Scientia Africana, Vol. 20 (No. 3), December, 2021. Pp 241-256 https://dx.doi.org/10.4314/sa.v20i3.20
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

A SURVEY ON GLOBAL CYBER-WARFARE AND NIGERIAN'S CYBER DEFENSIVE STRATEGY: A WAY FORWARD.

Usman, S. D., Junaidu, S. B., Obiniyi, A. A. and Bagiwa, M.B.

Department of Computer Science, Ahmadu Bello University Zaria, Kaduna State, Nigeria.
*Corresponding authors e-mail address: captsdusman@gmail.com

Received: 10-11-2021
Accepted: 05-12-2021

ABSTRACT

With two years having passed since the infamous cyber conflict between Estonia and Russia, on 08 May 2009 international society still lacks a coherent set of principles, rules, and norms governing state security and military operations in cyberspace. For parties committed to promoting the cause of peace and stability in a multipolar world, this is a troubling notion since history shows that the likelihood of a new arms race is high when disruptive technologies dramatically alter the means and methods of war. As more nations aspire to project national power in cyberspace, a new digital arms race appears to be imminent if not already upon us. Thus, there is a central question confronting international society and Nigeria in cyberspace: What steps can be taken both today and into the future to forestall a major arms race and interstate competition in cyberspace? In order to begin addressing this complex question from the perspective of the Euro-Atlantic Community, this paper discusses both the challenges and opportunities of regulating 21st century cyber warfare. The paper is divided into sections, which examine the evolution of the laws of armed conflict (LOAC) since the late 19th century, how the LOAC apply to cyber warfare as viewed primarily from a US perspective (since US scholars have dominated the international regime discourse thus far), and the historical facts on cyber warfare. The Nigerian roles in cyber defense strategy and what is needed to be done to meet up with a global regime for cyber warfare in respect of cyber defense are also highlighted. Global cyber strategies, threats/attacks, and types of cyber weapons d

Keywords: Conflicts, Cyber, Warfare, Revolution, Military, Defense, Strategy

INTRODUCTION

The world is addicted to computers and Nigeria is no exception. It is estimated that the U.S. Department of Defense uses more than 5 million computers on 100,000 networks at 1,500 sites in 65 countries worldwide [1,2,3]. This does not include computers embedded in weapons and weapons systems. While this is a significant amount of computers, it becomes miniscule when compared to those used by businesses or even those used by private citizens in homes across the country. The worst possible consequences of risks created by information and communication technologies manifest themselves in the possible failure of so-called critical infrastructures, which are systems and assets whose incapacity or destruction would have a debilitating impact on the national security and the economic and social well-being of a state [1]. Driven by a growing concern for the potential vulnerability of networked societies together with an increasing number of disruptions in the cyber-domain, many countries have taken steps to better understand the vulnerabilities of and threats to their (information) infrastructures, and have proposed measures for the protection of these assets.

Cyberspace serves as an adjunct to conflict in the physical domain and therefore shares many of the same characteristics (cite reference 2009). In cyber warfare weapons are predominantly military and dual-use; adversaries can be identified and deterred; the terrain is predictable; defense is the position of strength; and offensive actions risk vulnerability as one maneuvers upon the battlefield. Cyberspace has extended the battlefield and should be viewed as the fifth battle space alongside the more traditional arenas of land, air, sea and space. Cyber-attacks are just one component of the strategic ways and means available to a state or organized non-state group. As such, wars like challenges in cyberspace are more likely to occur in conjunction with other methods of coercion and confrontation.

However, the ways and means of cyber warfare remain undeniably distinct from these other methods. The weapons are almost always dual-use, in the sense that they are lines of code and physical hardware that can be modified for other purposes. Problems with attribution mean that adversaries are nearly impossible to identify and therefore deter. The terrain (cyberspace writ large) is constantly shifting and expanding. Offensive cyber weapons have been developed by multiple countries that could create havoc and damage to our information infrastructure. Cyber Arms have become easier to obtain, easier to use, and much more powerful. These weapons are a fraction of the cost of the conventional weapons such as tanks, fighter-jets and naval assaults crafts. Therefore, State or groups sponsored attacks against information systems using computer viruses and other techniques should be considered an act of war. We had now entered a new age of conflict.

When viewed systemically, the current generation of cyber weaponry demonstrates an enormous potential to alter the means of hostile attack and in turn of response. While our 21st century armed services are adjusting to the Revolution in Military Affairs (RMA), the broader community of business, transportation, energy, research, health, academic, and social services look up to their national leaders to provide plans and to conduct operations that will protect their domain of cyber space. Cyber defense for those old enough to remember may call to mind the home front nuclear alert drills plus the bunkers or bomb shelters constructed in the post-Second World War (WWII) decades. In cyberspace both military and civilian networks are potential targets.

Overarching questions confront us: What is the current state of cyber warfare when viewed from an international affairs perspective? What options are available to policy makers that seek to fashion a global regime to govern 21st century cyber warfare? And more specifically to the theme of the first **North Atlantic Treaty Organization (NATO)** cyber war conference, what role can an international military alliance such as NATO play in advancing such a regime? Since the enormous attack on Estonian digital networks, governments around the world have ordered their respective military branches to develop new offensive and defensive cyber capabilities. Some states have even gone as far as creating national cyber command authorities, as is evident in the United States [4, 5, 6].

However, as the attacks mount and more advanced 'cyber weapons' are introduced to the digital battlefield, there is little certainty or international consensus on the rules, or lack thereof, for governing modern cyber battles or larger warfare. Air Force Gen. Kevin P. Chilton, the head of U.S. Strategic Command (STRATCOM) issued a statement in May of this year that 'The Law of Armed Conflict will apply to this domain'[3, 29]. STRATCOM defends the Pentagon's Global Information Grid at home and abroad through its Strategic Command Joint Task Force-Global Network Operations (JFTGNO). Attempted penetrations of public and private systems number in the tens of thousands a day. As a commander who provides information for decisions by the US President and the Secretary of Defense, Gen. Chilton said that all combat options should be on the table for a US response to a cyber-attack. He noted that many attacks thus far have been for the purpose of espionage, and that there can be an argument about the 'semantics of attack versus espionage and intrusion' [7,8,9].

This paper examines and makes recommendations on the state of Nigeria's Readiness and Defensive Strategies in place to counter any type of cyber threats/attacks within Nigeria. It outlines the debilitating impact of cyber security system on the national security, economic and social well-being of Nigeria as well as its impact on National Information Infrastructure (NII), Defense Information Infrastructures (DII) and Global Information Infrastructure. The findings from this research work will be of immense benefit to the Nation as it will guide her in reviewing her cyber security strategy in securing NII, DII and GII as well as act as a reference point for other researcher that wishes to embark on similar research work.

LITERATURE REVIEW AND RELATED WORKS

The world realized in the late 1990s, when terrorists began to acquire advanced technologies that could help them wage cyber war against the civilized world. In 1998 and 1999, Russia proposed that the First Committee of the United Nations explore an international agreement on the need for arms controls for information warfare weapons. At this time, NATO does not define cyber-attacks as clear military actions.

The largest cyber-attack in the world occurred in 2001 when the Code Red and Nimda worms were released and rapidly spread globally. Collectively nearly 1 million computers were impacted. Consequently, the G-8 Government-Industry Conference on High Tech Crime in 2002 sought international agreement on ways to classify and control malicious computer code.

In 2006 the country of Estonia experienced the first cyber war. The Estonia Cyber-attack was unprecedented in size and scope and should alarm every nation around the world. Top selected targets in Estonia's Cyber War included:

- The Estonian Presidency and Parliament.
- Most of the Estonian Government's Ministries.
- Political parties.
- The top three of the country's six big news agencies.
- Two of the biggest banks.
- The Nation's telecommunications infrastructure providers.

In 2007, the United States Army and Air Force began efforts to acquire offensive cyber weapons. New Zealand officials reported finding spyware and other evidence on their computers and cyber forensic investigators were able to track the attacks to China. Technolytics found that 97% of cyber-attacks take advantage of known security vulnerabilities while using commonly available hacking tools or non-sophisticated cyber weapons [5, 27, and 37].

In September 2007, Lou Qinjian, China's Vice Minister of Information Industry accused the United States and other western countries of conducting a campaign of computer attacks and infiltration via the Internet. Hackers around the world have made sophisticated Distributed Denial of Service Attacks (DDoS) tools available on websites and claimed responsibility for hundreds of attacks. Computer experts fear that cyber skirmishes could escalate to a full blown cyber war if not a Cyber World War. NATO provided technical support to Estonia during the three week attack in late spring of 2007. NATO deployed some of its top cyber terrorism experts to Tallinn to investigate and to help the Estonians beef up their electronic defenses [6, 26].

Recently, USA in the year-2013~~,~~ recorded cyber-attacks launched at some of its financial institutions (the largest ones). While North Korea and China posed cyber threats to South Korea and USA Forces deployed at South Korea respectively.

Types of Cyber Threats/Attacks

There are varieties of threats in cyber space. Let's examine the prominent ones among them:

- One such threat is that of malicious code being embedded in firmware of computer or application software from foreign suppliers. This is perhaps the hardest threat to detect or to defend against.
- A foreign supplier of software or computers could easily slip harmful code in amongst the tens of millions of lines of code that come installed on the hard disk. Some industry experts even believe that this could also occur in the BIOS (Basic Instruction Operating Set).The BIOS is software that runs during the startup sequence where it configures devices and then boots the system. Every time you turn on the computer or other device, the malicious code would initiate and wait to arm itself and become a cyber weapon.
- Computer Virus Attacks (CVA) - A virus is a harmful software program that is secretly introduced into a system with the characteristic feature of being able to generate and distribute multiple copies of it, and thereby

Classification of Cyber Weapons

Cyber Weapons are defined as computer programs that are developed or utilized for the destruction of confidentiality, integrity and availability of computer data and systems [15, 20] Cyber Weapons are often considered as Weapons of Mass Disruption. Cyber Weapons are typically classified into three categories:

- Offensive
- Defensive
- Dual Use

TYPES OF CYBER WEAPONS

There are various types of software weapons which include; computer worms, software vulnerability exploitation, info-blockades, root kits, botnets, malicious embedded code, key loggers, IP spoofing, logic bombs, sniffing, spamming, trap doors, Trojan horses and video morphing. The following are the three most deadly cyber weapons [16, 17]:

- Electromagnetic pulse weapons; were designed to destroy the electronic underpinnings of the modern military as well as business. This class of weapons operates by using pulses or beams of electromagnetic energy to disrupt or destroy electronic components in a computer, missile, tank, or any smart weapons that have not been properly hardened against this type of attack.
- Directed Energy Weapons (DEWs) have been under developed for the last three decades. In the last few years they have emerged from the lab and into field trials. This class of cyber weapons is capable of disabling enemy computer systems without the use of explosives. DEWs include high energy microwaves (HEWs), high power microwave (HPWs) and transient electromagnetic devices (TEDs).
- AneBomb is another weapon that uses an intense electromagnetic field to create a brief pulse of energy that affects electronic circuitry without harming humans or buildings.

Samples of Cyber Weapons

Figure 1:**Electromagnetic pulse weapon**September of 2007Figure 2: **Directed energy weapons**September of 2007

Figure 3**:e Bomb weapon** September of 2007

Cyber weapons can also be precision strike devices. The characteristics; a specific computer virus might focus on a very specific piece of infrastructure like the power grid. Others include:

- Electronic countermeasure
- Defense shields against electronic attack

- Infrared decoys
- Angle reflectors
- False-target generators
- Root kits
- Malicious code
- Transient electromagnetic devices
- Trojans
- Spyware
- Back-doors in commonly used software
- Autonomous mobile cyber weapons
- Key loggers
- Viruses
- Worms and many other exploitation techniques

Characteristics of Cyber Weapons

There are two key characteristics of cyber weapons; versatility and propagation [18, 19].

- Versatility – This is the ability to generically attack a wide variety of applications. Most of them do not even require information about the program they are infecting.
- Propagation – Once a computer virus has affected a program – while this affected program is running - the virus is able to spread to other programs and files accessible to the computer system.

Each virus has a destructive payload that is activated under certain conditions. When activated a virus can corrupt, alter, or destroy data, generate bogus transactions, and even transfer information.

Distributed Denial of Service Attacks (DDoS) - DDoS attack is launched from as many remote computer systems as a hacker can compromise. When DDoS are launched, the attacks are hard to stop because the data flood originates from many computers from multiple locations. Typically, systems managers are unaware that their machines are attacking other systems. In this type of attack, websites are suddenly overloaded with traffic (sometimes tens of thousands of bogus hits), jamming and disabling websites by overloading the bandwidth of the site or processing capabilities of the servers running the sites. These attacks can and often are launched from computers that have been compromised all over the world.

Global Cyber Attacks/Threats

Moonlight Maze- is the U.S. government's code name for a series of coordinated attacks on U.S. computer systems in 1999. These are two years attacks that were discovered by the Department of Defense. The attacks were traced back to a mainframe computer in Moscow but it was unclear at this point if that is where they originated or who was behind the incidents.

Titan Rain was the U.S. Government's code name for an ongoing series of cyber-attacks on U.S. computer systems since 2003. Titan Rain is thought to rank among the most pervasive cyber security threats that U.S. computer networks have ever faced.

At this time investigators believe that this is a coordinated attack involving about two dozen hackers. Just recently, the "Titan Rain" code name has been changed, and the new name for the attacks is classified [12, 13, 21, 42]

Cyber Warfare Technology

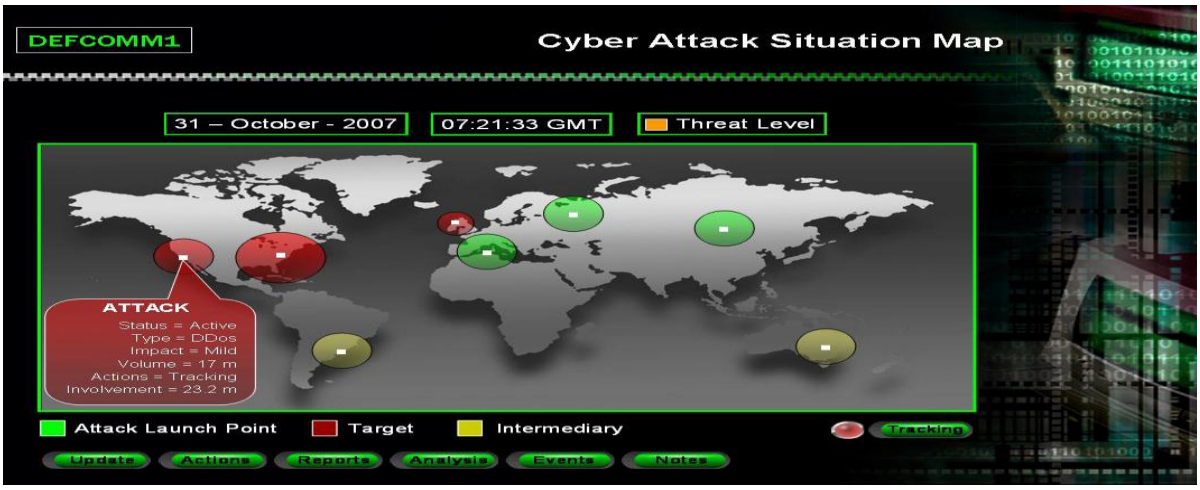


Figure 4: Cyber Attack Situation Map September 2007

The cyber-attack situation map above illustrates three points of attacks: one on the west coast and a second on the east coast of the U.S. and the third in the U.K. Additionally, this map also shows the status of the attacks on the west coast of the United States and illustrates the three points of attacks and the two intermediaries being used.

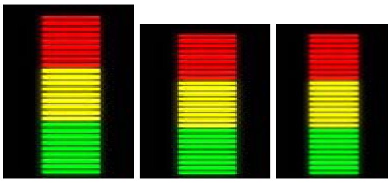
This is similar to the displays used at North American Aerospace Defense Command (NORAD) at PETERSON AIR FORCE BASE in Colorado. Case Example: There has been a massive, broad and successful series of attacks targeting the private sector and key government systems [39, 40, 41]. The U.S. Department of Defense confirmed in September of 2007 that cyber-spies sifted through some government computer systems.

They did not discuss or admit to the extent of damage that had occurred as a result of these attacks. This announcement follows allegations from Britain and Germany of attacks originated by China. Of course, Beijing denies launching cyber-attacks.

Measures of Success: How will you measure success and progress? This will be a challenge. The area of cyber security is hampered by its lack of adequate metrics and measures. Without such a measure and uniform reporting, it is difficult to assess the risks and progress toward security of cyber systems. [14] Here is an illustration of the Performance Measures:

- The time to respond to and contain a cyber outbreak.
- The time to respond to and mitigate a cyber-attack.
- The total times in hours computers or servers are down due to a cyber-attack.
- The total number of computers impacted by a cyber-attack.

Attacks Status



Attacks Impact Recovery

Figure 5: Attack Status

Metrics:

- Vulnerabilities reported before 1st exploit.
- Number of cyber emergency contacts.
- Number of cyber-attacks per month.
- Number of cyber-attacks per quarter.
- Number of cyber-attacks per year.
- Type of cyber-attacks.

If we fail to properly monitor cyber-attacks and measure the organizations' success, defending against and responding to these attacks will be an effort in futility. These and other measures must be designed to ensure our defenses for a cyber war. Remember, you get what you measure.

Global Cyber IT Security Conference Held in Nigeria

It is gratifying to state here that, Nigerian Defense Headquarters (NDH) is not resting on its oars as regards the war against the cyber Threats/Attacks. It was with these views that, the Headquarters Organized and hosted World Cyber IT Security Conference on 23 June, 2011 at the Command Officers Mess, Asokoro, Abuja.

The aim was to adequately sensitize members of the Armed Forces, principal officers of security agencies, the paramilitary formations and captains of industries in all aspects of the economy on how to secure the virtual world for National Security. This is in partnership with EC-Council, an international cyber security education body and New Horizons, world's largest IT and business skills training company with presence in 70 countries and on 6 continents [7, 25, 48,].

Cyber Warfare and Nigeria's National Security

In view of the contract awarded Elbit Systems by the federal government, Ojo Maduekwe inquired from cyber intelligence experts if there is no other way of spying on terrorist activities in Nigeria than monitoring phone conversations and reading private email messages.

Although the federal government has decided to remain silent regarding the matter of the contract awarded Israeli firm, Elbit Systems, the incidence has raised a number of issues that should not be swept under the carpet in a hurry until appropriate answers are provided. One is that in an age where most countries economic, political and social activities have gone online, it becomes perplexing that Nigeria is still contented at operating offline. Unlike in developed countries, the internet is not considered as part of the country's critical infrastructure.

Another issue is that, if Nigeria as a country must advance like the rest of the world, then the issues of cyber threats faced and experienced by countries like America must not be dismissed with a wave of the hand. This should not make us shy away from the benefits that come with the internet. In addition, now is the right time to seriously consider the strategies, tools, and techniques that would be proper in addressing issues of cyber security. Countries that have witnessed their public agencies online activities, including military apparatus, threatened have come to understand that cyber security is a part of national security and is bigger than what individual organizations can handle by themselves [38, 44, 45].

The government must be involved since they continually pledge by the constitution to secure lives and properties of the citizens. The most discussed issue that has been raised by the Elbit Systems contract is whether invading the citizen's privacy, through listening to phone conversations and reading personal email messages, is the only way the government can provide the much needed security. The $40 million contract awarded to Elbit Systems by the federal government is for "internet surveillance and for the purpose of gathering intelligence and national security" [8, 24, 49]. The company's global press release explained that it will supply its Wise Intelligence Technology (WiT) system to an unnamed country in Africa under a new $40 million contract announced 24 April for "Intelligence Analysis and Cyber Defence."

Opinion from a cross section of Nigerians revealed that it was not the nature of the contract that got people worried, neither was it the profile of Elbit Systems. The company is reputed as being "a world leader in the fields of intelligence analysis and cyber defense, with proven solutions highly suitable for countries, armies and critical infrastructure sites."

Naturally the contract should not have been a source of worry to any right thinking individual since its purpose is to "track down terrorist activities online." on 9 June 2011. The worry comes with the fact that history is replete with governments of different countries abuse of such enormous power that gives them the legitimate access to their citizen's private lives. A Cyber Intelligence Expert and Ethical Hacker with Centrex Ethical Lab, Nsikak Joseph, explained the nature of the contract thus: on 9 June 2011

This project will be more offensive than ordinary intelligence gathering or record keeping system. I will classify it as a "Black Operation Programme." For CEO of Digital Encode, a Lagos-based cyber security outfit, Adewale Obadare: "This is one of the most far-reaching policies ever designed in Nigeria's history to invade the privacy of citizens by secretly awarding Elbit Systems, a spy contract on Nigerian citizens. As usual, the justification is that only by having access to our confidential communications can the law enforcement agencies and security services keep us safe from criminals and terrorists."

Monitoring System with or without the Elbit Systems contract, the fact according to experts, remains that our online and in extension offline activities are already being monitored.The Internet as a whole has no privacy; the biggest technology being used in the world today is the biggest spy project in the world, said Joseph. Maintaining privacy on the Internet is nearly impossible.

In addition, Obadare said:

Google tracks us both on its pages and on other pages it has access to as well as its range of android devices. Same with Facebook - it even tracks non-Facebook users. Apple tracks us on our iPhones and iPads. One reporter used a tool called Collusion to track people who were tracking him [9, 10, 23].It was reported that over 100 companies tracked him during a 36-hour period. Facebook, for example, correlates your online behaviour with your purchasing habits offline even your cell phone has location data. This is a clear case of all round surveillance. We are all being watched at all times, and that data being stored forever. These available data can be analyzed and effectively used in tracking online criminal activities.

As the world converges, online and criminal elements decide to take advantage of such gathering, we must act to protect ourselves and our properties. Nigeria's cyber security issues could be addressed through both overt (open) and covert (clandestine) sources. Open Source Information (OSIF) comprises data garnered from newspapers, books, broadcast, and general daily reports which are publicly available.

The covert system remains the most effective as the clandestine Cyber HUMINT is still the best way of spying on criminal systems. But such operation needs to have a legal framework, cyber laws etc

The current plan described in the National Strategy to Secure Cyberspace does not ensure that companies will implement sound security practices in Nigeria since determining the source and veracity of attacks is difficult. An attack might be traced to computers in a given country, but that doesn't mean the government of that country is behind it. It might be launched by zombie machines in that country but are controlled by someone else.

Therefore, having an in-depth knowledge of the various aspects of IT Security will not only benefit the armed forces but the Security experts within and outside the country. The recent steps taken by the Government to review the national strategy is an excellent welcome development but, it should be directed to take proper account of Nigerian Cyber Defense.

Cyber Warfare Strategy

Cyber war has significant different strategies, tactics, targets and weapons. Military leaders worldwide have a challenge when it comes to recruiting and training the new type of soldier for Cyber warfare. The advanced education and skills required in computer science coupled with the high demand for the same resources in the private sector make these huge issues.

Cyber warfare must be analyzed systematically, rather than presented and interpreted as a series of alarming anecdotes. Cyber warfare is a complex, fast-evolving political and technological phenomenon which can only be understood and managed if placed within a framework of national strategy [11, 22, 43].

CONCLUSION

While cyber warfare is not an entirely new area of modern warfare (at least as viewed within an Internet world), its current evolution poses many challenges to international peace and stability. The increasing quantity and quality of online attacks threaten many parts of civil society

Scientia Africana, Vol. 20 (No. 3), December, 2021. Pp 241-256 https://dx.doi.org/10.4314/sa.v20i3.20
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

that depend on reliable networks and information systems. Growing evidence of state-sponsored cyber attacks is especially alarming and could spark a serious arms race in cyberspace. Understandably, a number of countries have announced plans for full spectrum military cyber commands. As history has demonstrated, while international law cannot stop states from going to war with one another, it can go a long way towards regulating their conduct should hostilities boil over into actual war.

Some may argue that because cyber warfare is still in its formative stages, it is premature to begin work on a global regime to regulate it. However, it can also be logically argued that in the absence of some rules of the game, states will not feel constrained to develop and deploy cyber weaponry if the consequences are not understood by both military and civilian planners. While it is difficult to estimate the true potential for a catastrophic attack to spill over to kinetic warfare between states, the notion that the threat exists at all is cause enough to begin constructing a regime or legal framework through which to conduct cyber warfare.

History presents another lesson in that even with the best intentions and resources, a global cyber security regime will not transpire in short order. It will take many years to form an effective international consensus that might translate into a revision of the Law of Armed Conflict as spelled out by the Geneva Conventions. The operative concept is regime. And, the time to establish a global cyber security regime is now. As a proper follow-up to the innovative inaugural Tallinn CCD COE conference of 2009, NATO can and should play an important role by bringing together in short order the relevant stakeholders to outline a viable cyber security regime.

For cyber warfare to be fully understood it must be analyzed systematically and placed within a framework of national strategy. Strategy is concerned with the relationship between ends, ways and means. The national strategic framework is more than an explanatory device. However, by placing cyber warfare within a Clausewitzian politico-military model in which warfare is considered to be a phenomenon both constrained and validated by politics.

The Nigerian Defense Headquarters, should therefore, be poised to tackle the issues of Cyber attacks or threats to the Nigerian cyber space heads-on with the acquisition of relevant knowledge aimed at adequately beefing up security amongst its personnels.

Offensive cyber weapons have been developed by multiple countries that could create havoc and damage to our information infrastructure. There is therefore, an urgent need for countries and organizations especially Nigeria to brace up to this challenge by designing and developing a very strong counter measure to this menace.

RECOMMENDATIONS

The best option now may be to create and empower a Robust Cyber Security Agency to be named- ***NIGERIAN CYBER DEFENSIVE STRATEGY CENTRE.*** This agency will be responsible for coordinating and providing the cyber defensive capacity across the government, multiple organizations like the business industry and offensive operations within the Nigerian cyber domain.

One thing is sure, success in future conflicts will depend less on Bombs and Bullets, but more on Bits and Bytes respectively. The following is a list of suggested regulatory requirements: Registration of emergency cyber contact, Requirement of minimum protective measures, Reporting of cyber-attacks and incidents, Reporting of software vulnerabilities and Regulating and controlling cyber arms internationally.

- "Security...is everyone's Business," therefore, the organization shall work with business, industry and government agencies to design, implement, and maintain effective defensive cyber capabilities. They will work with key stakeholders to minimize risks associated with cyber attacks by effectively developing and promoting adoption of the latest best practice models and supporting technology solutions.

- Our National Strategy to Secure Cyberspace must actively engage the private sector that has a crucial role in protecting national security because it largely runs the nation's critical infrastructure. Tightly coupling business and industry into the Cyber War Defense strategy is arguably the most critical component and the one area that the Government has to properly tackle.

- The National Strategy to Secure Cyberspace must contain language that requires by law that business, government and industry adopt a set of minimal cyber security measures to protect the nation's information assets.

Remember! If we fail to create and empower this agency to mandate cyber protections and take corrective actions with those who fail to comply then, the entire nation would be at risk of falling victim to cyber-attacks/threats. Consequently, history and future generations of Nigerians may not forgive such grievous negligence of our responsibilities. Security is money and money is Security! If Nigeria fails to seriously plan against cyber threats and attacks, it becomes imperative that she has planned to fail in the area of cyber security.

REFERENCES

Arquilla, John and David F. Ronfeldt (1996*): The Advent of Netwar (*Santa Monica: RAND).

Arquilla, John and David Ronfeldt (eds.) (2001): *Networks and Netwars:BThe Future of Terror, Crime, and Militancy* (Santa Monica: RAND).

Ashby, W. Ross (1956*): Introduction to Cybernetics (Methuen, London).*

Akdeniz, Yaman (1999): *The Regulation of Internet Content in Europe: Governance Control versus Self-Responsibility,* in: Swiss Political Science Review, 5, 2: pp. 123-31.

Bourdieu, Pierre (1991): *Language and Symbolic Power* (Cambridge: Harvard University Press).

Buzan, Barry, Ole Wæver, and Jaap de Wilde (1998): Security*: A New Framework for Analysis* (Boulder: Rienner).

Baird, Zoë (2002): Governing the Internet: *Engaging Government, Business, and Nonprofits, in: Foreign Affairs,* 81, 6, pp. 15-20.

Baldwin, D.A. (1997): *The Concept of Security, in: Review of International Studies*, l 3,13: pp. 5-26.

Stars and Stripes (2009) 'Pentagon Steps Up to Fight Cyber War' (30 May 2009) http://www.military.com/news/article/pentagon-steps-up-to-fight-cyber-war.html?col=1186032310810

Scientia Africana, Vol. 20 (No. 3), December, 2021. Pp 241-256 *https://dx.doi.org/10.4314/sa.v20i3.20*
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

Bendrath, Ralf (2003): *The American Cyber-Angst and the Real World- Any Link?, in: Robert Latham* (ed.): Bombs and Bandwidth: The Emerging Relationship between IT and Security (New York: The New Press), pp. 49-73.

Bosch, Olivia (2002): *Cyber Terrorism and Private Sector 21forts for Information Infrastructure Protection, paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures* (Seoul, 20-22 May 2002).

Campen, Alan D. and Douglas H. Dearth (eds.) (1998): Cyberwar 2.0: Myths, Mysteries and Reality (Fairfax, AFCEA International Press).

Cyber Warfare and Nigeria's National Security*, a Conference held in Abuja-Nigeria* on 10 July 2012

Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel (2004): *The Economic Impact of Cyber-Attacks, Congressional Research Service Documents,* CRS RL32331 (Washington DC).

Chapman, Gary (1998): *National Security and the Internet, paper presented at the Annual Convention of the Internet Society* (Geneva, July 1998).

Cukier, Kenneth Neil (1999): *Internet Governance and the Ancien Regime, in: Swiss Political Science* Review, 5, 1: pp. 127-33.

Denning, Dorothy E (1999): Activism, Hacktivism, and Cyberterrorism: *The Internet as a Tool for Influencing Foreign Policy, presented at Internet and International Systems: Information Technology and American Foreign Policy* Decisionmaking Workshop, 10 December).

Dorothy E. Denning (2001): *Obstacles and Options for Cyber Arms Controls, paper presented at Arms Control in Cyberspace* Conference, Heinrich Böll Foundation, Berlin, Germany, June 29-30. URL: http://www.cs.georgetown.edu/~denning/infosec/berlin.doc [last accessed on 10 June 2005].

Dunn, Myriam (2005): *The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP), in: International Journal for Critical Infrastructure Protection,* 1, 2/3: pp. 58-68.

Eriksson, Anders E. (1999): *Information Warfare: Hype Or Reality?, in: The Non-Proliferation Review,* 6, 3: pp. 57-64.

School, Jeff (2009) 'official: No options 'off the table' for U.S. response to cyber attacks**'**, Stars and Stripes (Mideast edition, 08 May 2009).http://www.stripes.com/article.asp?section=104&article=62555

Eriksson, Johan (2001) (ed.): *Threat Politics: New Perspectives on Security, Risk and Crisis Management*. (Aldershot : Ashgate).

French, Geoffrey S. (2000): *Shunning the Frumious Bandersnatch: Current Literature on Information Warfare and Deterrence (Washington DC: Information Warfare ResearchCenter*).

Giacomello, Giampiero and Fernando Mendez (2001): Cuius Regio, Eius Religio, Omnium Spatium? State Sovereignty in the Age of the Internet, in: Wenger, Andreas (ed.): *The Internet and the Changing Face of International Relations and Security. Information*

Geneva Conventions: A Reference Guide' (2009) *Society of Professional Journalists. http://genevaconventions*.org (Accessed: 01 June 2009)

Goldman, Emily O. (2001): New Threats, New Identities and New Ways of War: *The Sources of Change in National Security Doctrine, in: Journal of Strategic Studies*, 24, 3: pp. 12-42.

Howarth, David (1995): Discourse Theory, in: March, D. and G. Stoker (eds.): Theory and Methods of Political Science (London: Macmillan): pp. 115-33.

Hanseman, Capt. Robert G. (1997) '*The realities and legalities of information warfare' Air Force Law Review*(42:1997).

Ingles-le Nobel, Johan J. (1999): Cyberterrorism Hype, in: Jane's Intelligence Review, 10/21/1999.

Kolet, Kristin S. (2001): *Asymmetric Threats to the United States, in: Comparative Strategy*, 20, 3: pp. 277-292.

Libicki, Martin (1995) 'What is information warfare?' ACIS Paper 3: August 1995; National Defense

Moteff, John, Claudia Copeland, and John Fischer (2003): *Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556* (30 August 2002). URL: http://www.fas.org/irp/crs/RL31556.pdf

[last accessed on 10 June 2005]. Papp, Daniel S. (2003): *Cyberterrorism: Threat (?) And Response, paper given at the CEEISA/ISA International Convention, Budapest, Hungary,* June 26 -28, 2003.

Gertz, Bill (2009) '*Cyber warfare plans' Inside the Ring*(04 June 2009) http://www.gertzfile.com/gertsfile/InsidetheRing.html

Porteous, Holly (1999): *Some Thoughts on Critical Information Infrastructure Protection, in: Canadian IO Bulletin,* 2, 4, October.vURL: http://www.ewa-canada.com/Papers/IOV2N4.htm [last accessed on 10 June 2005].

Rathmell, Andrew (2001): *Controlling Computer Network Operations, in: Wenger, Andreas (ed): The Internet and the Changing Face ofInternational Relations and Security, Information & Security An International Journal*, Volume 7: pp. 121-44.

Shea, Dana A. (2003): *Critical Infrastructure: Control Systems and the Terrorist Threat. CRS Report for Congress* (February 21, 2003). URL: http://www.fas.org/irp/crs/RL31534.pdf [last accessed on 10 June 2005].

Virilio, Paul (1995): Speed and Information: Cyberspace Alarm!, in: Ctheory, 18 March 1995.

Wiener, Norbert (1948): *Cybernetics, or Control and Communication in the Animal and Machine* (Cambridge: MIT Press).

Wolfers, Arnold (1962): *National Security as an Ambiguous Symbol, in Idem: Discord And Collaboration: Essays on International Politics* (Baltimore: Johns Hopkins): pp. 147-65.

Walker, Jeffrey K. (2001) 'T*he demise of the nation-state, the dawn of new paradigm warfare, and a future for the profession of arms' Air Force* Law Review (51:2001).

World Summit on the Information Society (2003): *Plan of Action. Document WSIS*-03/GENEVA/DOC/5-E, 12

December 2003 URL: http://www.itu.int/wsis/docs/geneva/official/poa.html [last accessed on 10 June 2005].

Yates, Athol (2003): *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment*. (Institution of Engineers, Australia).

Global Cyber IT Internation *Security Conference Held in Abuja-Nigeria*on 9June 2011).

Reynolds, Jeffrey. (2005) '*Collateral Damage on the 21st Century Battlefield'*, Air Force Law Review (56:2005).

Stephens, Dale and Michael Lewis (2005) '*The law of armed conflict—a contemporary critique' Melbourne* Journal of International Law (6:2005).

'ICRC-*International Committee of the Red Cross* (2009) 'The mission'. http://www.icrc.org/HOME.NSF/

Owens, William (2001) *Lifting the Fog of War (New York: Farrar, Straus*& Giroux).

University Press. http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html