of computers doubles every eighteen months. Increased Internet penetration is leading to the rapid growth of the cyberspace, since the size of cyberspace is proportional to the activities that are carried through it. Among those activities: the exchange of goods or services, financial transactions through banks, credit card payments, email communications, social networking, exchange of pictures, videos or music. These activities lead to the seamless merging of cyberspace with the physical world. No wonder that cyber crimes/terrorism impact the physical world, too. Cyber terrorism are used to disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in physical space and a treat to national security. Their users range from entire nation states and their component organizational elements and communities down to lone individuals and amorphous transnational groups who may not profess allegiance to any traditional organization or national entity.

National Security.

Albert defined national security as thus: the *protection of a state, its territories, and its peoples from physical assault by an external force, as well as the protection of important state economic, political, military, social, cultural, and valuable interests from attacks emanating from foreign or domestic sources which may undermine, erode, or eliminate these interests (national or international), thereby threatening the survival of the state. Such protection may be pursued by military or non military means. Critical infrastructure protection creates a new set of problems for national security. Studies conducted have shown that government installation and commercial organizations are major targets of cyber offenders as shown on the illustration below.*

RELATIONSHIP BETWEEN CYBERWARFARE AND NATIONAL SECURITY

Cyber attacks are often presented as a threat to military forces and the Internet has major implications for espionage and warfare. The Armed Forces of Nigeria (AFN) are mandated by Section 217 (2) of the 1999 Constitution to defend Nigeria from external aggression, maintain its territorial integrity and secure her borders from violation on land, sea and air. In an era of nation states, this has included not only the protection of the citizens,



but also the safeguarding of nation borders, control of the flow of goods and services across those borders and interaction with other nation state in which cyberspace is not excluded. Therefore, there is direct relationship between cyberwarfare and national security, knowing that improvement in cyberwarfare of a nations cyberspace enhance national security and vice versa.

STATES WITH CYBERWARFARE INCORPERATED IN IT'S MILITARY DOCTRINE TO ENHANCE NATIONAL SECURITY

CYBERWARFARE & NATIONAL SECURITY:

AN IMPERATIVE OF NIGERIAN ARMY PREPAREDNESS

"The supreme art of war is to subdue the enemy without fighting"
- Sun Tzu's *The Art of War*

Twitter@Fredwave

By: Ikerionwu Fredrick
Web Developer

JA Lewis in his study "Cyber Security and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization" identified 33 states that are planning to include cyberwarfare in their military planning and organization to combat cyber terrorism. The United States (US), United Kingdom (UK), France, Germany, Russia and China have already incorporated cyberwarfare as part of their military doctrine to improve national security. The nature of threat to national security has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, scale, and power of an attack with dire consequences on national security.

The United States.

The United States has focused on cyber security since the 1990s. Responsibility is divided between the Department of Homeland Security, the Federal Bureau of Investigation, and the Department of Defense, including the new US Cyber Command (which has the National Security Agency as one of its components). Offensive operations are most likely assigned to Cyber Command and to elements of the Central Intelligence Agency. The Department of Homeland Security has primary responsibility for domestic defence. Its National Cyber Security Division is tasked to "work collaboratively with public, private, and international entities to secure cyberspace and America's cyber interest". Cyber Command, a military subcommand under US Strategic Command, is responsible for dealing with threats to the military cyber infrastructure. In order to facilitate cooperation, the Department of Defense and the Department of Homeland Security signed a memorandum of agreement on cyber security in October 2010 to increase interdepartmental collaboration. The May 2011 *International Strategy for Cyberspace,* states that the United States "reserves the right to use all necessary means" to defend itself and its allies and partners, but that it will "exhaust all options before [the use of] military force".

The Republic of Korea

In 2008 *Korean Defense issued a white paper* identifying cyber security as an essential component of it's national defence. The White Paper also details the security measures taken by the Ministry of National Defence to protect the Defence Information Network as well as the Battlefield Management System. Korean Ministry of National Defence has a Cyber War Centre, created in January 2010. Its primary aim is to increase the security of government and financial information networks. The Defence Ministry also stated it's interest on creating an independent Cyber Warfare Command responsible for defensive and offensive operations in cyberspace. The military and Korea University collaborates in the creation of a cyberwarfare school where students will be trained to deal with a variety of cyber threats. Upon graduation, the students will become military officers working in cyberwarfare units.

South Africa.

In early 2010, the South African Cabinet and the Ministry of Communication developed the requisite legislations in order to effectively combat cyber terrorism. In 2011, follows the enactment of cyber security policy aimed at creating institutional capacity to respond to these challenges. This effort contributed to the successful establishment of a Cyber Inspectorate in 2012, to establish relevant structures, reduce threats, facilitate cooperation between government agencies, and build it's cyberwarfare capacity.

Nigeria.

Nigeria is very concerned with the negative effects of cybercrime on its economy. A National Cyber security Initiative, created by a Presidential Committee, was tasked to create cyber security recommendations. They issued three main recommendations: raise awareness on cybercrime, pass new legislation criminalizing certain cyber activities, and build Nigeria's institutional capacity to combat cybercrime. In 2004, the Nigerian Cybercrime Working Group was established to implement these recommendations within a two-year time frame. After two years, the Directorate for Cyber security was created within the Office of the National Security Adviser, to continue to update Nigerian cyber policy and to coordinate these efforts.

From the study, it is obvious that nations all over the world are increasingly incorporating cyberwarfare in their military doctrine as a means to counter cyber terrorism and enhance national security on their nation's borders. The strategies being employed by the nations examined are dependent upon the nature and dynamics of cyber threats being experienced in their countries. This is instructive for NA in preparation to counter any form of cyber terrorism to counter the prevalent threat on its national security**.**

LESSONS FROM OTHER COUNTRIES ON CYBERWARFARE AND NATIONAL SECURITY

In essence, the increasing reliance of the Nigerian Armed Forces on sensors, computers and information systems, translates to vulnerability to cyber-terrorism. Therefore, it is important to introduce strategies to stem these new threats and vulnerabilities as a means to enhance national security.

Cyberspace Legislation.

Cyberspace legislations are increasingly being put together in the countries examined. These are requisite legislations that would aid to enhance their cyber defence initiatives. For instance, South Africa's preparation has been along provision of appropriate legislation to address the issues of cyber attacks thereby, impacting positively on its national security. Nigeria like South Africa needs to legislate against cyberwarfare to enhance national security.

Cyber Defence Initiatives.

Comprehensive cyber defence initiatives and cyber doctrine have already been developed by the USA in preparation for full blown cyberwarfare. However, Nigeria does not have any in spite of the emerging threat. Therefore, there is the need for the NA to assess the nature of its cyber threat with the view to determining the strategies to be adopted against any cyber related attack that could undermine Nigeria's national security.

Manpower Development.

One obvious consequence of the advancement in technology is the complex nature of the modern battlefield. This was brought about by the constantly improving IT systems and their application in weapon systems. The study from the Republic of Korea revealed that high level of computer knowledge is essential in building capacity for application or incorporation of cyberwarfare in military doctrine. "A highly skilled manpower (work force), is sine quo non to high productivity". Consequently, the NA needs to train more IT personnel with emphasis on computer programming, cybernetic and computer hardware maintenance.

CONCLUSION

Sun Tzu in The Art of War says ""If you know the enemy and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, for every victory gained you will also suffer a defeat; if you do not know your enemies nor yourself, you will succumb in every single battle." Cyberwarfare is an instrument of national policy at the nexus of technology, policy, law, ethics, and national security.

However, efforts made by other developed and developing countries in improving their military capability in cyberwarfare as reviewed in this paper are of great imperative to the NA, hence NA is one of the major stakeholders on implementing the Section 217 (2) of the 1999 Constitution. The paper examined cyberwarfare capability in the NA and its implications for national security. The study also appraised the relationship between cyberwarfare and national security. Having seen the prominence and significance of cyberwarfare in other countries reviewed, it is therefore interesting and equally important for the NA to incorporate cyberwarfare on its military doctrine to enhance national security.