UNIVERSIDAD DE LA DEFENSA NACIONAL
(Ley 27015 12/12/14)

FACULTAD DE LA DEFENSA NACIONAL

MAESTRÍA EN DEFENSA NACIONAL
(Res CONEAU 615/10)

TESIS DE MAESTRÍA

CIBERGUERRA Y SEGURIDAD NACIONAL EN NIGERIA: ANÁLISIS DE LAS CAPACIDADES DE LAS FUERZAS ARMADAS PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO (2009- 2018)

DIRECTORA: Mg. Sol Gastaldi

AUTOR: Coronel Jamiu Olayinka Are (Nigeria)

Buenos Aires
2020

CERTIFICACIÓN

Esto es para certificar que el proyecto CIBERGUERRA Y SEGURIDAD NACIONAL EN NIGERIA: ANÁLISIS DE LAS CAPACIDADES DE LAS FUERZAS ARMADAS PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO (2009- 2018), fue realizado por el Coronel Jamiu Olayinka ARE y completado bajo mi supervisión. Sin embargo, el participante es totalmente responsable de los contenidos de este proyecto.

…….. ……

Fecha **Mg. Sol GASTALDI**
Directora de Tesis

DEDICATORIA

Este proyecto está dedicado al Dios Todopoderoso por su gracia, fidelidad y protección extraordinaria en mi vida. Le entrego a Él todas las alabanzas y toda mi adoración por permitirme embarcarme en este trabajo y finalmente poder completar el mismo.

AGRADECIMIENTOS

Agradezco al Jefe de Estado Mayor del Ejército, Teniente General Tukur Yusuf Buratai, por encontrarme digno de la nominación para asistir a este curso en la Universidad de la Defensa Nacional Argentina. Que el Dios Todopoderoso continúe sosteniéndolo y otorgándole cualquier deseo que albergue su corazón. También quiero agradecer al decano de la Facultad de la Defensa Nacional, Dr. Julio César Spota, por sus palabras de aliento y sus esfuerzos por hacer que nuestra estadía en el curso sea muy interesante y cómoda. Además, agradezco el papel vital desempeñado por mi supervisora, la profesora Sol Gastaldi, por sus incansables y meticulosos esfuerzos para leer mi tesis. Ella hizo comentarios útiles, observaciones y correcciones que han enriquecido el contenido de este trabajo. Me siento muy honrado de tenerla como mi Directora y estoy realmente agradecido. Ruego que Dios Todopoderoso continúe favoreciéndola y bendiciéndola en todas sus tareas diarias. También quiero agradecer el apoyo inquebrantable y las minuciosas contribuciones de Trinidad Cerri. Ella personalmente se ofreció a ayudarnos con el idioma español y con la traducción nuestros power points de las clases y este trabajo de investigación. De hecho, contribuyó inmensamente para que nuestra estadía en Argentina valiera la pena y sus sacrificios personales jugaron un papel vital para ayudarnos a lograr nuestros objetivos principales de asistir al curso. Estoy muy agradecido, aprecio todo su apoyo y rezo para que Dios continúe bendiciéndola. Finalmente, quiero agradecer a mi querida esposa Adebimpe Are y a mi hijo Abdulkareem Are por sus oraciones, paciencia y aliento durante todo el curso. De hecho, son un pilar de apoyo y rezo para que Dios Todopoderoso continúe protegiéndolos y otorgándoles las cosas buenas de este mundo y del Más Allá.

TABLA DE CONTENIDOS

LISTA DE TABLAS Y FIGURAS

TABLAS

FIGURAS

LISTA DE ABREVIATURAS

AFN - Fuerzas Armadas de Nigeria

AFF - Estafas de Pago por Adelantado

BHT - Grupo Terrorista Boko Haram

CSIRT - Equipos de Respuesta a Incidentes de Seguridad Informática

CNI - Infraestructura Nacional Crítica

CNII - Infraestructura Nacional de Información Crítica

CT - Contraterrorismo

DRDB - Buró de Investigación y Desarrollo de Defensa

DCOC - Centro de Ciberoperaciones de Defensa

DCS - Dirección de Ciberseguridad

DSA - Administración Espacial de Defensa

DSS - Departamento de Servicios del Estado

DHQ - Cuartel General de Defensa

DDoS - Ataques de Denegación de Servicio

DIA - Agencia de Inteligencia de Defensa

GCI - Índice Global de Ciberseguridad

ISR (capacidad) - Inteligencia, vigilancia y reconocimiento

ICSP - Programa de Inteligencia y Ciberseguridad

IoT - Internet de las Cosas

ISWAP - Estados Islámicos de la Provincia de África Occidental

MOD - Ministerio de Defensa

NSA - Agencia de Seguridad Nacional

NCSPS - Política y Estrategia Nacional de Ciberseguridad

ngCERT - Equipo de Respuesta a Emergencias Informáticas de Nigeria

NIA - Agencia Nacional de Inteligencia

NCC - Comisión de Comunicaciones de Nigeria

NITDA - Agencia Nacional de Desarrollo de Tecnología de la Información

NDC - Colegio de Defensa Nacional

NDA - Academia de Defensa de Nigeria

NAF - Fuerza Aérea de Nigeria

NA - Ejército de Nigeria

NN - Armada de Nigeria

ODT - Teoría Ofensiva-Defensiva

ONSA - Oficina del Asesor de Seguridad Nacional

TIC - Tecnología de la Información y las Comunicaciones

TAF - Fuerzas Armadas de Túnez

UIT - Unión Internacional de Telecomunicaciones

LISTA DE APENDICES

CAPÍTULO 1:
INTRODUCCIÓN

Las computadoras y las redes que las conectan se conocen colectivamente como el dominio del ciberespacio, como el cibercrimen, el espionaje cibernético, el ciberterrorismo y la ciberguerra. Recientemente ha surgido el tema de la seguridad en el ciberespacio, en particular el creciente temor a la ciberguerra librada por un estado, o sus representantes, contra las redes gubernamentales y militares con el fin de interrumpir, destruir o negar su uso. Los países desarrollados dependen del ciberespacio para el funcionamiento diario de casi todos los aspectos de su sociedad moderna, incluidas las infraestructuras críticas y las instituciones financieras, mientras que los países menos desarrollados son cada vez más dependientes y están más conectados al ciberdominio. Por lo tanto, la amenaza de una ciberguerra y sus supuestos efectos son motivo de gran preocupación para los gobiernos y las instituciones militares de todo el mundo.[1]

El término ciberguerra refiere a actividades en el ciberespacio que implican el uso de armas de Tecnología de la Información y las Comunicaciones (TIC) para operaciones ofensivas y defensivas por parte de actores estatales y no estatales contra otros estados nacionales o actores no estatales. Dentro de las armas utilizadas en la ciberguerra se incluye la utilización de un software malicioso que tiene el potencial de explotar vulnerabilidades en sistemas militares o en la infraestructura nacional crítica como las áreas de comunicaciones, energía, comercio, transporte o sectores financieros con el fin de interrumpir o incapacitar sus operaciones óptimas.[2] La mayoría de los países han reconocido los riesgos en el ciberespacio y lo han designado como el nuevo dominio de la guerra que se une a los dominios tradicionales de tierra, mar, aire y espacio ultraterrestre. Actualmente, la mayoría de los conflictos interestatales modernos tienen dimensiones ciberespaciales. La ciberguerra se puede utilizar para llevar a cabo operaciones militares independientes, o puede servir como un multiplicador de fuerza para ataques cinéticos en otros dominios de guerra, por lo que la utilización efectiva de las capacidades de las naciones para enfrentar las amenazas del ciberespacio mejoraría invariablemente la seguridad nacional.

La seguridad nacional connota los esfuerzos agregados del gobierno para asegurar una nación y

[1] Sheldon, John B. **The cyber warfare: The invisible threat,** an article published in Britannica book of the year. Nov 2010.

[2] Carr, J. **Inside cyber warfare: Mapping the cyber underworld** Cambridge: O Reilly 2011, p.6.

preservar el bienestar de sus ciudadanos. Incluye el empleo de medidas políticas, diplomáticas, económicas y militares a fin de proteger la integridad territorial, la soberanía y los bienes de una nación, al tiempo que garantiza la seguridad, el bienestar y la preservación del estilo de vida de sus ciudadanos.[3] Una de las formas de preservar el bienestar de los ciudadanos es protegiéndolos de las vulnerabilidades asociadas con el uso del ciberespacio. Cuando el uso del ciberespacio de una nación se ve amenazado o atacado, le corresponde a la nación desplegar sus capacidades para enfrentar las amenazas del ciberespacio a fin de defenderlo de estos ataques, al mismo tiempo que mantiene la capacidad de responder de una manera comparable o más abrumadora. A la luz de esto, las naciones exploran continuamente formas y medios para desarrollar y ejercer sus capacidades para enfrentar las amenazas del ciberespacio a fin de mejorar su seguridad nacional.

El dominio del ciberespacio se compone de tres capas: la física, que incluye hardware, cables, satélites y otros equipos; la sintáctica, que incluye sistemas operativos informáticos y otro software; y la semántica, que implica la interacción humana con la información generada por las computadoras y la forma en que la información es percibida e interpretada por su usuario.[4]

Los ataques físicos generalmente ocurren durante conflictos convencionales, como la Operación Fuerza Aliada lanzada por la OTAN contra Yugoslavia en 1999 y la operación dirigida por Estados Unidos contra Irak en 2003, en la que las redes de comunicación, las instalaciones informáticas y las telecomunicaciones resultaron dañadas o destruidas.

Se pueden realizar ataques contra la capa sintáctica mediante el uso de ciberarmas que destruyen, interfieren, corrompen, controlan o que de otra forma dañan el software. Dichas armas incluyen software malicioso o malware, como virus, troyanos, programas espías y gusanos informáticos que pueden introducir un código corrupto o dañado. En los Ataques de Denegación de Servicio (DDoS, por sus siglas en inglés), los piratas informáticos o hackers, usando un malware, secuestran una gran cantidad de computadoras para crear botnets, grupos de computadoras zombies que luego atacan otras computadoras objetivo, impidiendo su correcto funcionamiento. Este método se usó en ciberataques contra Estonia en abril y mayo de 2007 y contra Georgia en agosto de 2008. En ambas ocasiones se alegó que los hackers rusos, en su mayoría civiles,

[3] Ibrahim, AM and Azubuike, AS, **Review of the security challenges in northern Nigeria and its implications for business survival and sustainable development**:,Journal of management and corporate governance, Vol 6, No 2, 2004,p.6.
[4] Sheldon, John B. **The cyber warfare: The invisible threat,** an article published in Britannica book of the year. Nov 2010.

realizaron ataques DDoS contra sitios web gubernamentales, financieros, informativos y comerciales clave. En 2010, los sitios web del gobierno australiano fueron atacados por DDoS llevados a cabo por ciberactivistas que protestaban por los filtros nacionales de internet.[5]

Los ciberataques semánticos manipulan las percepciones e interpretaciones de los usuarios humanos de los datos generados por computadora con el fin de obtener información valiosa (como contraseñas, detalles financieros e información gubernamental clasificada) de los usuarios a través de medios fraudulentos. Las técnicas de ingeniería social incluyen phishing (los atacantes envían correos electrónicos aparentemente inofensivos a usuarios específicos, invitándolos a divulgar información protegida con fines aparentemente legítimos) y baiting (el software infectado con malware se deja en un lugar público con la esperanza de que un usuario objetivo lo encuentre y lo instale, comprometiendo así todo el sistema informático). Los métodos semánticos se utilizan principalmente para realizar espionaje y actividades delictivas.[6]

En 2010, se realizó un ciberataque contra la instalación nuclear iraní en Natanz.[7] Se alegó que este ataque era un ataque colaborativo de Israel y Estados Unidos con la intención de frenar el progreso de Irán hacia la capacidad de armas nucleares.[8] El ciberataque se lanzó a través de un malware llamado Stuxnet, que se propagó a través de dispositivos de almacenamiento portátiles para llegar a las instalaciones nucleares de Irán.[9] Irán reconoció públicamente que el malware Stuxnet destruyó aproximadamente 984 de sus 6.000 centrífugas enriquecedoras de uranio.[10] Esto representó una disminución del 30% en la eficiencia del enriquecimiento y retrasó la producción de enriquecimiento nuclear de Irán en 2 años, lo que tuvo un impacto negativo en la seguridad nacional en el país.[11] La Agencia Internacional de Energía Atómica verificó esta cuenta de que 1.000 centrifugadoras iraníes fueron desmanteladas y reemplazadas a principios de 2010.

En respuesta, Irán desarrolló la capacidad de lanzar ciberataques preventivos invirtiendo más de

[5] Sheldon, John B. **The cyber warfare: The invisible threat,** an article published in Britannica book of the year. Nov 2010.
[6] Sheldon, John B. **The cyber warfare: The invisible threat,** an article published in Britannica book of the year. Nov 2010.
[7] Zetter, K. **Countdown to zero day: Stuxnet and the launch of the world's first digital weapon**, Boston: Crown/Archetype, 2014, pp.8-14.
[8] Reardon, RJ. **Containing Iran: Strategies for addressing the Iranian nuclear challenge**, Santa Monica: R and D Corporation, 2012, p.13.
[9] Green, JA . **Cyber warfare: A multidisciplinary analysis**, New York: Routledge, 2015, pp.18-21.
[10] Green, JA . **Cyber warfare: A multidisciplinary analysis**, New York: Routledge, 2015, pp.18-21.
[11] M Holloway, M "**Stuxnet worm attack on Iranian nuclear facilities. Stanford University**: 16 Jul 15, <http://large.stanford.edu/courses/2015/ph241/ holloway1/> accessed 2 Oct 19.

un billón de dólares estadounidenses (US$) en infraestructura ciberespacial, manteniendo un presupuesto anual promedio de US$ 76 millones para su programa de ciberespacio entre 2011 y 2012.[12] Además, la Guardia Revolucionaria Islámica, una rama de las Fuerzas Armadas de Irán, reclutó a más de 120.000 personas durante 3 años, a fin de desarrollar sus capacidades para enfrentar las amenazas del ciberespacio, convirtiéndola en la quinta nación más grande en cuanto a su presencia en el ciberespacio detrás de Estados Unidos, Rusia, China e Israel.[13] Como resultado de la capacidad adquirida, Irán pudo contener los ataques en el ciberdominio y proyectar la superioridad para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional. Las inversiones en las ciberoperaciones de Irán aumentaron sus capacidades para enfrentar las amenazas del ciberespacio, mejorando así su seguridad nacional.

Las capacidades para enfrentar las amenazas del ciberespacio también son fundamentales para mejorar la seguridad nacional de los países de África, ya que el continente conecta cada vez más sus infraestructuras críticas con el ciberespacio. Específicamente, Túnez se encuentra entre los 10 países más ciberatacados en África.[14] En 2011, después de las protestas de miles de tunecinos que pedían un cambio económico y social en su país, el gobierno tunecino llevó a cabo la censura on line y off line de sus ciudadanos mediante operaciones dirigidas de phishing para erradicar las críticas que se encontraban online contra el gobierno.[15] En respuesta, un grupo activista global no estatal llamado Anonymous, lanzó ataques DDoS simultáneos contra el gobierno tunecino. Estos ciberataques se dirigieron a los sitios web de las agencias gubernamentales tunecinas y al menos 8 sitios web fueron dañados, incluidos los del Presidente y los ministerios clave del Gobierno.[16] Cada uno de los objetivos recibió ataques DDoS de 8 horas con anchos de banda de hasta 840 gigabytes por segundo que desactivaron las operaciones en las organizaciones durante el período, lo que impidió la protección a la seguridad nacional en el país.

---

[12] Brunner, J. **Iran has built an army of cyber-proxies**, **The tower**, 29 Aug 15, <http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/> accessed 2 Oct 19.

[13] Reardon, RJ. **Containing Iran: Strategies for addressing the Iranian nuclear challenge**, Santa Monica: R and D Corporation, 2012, p.13.

[14] Hadjizenonos, D. **Africa in the cyber war**", **Hi tech security solutions**, 3 Feb 16, < http://www.securitysa.com/53798n> accessed 2 Oct 19.

[15] Howard PN and Hussain MM, Democracy's fourth wave?: Digital media and the Arab spring, New York: Oxford Press, 2013, pp.13-20.

[16] Singer PW and Friedman, A Cybersecurity: What everyone needs to know, New York: Oxford university press, 2014, p.22.

En el momento de estos ataques, las capacidades de las Fuerzas Armadas de Túnez (TAF, por sus siglas en inglés) para enfrentar las amenazas del ciberespacio eran limitadas. Como resultado, el Gobierno se asoció con la OTAN para desarrollar sus capacidades para enfrentar las amenazas del ciberespacio, junto con otras.[17] Esta asociación implicó una donación de la OTAN de US$3,7 millones de dólares a las TAF para establecer un Centro de Fusión de Inteligencia en Túnez a fin de abordar cuestiones de ciberseguridad y lucha contra el terrorismo.[18] Este acuerdo resultó en la capacitación de más de 100 miembros de las TAF en operaciones de ciberguerra a fin de mejorar la seguridad nacional del país. La asociación entre las TAF y la OTAN mejoró así las capacidades para enfrentar las amenazas del ciberespacio también de Túnez.

Nigeria tiene más de 123 millones de usuarios de Internet, lo que representa el 23,5 por ciento de todos los usuarios de Internet en África.[19] Este amplio acceso al ciberespacio no está exento de los riesgos asociados de los ciberataques. En 2017, Nigeria experimentó un total de 3.500 ciberataques, lo que provocó pérdidas por un total de aproximadamente U$S500 millones de dólares.[20] No obstante, la utilización del ciberespacio en Nigeria está en aumento. En 2017, el gobierno nigeriano lanzó una iniciativa llamada Internet de las Cosas (IoT, por sus siglas en inglés) para enriquecer aún más el uso del ciberespacio y, eventualmente, crear ciudades inteligentes en el país.[21] Con el afianzamiento de la iniciativa IoT en Nigeria, los dispositivos domésticos, los automóviles, las empresas y la infraestructura nacional crítica están vinculados a miles de millones de otros dispositivos conectados a Internet.[22] Esto permite una interacción ilimitada entre personas, empresas, máquinas e infraestructura, así como mejoras en la experiencia y eficacia de los usuarios. Esta emocionante innovación ha generado más oportunidades y colaboraciones en el ciberespacio y también abre nuevas fronteras para la

[17] Varga, G. Building partnerships in challenging times: The defence arrangements of Tunisia. European Institute of the Mediterranean, < https://www.euromesco.net/publication/building-partnerships-in-challenging-times-the-defence-arrangements-of-tunisia/ accessed 2 Oct 19.

[18] Adesewo, R.Attaché, Embassy of Nigeria in Tunisia, lecture on **Cyber warfare and national security: Armed Forces of Nigeria in perspective**" delivered at NDC Abuja on 12 Jan 18**.**

19 Internet users statistics for Africa" Internet world statistics as at 30 Jun 19.

http://www.internetworldstats.com/stats.htm accessed 3 Oct 19.

[20] Shittu, A. Former minister of communication, lecture on "**Cyber warfare and national security: Armed Forces of Nigeria in perspectives,** delivered at NDC Abuja on 12 Jan 18.

[21] Shittu, A. Former minister of communication, lecture on "**Cyber warfare and national security: Armed Forces of Nigeria in perspectives,** delivered at NDC Abuja on 12 Jan 18.

[22] Shittu, A. Former minister of communication, lecture on "**Cyber warfare and national security: Armed Forces of Nigeria in perspectives,** delivered at NDC Abuja on 12 Jan 18.

ciberseguridad como infraestructura crítica, en tiempos de paz y guerra.

Actualmente, las 15 infraestructuras nacionales críticas identificadas por la Política y Estrategia Nacional de Ciberseguridad 2014, entre las que se encuentran los sectores de energía, transporte, defensa y finanzas, son vulnerables a los ciberataques debido a los avances tecnológicos y la creciente conectividad de Nigeria al ciberespacio.

Este hecho, y el uso extendido de redes y sistemas para actividades militares, muestran que el uso continuo del ciberespacio en Nigeria requiere un desarrollo correspondiente de las capacidades para enfrentar las amenazas del ciberespacio por parte de la pertinente agencia gubernamental, que son las Fuerzas Armadas de Nigeria (AFN, por sus siglas en inglés).

Como se consagra en la Sección 217 (2) de la Constitución de la República Federal de Nigeria, 1999, las AFN son responsables de abordar las actividades que amenazan la integridad territorial o la soberanía del país. Esta responsabilidad podría lograrse a través de cualquier medio, incluyendo el ciberespacio, el cual involucra operaciones para proteger la infraestructura nacional crítica de Nigeria y proyectar poder militar en el ciberespacio, a través de operaciones defensivas y ofensivas.

Sin embargo, en realidad las AFN solo han dado algunos pasos a fin de desarrollar sus capacidades para enfrentar las amenazas del ciberespacio. Estos incluyen programas de concientización sobre ciberseguridad por parte del Cuartel General de Defensa (DHQ, por sus siglas en inglés) en 2012 y el establecimiento de una subdirección de ciberseguridad en el DHQ en 2014. Otros son la creación de un Departamento de Ciberseguridad y un Centro de Ciberoperaciones de Defensa en la Administración Espacial de Defensa (DSA, por sus siglas en inglés) en 2016 y el establecimiento del Comando de Ciberguerra en el Cuartel General del Ejército en 2018, donde los oficiales y soldados con el conocimiento necesario se entrenan y se despliegan para monitorear y responder a las amenazas del ciberespacio que enfrenta el ejército. A pesar de estos esfuerzos, Nigeria todavía parece vulnerable a los ciberataques y está clasificada entre los objetivos de alta prioridad en África debido a su población, capacidades militares y crecimiento económico. Con las crecientes amenazas del Grupo Terrorista Boko Haram (BHT, por sus siglas en inglés) y su reciente afiliación a los Estados Islámicos de la Provincia de África Occidental (ISWAP, por sus siglas en inglés), el grupo posee la capacidad de llevar a cabo

propaganda, reclutamiento y ciberespionaje sobre el ejército, por lo tanto, las AFN necesitan desarrollar las capacidades y equipamiento adecuados para enfrentar las amenazas del ciberespacio a fin de detectar, detener y defender al país contra tales ataques o para lanzar ciberataques preventivos contra cualquier nación o actor no estatal a fin de mejorar la seguridad nacional de Nigeria.

Por lo tanto, el propósito de esta investigación es identificar, analizar y evaluar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de detectar, detener y defender ciberataques contra el país. El período del estudio abarca el período 2009-2018.

Esta investigación fue motivada por el deseo de explorar e identificar formas de impulsar las capacidades de las AFN para enfrentar las amenazas del ciberespacio y también ofrecer estrategias para incrementar dichas capacidades a fin de mejorar la seguridad nacional en Nigeria.

Este estudio, por lo tanto, busca evaluar las capacidades de las AFN para enfrentar las amenazas del ciberespacio y su implicancia en la seguridad nacional de Nigeria. Además busca dar respuestas a las siguientes preguntas de investigación:

Interrogante principal

a) ¿Cuál es la relación entre ciberguerra y seguridad nacional en Nigeria?

b) ¿De qué manera se relacionan la ciberguerra, la seguridad nacional y las AFN?

c) ¿Cuáles son las capacidades que tienen las AFN para enfrentar las amenazas del ciberespacio a fin de fortalecer la seguridad nacional en Nigeria?

d) ¿Cuáles son los desafíos que poseen en la actualidad las AFN para enfrentar las amenazas del ciberespacio en Nigeria?

HIPÓTESIS DEL ESTUDIO

La hipótesis del estudio es:

H – El incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio conducirá a una mejora de la seguridad nacional de Nigeria.

OBJETIVOS DEL ESTUDIO

El objetivo principal del estudio es evaluar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de detectar, detener y defender los ciberataques llevados a cabo contra el país. Sin embargo, los objetivos específicos son:

a. Establecer la relación entre ciberguerra y seguridad nacional.

b. Identificar los problemas asociados con las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria.

c. Describir los alcances[23] que tienen las capacidades de las AFN para enfrentar las amenazas del ciberespacio para la seguridad nacional en Nigeria.

d. Identificar las vulnerabilidades y desafíos que afrontan las capacidades de las AFN para enfrentar las amenazas del ciberespacio para la seguridad nacional en Nigeria.

IMPORTANCIA DEL ESTUDIO

El estudio es significativo ya que el resultado ayudará a mejorar las políticas y el rendimiento, a su vez de contribuir a lograr una mayor investigación y aumentar el conocimiento existente sobre la ciberguerra en Nigeria.

a. **Mejora de políticas.** El estudio beneficiará a los responsables de formular políticas a nivel estratégico y operativo al promulgar políticas relacionadas con el enfrentamiento de las amenazas del ciberespacio para la mejora de la seguridad nacional. La Oficina del Asesor de Seguridad Nacional (ONSA, por sus siglas en inglés), el Ministerio de Defensa (MOD, por sus siglas en inglés), el Ministerio de Información y Comunicaciones y el DHQ considerarán que el estudio es útil para la formulación y mejora de políticas.

b. **Mejora del rendimiento.** El estudio beneficiará a organizaciones como el DHQ, la Agencia de Inteligencia de Defensa (DIA, por sus siglas en inglés), DSA, Departamento de Servicios del Estado (DSS, por sus siglas en inglés), NA(Ejército de Nigeria, por sus siglas en inglés), NN (Armada de Nigeria, por sus siglas en inglés) y NAF (Fuerza Aérea de Nigeria, por sus siglas en inglés) que se ven directamente afectadas por el rol llevado a

[23] NdT: Con fines idiomáticos, la traducción del término "implications" empleado en el idioma original de la tesis, fue reemplazado por "alcances".

cabo por las AFN de enfrentamiento de las amenazas del ciberespacio. Específicamente, estas organizaciones se beneficiarán de cualquier recomendación hecha como resultado de este estudio. Además, algunas agencias de gobierno que complementan los esfuerzos de las AFN, el rol llevado a cabo por ellas de enfrentamiento de las amenazas del ciberespacio, encontrarán útil el estudio para identificar las formas y los medios para brindar apoyo. Estas agencias incluyen la Agencia Nacional de Inteligencia (NIA, por sus siglas en inglés), la Comisión de Comunicaciones de Nigeria (NCC, por sus siglas en inglés), la Agencia de Investigación y Desarrollo Espacial de Nigeria, la Galaxy Backbone Limited y la Agencia Nacional de Desarrollo de Tecnología de la Información (NITDA, por sus siglas en inglés) entre otras.

c. **Mayor investigación.** El estudio beneficiaría a estudiantes e investigadores deseosos de mejorar en este campo. El resultado del estudio podría servir como material de referencia para futuros estudios en la materia.

d. **Cuerpo de conocimientos.** El estudio también beneficiaría al público en general, ya que aumentará el conocimiento existente sobre ciberseguridad, ciberguerra y el rol llevado a cabo por las AFN, y otros asociados, de enfrentamiento de las amenazas del ciberespacio. El público en general también podría encontrarlo útil para extender las fronteras del conocimiento.

ALCANCE DEL ESTUDIO

El alcance del estudio se definiría en términos de tiempo, espacio y límites a su contenido.

a. **Tiempo.** El estudio abarca el período comprendido entre 2009 y 2018. Este período se eligió porque es la era del aumento de las actividades en el ciberespacio en Nigeria que condujo a mayores problemas de ciberseguridad. Además, la Política y Estrategia Nacional de Ciberseguridad, así como la Ley Nacional de Ciberdelitos se promulgaron durante este período a fin de mejorar la seguridad nacional. Además, las AFN establecieron instituciones como el Centro de Ciberoperaciones de Defensa en la DSA, así como subdirecciones de ciberseguridad en el DHQ y los 3 servicios dentro del período.

b. **Espacio.** En términos de espacio, el estudio se centra en las actividades llevadas a cabo

por las AFN de enfrentamiento de las amenazas del ciberespacio en las 6 zonas geopolíticas del país. Esto comprende las operaciones militares realizadas en Nigeria y las ofrecidas para proteger la infraestructura nacional crítica necesaria para mejorar la seguridad nacional.

c. **Contenido.** El contenido del estudio destaca las operaciones las AFN de enfrentamiento de las amenazas del ciberespacio. En esencia, el estudio examina las capacidades de las AFN para enfrentar las amenazas del ciberespacio, que fueron los elementos principales necesarios para salvaguardar la nación y, por extensión, mejorar su seguridad nacional.

METODOLOGÍA DEL ESTUDIO

La metodología adoptada en este estudio cubre 6 aspectos clave que fueron el tipo de investigación, las fuentes de datos y los métodos de recolección de datos. Otros son el muestreo, el método de análisis de datos y el método de presentación de datos. Dichos aspectos se detallan a continuación:

Tipo de investigación. El tipo de investigación adoptado en este estudio es categorizado por la naturaleza de la investigación, el nivel de investigación y el diseño de la investigación.

a. **Naturaleza de la investigación.** El estudio es una investigación aplicada que empleó datos empíricos. Ambos, datos cualitativos y cuantitativos fueron recopilados y analizados en relación con las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria.

b. **Nivel de investigación.** El estudio adopta un enfoque de investigación descriptivo. Este se usó para analizar datos sin manipular el medio ambiente a fin de explicar mejor cómo el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio conduce a una mejora de la seguridad nacional de Nigeria.

c. **Diseño de la investigación.** El estudio adopta un diseño de investigación mediante encuestas utilizando un enfoque transversal. Este diseño permitió a los encuestados ser estudiados en su entorno natural en un momento particular.

Fuentes de datos. Los datos para la investigación se obtuvieron de fuentes primarias y

secundarias.

a. **Fuentes primarias.** Los datos primarios para el estudio se obtuvieron del personal de nivel estratégico y operativo en las AFN responsable de las áreas directamente relacionadas con el enfrentamiento de las amenazas del ciberespacio y la seguridad nacional en Nigeria. Algunas otras fuentes incluyen representantes responsables de la ciberseguridad en Nigeria, particularmente aquellos que desarrollan sus tareas en agencias como ONSA, NITDA, organizaciones privadas relevantes y expertos en ciberseguridad seleccionados. Los datos primarios se obtuvieron igualmente de una muestra de personal de las AFN que está cargo directamente de llevar a cabo ciberoperaciones a fin de mejorar la seguridad nacional en Nigeria. Una lista completa de las personas entrevistadas se encuentra en el Apéndice 1.

b. **Fuentes secundarias.** Se obtuvieron datos secundarios de libros, publicaciones periódicas, disertaciones, seminarios y documentos de conferencias, revistas, periódicos y otros materiales relevantes publicados y sin publicar. Los materiales relevantes se obtuvieron de internet, así como las bibliotecas de ONSA, DHQ, DSA, el Colegio de Defensa Nacional (NDC, por sus siglas en inglés), la Academia de Defensa de Nigeria (NDA, por sus siglas en inglés), NA, NN y NAF.

Los métodos de recopilación de datos. Los métodos de recolección de datos adoptados en este estudio son el método de campo y el análisis documental.

a. **Método de campo.** Se usó una combinación de 2 métodos de campo en este estudio. Estos fueron los métodos de entrevista y cuestionario. En el método de entrevista, el investigador utilizó una combinación de entrevista telefónica y entrevistas orales no estructuradas. Por otro lado, se utilizaron cuestionarios para obtener las opiniones de los encuestados sobre diferentes aspectos de la relación entre ciberguerra y seguridad nacional. El cuestionario se administró al personal de los 3 Servicios que son de la especialización relacionada con las TIC. Una copia del cuestionario se encuentra en el Apéndice 2.

b. **Análisis de documentos.** Los datos secundarios en forma de documentos electrónicos e impresos se analizaron mediante la búsqueda en la biblioteca de archivos. Esto aseguró

que se obtuviera suficiente literatura sobre ciberguerra y seguridad nacional con el fin de reforzar o refutar los datos primarios.

Muestreo. Las técnicas de muestreo utilizadas en este estudio se consideran: la población del estudio, la descripción de la muestra del estudio y la técnica de muestreo aplicada.

a. **Población del estudio.** La población de este estudio está compuesta por personal de las AFN especializados en las TIC de las tres fuerzas. Se trata de un total de 1.930 personas basadas en los datos obtenidos de los directores pertinentes de TIC en la sede del NA, la NN y la NAF. Algunos especialistas en TIC seleccionados de las AFN, agencias gubernamentales y el sector privado también fueron entrevistados.

b. **Muestra del estudio.** El tamaño de la muestra para el estudio se calculó utilizando la fórmula de tamaño de muestra Taro Yamane. La estimación del tamaño de la muestra se realizó con un margen de error del 5% y un nivel de confianza del 95%. Los detalles del cálculo del tamaño de la muestra se encuentran en el Apéndice 3. El resultado del cálculo indicó un tamaño de muestra de aproximadamente 331. En consecuencia, los cuestionarios se administraron a un tamaño de muestra de 350 participantes a fin de tener en cuenta las respuestas no válidas o los casos de no respuesta.

c. **Técnica de muestreo.** El estudio adopta 2 métodos de muestreo, uno para el personal de las AFN administrado con cuestionarios y el otro para expertos en TIC seleccionados de las AFN, agencias gubernamentales y el sector privado. La técnica de muestreo probabilístico se utilizó para seleccionar las personas entrevistadas mediante cuestionarios. La técnica específica utilizada fue la técnica de muestreo estratificado. Las tres fuerzas formaron los estratos, mientras que se realizó un muestreo aleatorio en cada estrato. Esto ayudaría a mejorar la representación adecuada, evitar sesgos de muestreo y maximizar la validez externa. Sin embargo, un problema con este método es que los distintos subconjuntos podrían ser desiguales en tamaño. El estudio adoptó la técnica de muestreo intencional no probabilístico para seleccionar a los expertos en TIC de las AFN, agencias gubernamentales y el sector privado para entrevistas no estructuradas. Esta técnica aseguró que se hicieran deducciones válidas y se obtuvieran respuestas adecuadas para las preguntas de investigación.

Método de análisis de datos. Los datos recopilados se analizan cuantitativa y cualitativamente. Se utilizaron medidas de tendencia central, como la distribución de frecuencias, para analizar los datos descriptivos. El razonamiento lógico se utilizó para analizar los datos cualitativos obtenidos a través de entrevistas.

Método de presentación de datos. Los datos generados en el estudio se presentan mediante tablas, cuadros y gráficos. Estos formatos mejoran la ilustración de las relaciones entre las variables en el estudio.

LIMITACIONES DEL ESTUDIO

El enfrentamiento de las amenazas del ciberespacio tiene que ver con la seguridad y la inteligencia, por lo que algunas agencias gubernamentales se mostraron reacias a proporcionar información sobre el tema, mientras que otras se negaron. Además, hubo una escasez de datos secundarios sobre el tema, ya que la ciberguerra es un tema en evolución en Nigeria y muchas de las agencias reguladoras no generan datos relevantes. Sin embargo, estas limitaciones se abordaron extrapolando los datos disponibles y realizando más entrevistas, debates y consultas para enriquecer aún más los datos primarios.

Debido a la naturaleza dispersa de la población para el estudio, administrar un cuestionario a la muestra seleccionada también resultó desafiante en algunos casos, pero esto se superó con la persistencia y los esfuerzos dedicados del asistente de investigación que aseguran que obtuvo los cuestionarios completos.

CAPITULO 2:
REVISIÓN DE LITERATURA

Este capítulo comienza con un discurso conceptual de las 2 variables en el estudio, ciberguerra y seguridad nacional. Luego presenta una revisión de la literatura existente en el campo de estudio para identificar los vacíos que el estudio pretende llenar. Luego, proporciona el marco teórico utilizado para situar adecuadamente el estudio. También considera el enfrentamiento de las amenazas del ciberespacio por parte de Estonia y Estados Unidos, con el fin de extraer lecciones para el estudio. Finalmente, el capítulo describe una visión general sobre la relación entre ciberguerra y seguridad nacional en Nigeria y presenta los temas clave involucrados.

DISCURSO CONCEPTUAL

Las 2 variables en este estudio son la ciberguerra, que es la variable independiente y la seguridad nacional, la variable dependiente. Estas variables se conceptualizan y se establece su relación a fin de comprender el contexto en el que se utilizan en este estudio.

Ciberguerra

Los académicos y los profesionales no han establecido puntos en común precisos en el campo de la ciberguerra. En este sentido, se consideraron las opiniones de Alexander, Billo y Chang, así como de Green. Alexander ve la ciberguerra como el acto de explotar el ciberespacio para atacar instalaciones, equipos o personal, con la intención de degradar, neutralizar o destruir la capacidad de combate de un enemigo, al tiempo que protege sus propias capacidades.[24] Esta visión identifica claramente la ciberguerra como un acto de guerra que involucra acciones ofensivas y defensivas llevadas a cabo a través del ciberespacio. Sin embargo, no identifica a los actores que llevan a cabo las acciones. Tampoco considera los medios por los cuales los ataques se librarían a través del ciberespacio. Por estas razones, no es lo suficientemente completo, por lo tanto, no se adopta para este estudio.

Billo y Chang ven la ciberguerra como actos de unidades organizadas como estados-nación, en operaciones defensivas y ofensivas, explotando computadoras para atacar redes informáticas a través del medio electrónico.[25] Esta visión destaca las computadoras y la electrónica como los

[24] Alexander, K. ***Warfighting in cyberspace, Joint force quarterly***, Vol.3, No.46, (2007).

[25] Billo, CG and Chang, W. Cyber warfare an analysis of the means and motivations of selected nation state, ***Institute for security technology studies***, < http://www.ists. dartmouth.edu/docs/cyberwarfare.pdf> accessed 15 Oct 19.

medios para librar acciones de ciberguerra. También identifica a los estados nacionales como los principales actores involucrados en la realización de las acciones. Sin embargo, no contempla detalles sobre los fines de la ciberguerra y no tiene en cuenta el hecho de que la ciberguerra podría ser iniciada y dirigida por actores no estatales. Esto ocurre cada vez más dada la baja barrera de entrada para la ciberguerra en términos de equipos y armas, en comparación con las operaciones en otros dominios de guerra. El punto de vista no es lo suficientemente completo y, por lo tanto, no se adopta para este estudio.

Green ve la ciberguerra como una extensión de la política a través de la explotación del ciberespacio por parte de actores estatales, o por actores no estatales con un importante apoyo estatal, utilizando infraestructura de TIC y ciberarmas.[26] Además, postula que implica el uso de malware, botnets o gusanos contra redes militares o civiles, a través de ciberoperaciones ofensivas o ciberacciones defensivas, tomadas en respuesta a amenazas graves a la seguridad del propio estado. La posición de Green aclara claramente las formas, los medios y los fines de la ciberguerra. También menciona a los actores involucrados y las armas utilizadas, mientras hace hincapié en que la ciberguerra se centra principalmente en amenazas graves, como aquellas contra la infraestructura nacional crítica o los sistemas militares. La visión de Green captura los atributos esenciales necesarios para el estudio y, por lo tanto, se adopta.

Seguridad Nacional

La conceptualización de la seguridad nacional ha evolucionado a lo largo de los años a medida que evoluciona la naturaleza de lo que constituye la seguridad de una nación. En consecuencia, se consideraron las opiniones de Dyke, Romm y el Consejo de Seguridad Nacional de la República de Filipinas. Dyke ve a la seguridad nacional como la protección de la soberanía del estado-nación, la santidad de sus territorios, con un enfoque específico en la protección contra ataques militares y los derechos colectivos e individuales de defensa personal contra amenazas externas e internas.[27] Esta definición aborda el ingrediente fundamental de la seguridad nacional, que es la protección de un país contra ataques externos e internos. Sin embargo, la seguridad nacional ya no se trata solo de las fuerzas de combate y el armamento. La visión de Dyke no cubre elementos de seguridad humana que son esenciales para abordar las variables en este

[26] Green*, JA. Cyber warfare: A multidisciplinary analysis*, New York: Routledge, 2015, pp.15-22.

[27] Dyke*, VV.* ***Security and sovereignty in international politics***, New York: Appleton-Century-Crofts, 1966, pp.6-9.

estudio. En vista de esto, no se adopta para este estudio.

Romm ve la seguridad nacional como la ausencia de amenaza militar contra un país y la protección de una nación contra ataques externos o derrocamientos, así como los elementos de seguridad humana como la seguridad económica, la seguridad energética, la seguridad laboral y la seguridad ambiental.[28] Además, afirma que no puede haber verdadera paz o seguridad a menos que exista en todos los aspectos de la vida cotidiana de los ciudadanos.[29] Esta definición considera la seguridad nacional más allá de los aspectos militares convencionales. Destaca los aspectos no militares que también se centran en la protección de ciertos aspectos de la vida de un ciudadano. Sin embargo, la opinión de Romm no menciona ciertos factores internos en un país, como la preservación del acceso al ciberespacio y la protección de la infraestructura crítica de un país, que son elementos necesarios para este estudio. En consecuencia, este punto de vista no es lo suficientemente inclusivo y, como tal, no se adoptó para el estudio.

El Consejo de Seguridad Nacional de la República de Filipinas se refiere a la seguridad nacional como una condición en la cual el bienestar y la calidad de vida de las personas, como la salud, la alimentación, el agua; sus formas de vida, como la libre circulación, el acceso a la energía, el ciberespacio, el comercio real y electrónico; el gobierno y sus instituciones tales como la infraestructura nacional crítica; la integridad territorial y la soberanía incluyendo espacio aéreo y seguridad marítima, lucha contra el terrorismo y otras operaciones militares, son mejoradas y protegidas.[30] Estos aspectos de la seguridad se centran en eventos que generalmente requieren una respuesta nacional, ya que se extienden más allá de la capacidad de las personas. Además de la protección del bienestar socioeconómico de los ciudadanos, esta visión de la seguridad nacional incorpora la preservación de la forma de vida de los ciudadanos. También aborda la protección de la infraestructura crítica, los activos militares y las operaciones, que son clave para este estudio. En vista de esto, la definición se considera adecuada y es adoptada para el estudio. El discurso conceptual considerado subraya la necesidad de examinar el nexo entre la ciberguerra y la seguridad nacional.

[28] Romm, JJ. ***Defining national security: The non-military aspects***, New York: Council on foreign relations press, 1993, p.29.

[29] Romm, JJ. ***Defining national security: The non-military aspects***, New York: Council on foreign relations press, 1993, p.38.

[30] National security policy for change and well-being of the Filipino people (2017-2022), ***National security council of the Republic of Philippines***, < http:// www.nsc.gov.ph/attachments/article/NSP/NSP-2017-2022.pdf> accessed 15 Oct 19.

RELACIÓN ENTRE CIBERGUERRA Y SEGURIDAD NACIONAL

La ciberguerra implica la explotación del ciberespacio, la infraestructura de las TIC, las ciberarmas, las ciberacciones ofensivas y defensivas. La seguridad nacional implica la protección de la infraestructura nacional crítica, las operaciones militares, la lucha contra el terrorismo, el comercio electrónico mejorado, así como la necesidad de garantizar el bienestar de los ciudadanos. La explotación efectiva del ciberespacio mediante el uso de la infraestructura de las TIC y las ciberarmas a fin de llevar a cabo ciberacciones ofensivas y defensivas, conduciría a la protección de la infraestructura nacional crítica, a la mejora de las operaciones militares y antiterroristas, al incremento del comercio electrónico y al bienestar de los ciudadanos.

Por el contrario, cuando una nación falla al explotar el ciberespacio utilizando infraestructura de TIC y ciberarmas a fin de llevar a cabo ciberacciones tanto ofensivas como defensivas, su capacidad para efectuar operaciones antiterroristas o proteger su infraestructura nacional crítica, operaciones militares, comercio electrónico y el bienestar de su gente se verá disminuida. En consecuencia, el incremento de las capacidades para enfrentar las amenazas del ciberespacio conduce a una mejora de la seguridad nacional, mientras que una disminución en las capacidades para enfrentar las amenazas del ciberespacio podría menoscabar la seguridad nacional. Existe, por lo tanto, una relación directa entre ciberguerra y seguridad nacional. Habiendo examinado la relación entre ciberguerra y seguridad nacional, es necesario revisar la literatura existente sobre las 2 variables para identificar los vacíos que se abordarán en este estudio.

REVISIÓN DE LA LITERATURA EXISTENTE

En los últimos años, se han realizado varios estudios sobre ciberguerra y seguridad nacional. La mayoría de los estudios difieren en contexto y enfoque, así como en las teorías subyacentes. En este sentido, los estudios de Schmitt et al., Valerriano y Maness, Eun y Abmann, Osho y Onoja, así como Alechenu son revisados en esta sección. Schmitt et al., en su libro de asesoramiento no empírico sobre ciberguerra, titulado "El Manual de Tallin, Primera edición", articula un conjunto de reglas al proponer cómo se aplica el derecho internacional existente al uso de la fuerza en el ámbito del ciberespacio. Utilizando una metodología exploratoria basada en situaciones hipotéticas, el estudio especifica qué cuenta como uso de la fuerza o ataque armado en el ciberespacio, como los ataques de denegación de servicio, y cómo se clasifican quienes llevan a

cabo estos ataques armados.[31] Además, refleja la perspectiva occidental que postula que el derecho internacional humanitario solo se aplicaría a la ciberguerra, si los ciberataques asociados equivalen a un conflicto armado. En la práctica, algunos ciberataques, como los ataques a hospitales o redes de transporte, no necesariamente implican un conflicto armado, sin embargo, invariablemente pueden conducir a la pérdida de vidas. La perspectiva de Schmitt et al., sirve como un buen recurso para académicos y formuladores de políticas. Sin embargo, el manual carece de diversidad de puntos de vista, ya que se basa en la perspectiva occidental de la ciberguerra que puede dificultar su aceptación en países como Rusia y China. Por lo tanto, este trabajo no refleja una visión globalmente aceptada de ciberguerra y seguridad nacional, que es el enfoque de este estudio.

Valerriano y Maness, en su libro titulado "Ciberguerra vs. Ciberrealidades: el ciberconflicto en el sistema internacional", cuestionaron el argumento convencional presentado por los expertos sobre la gravedad de las ciberamenazas. Utilizando evidencia empírica de ciberconflictos llevados a cabo en la década anterior, argumentaron que las ciberamenazas fueron exageradas por el complejo ciberindustrial que está llevando la adquisición de armas en la dirección equivocada.[32] La evidencia empírica mostró que dentro del período revisado, solo 20 de los 126 estados nacionales rivales se habían involucrado en ciberconflictos y tales compromisos tenían una frecuencia y magnitud limitadas. El libro utiliza métodos mixtos para explicar las interacciones entre los estados en el ciberdominio. Esto es bastante distintivo porque la mayoría de los estudios similares se han basado principalmente en datos cualitativos en gran parte debido a la escasez de datos en este dominio bastante nuevo. Los autores postularon que los Estados que actúan sin competencia continua, actúan de manera diferente a los rivales.[33] Sin embargo, no proporcionaron ninguna base para esta afirmación, por lo que no está claro si implica que los Estados que no participan en la competencia tienen menos probabilidades de estar involucrados en un ciberconflicto. Los autores propusieron una teoría que establece que la decisión de un Estado de lanzar una ciberoperación está socialmente construida por normas, rivalidad y miedo a

[31] Schmitt MN et al, ***Tallinn manual on the international law applicable to cyber warfare***, New York: Cambridge university press, 2013, pp.50-57.
[32] Valeriano, B and Maness, RC. ***Cyber war versus Cyber realities: Cyber conflict in the international system***, New York: Oxford university press, 2015, p.5.
[33] Valeriano, B and Maness, RC. ***Cyber war versus Cyber realities: Cyber conflict in the international system***, New York: Oxford university press, 2015, p.6.

la respuesta.[34] Esto puede influir en los responsables políticos para reevaluar sus acciones en el ciberespacio y, por lo tanto, evitar una reacción exagerada al ciberconflicto. Este trabajo, sin embargo, no examinó la relación entre ciberguerra y seguridad nacional, que es uno de los focos de este estudio.

Eun y Abmann, en su estudio descriptivo, titulado "Ciberguerra: Haciendo un Balance de la Seguridad y la Guerra en la Era Digital", presentaron una visión más severa de la ciberguerra. Los autores utilizaron métodos cualitativos para examinar las implicancias de la ciberguerra en la guerra tradicional y la seguridad nacional y descubrieron que la ciberguerra puede ser un multiplicador de fuerza para los ataques cinéticos sin hacer obsoleta la guerra convencional.[35] Identificaron ciertas características distintivas de las ciberarmas que podrían exacerbar la ocurrencia y el impacto de la ciberguerra. Estos incluyen el hecho de que las ciberarmas son más baratas de adquirir y más fáciles de implementar que las armas convencionales, así como la dificultad de atribución ya que las direcciones IP pueden ser manipuladas.[36] Estas características nivelan el campo de juego de la ciberguerra, particularmente a favor de los países que carecen de influencia en el poder militar convencional. El estudio, por lo tanto, postula que la ciberguerra es un componente integral de la guerra que se está interconectando más con la guerra convencional a medida que las sociedades avanzan hacia la era digital.[37] A pesar de la afirmación de los autores de que todas las guerras interestatales futuras tendrían ciberdimensión, el estudio no mencionó que, a diferencia de las armas convencionales, una vez utilizadas, las ciberarmas se vuelven menos efectivas porque podrían haberse desarrollado mecanismos de defensa contra esas armas en particular. Este trabajo no examinó vívidamente el nexo entre ciberguerra y seguridad nacional en el que el presente estudio pretende centrarse.

Osho y Onoja, en su investigación descriptiva titulada "Política y Estrategia Nacional de Ciberseguridad de Nigeria: un Análisis Cualitativo", utilizaron una metodología cualitativa para analizar la implementación de la Política y Estrategia Nacional de Ciberseguridad Nigeriana.[38]

---

[34] Valeriano, B and Maness, RC. ***Cyber war versus Cyber realities: Cyber conflict in the international system,*** New York: Oxford university press, 2015, p.6.

[35] Eun YS and Abmann, JS. *Cyberwar: Taking stock of security and warfare in the digital age,* ***International studies perspectives,*** Vol.17, (2016), pp.2-10.

[36] Eun YS and Abmann, JS. *Cyberwar: Taking stock of security and warfare in the digital age,* ***International studies perspectives,*** Vol.17, (2016), pp.3.

[37] Eun YS and Abmann, JS. *Cyberwar: Taking stock of security and warfare in the digital age,* ***International studies perspectives,*** Vol.17, (2016), pp.4.

[38] Osho O and Onoja, AD. ***National cyber security policy and strategy of Nigeria: A qualitative analysis", International journal of cyber criminology***, Vol.9, No.1, 2015, pp.120–143.

Utilizando los estándares de la Unión Internacional de Telecomunicaciones (UIT) en ciertos aspectos, los autores realizan un análisis comparativo de las políticas y estrategias de ciberseguridad del Reino Unido, Canadá, Francia, Países Bajos, Kenia y Japón. El análisis resultante revela que estos documentos de política y estrategia contienen los parámetros clave de la UIT que normalmente están presentes en los documentos estándar.[39] Sin embargo, los autores encontraron que ciertos aspectos críticos fueron omitidos o apenas mencionados, como los detalles sobre la capacidad de ciberdefensa de los militares. Además, los autores no ampliaron su estudio para tomar en cuenta acciones independientes realizadas en el desarrollo de la cibercapacidad militar.[40] Esto les habría permitido hacer recomendaciones más amplias en este contexto. Además, el trabajo no relacionó la ciberguerra con la seguridad nacional, que es el objetivo del presente estudio.

La investigación de métodos mixtos de Alechenu titulada "Ciberamenazas y Seguridad Nacional: Una Evaluación" utilizó un diseño descriptivo para evaluar la capacidad de Nigeria para frenar las ciberamenazas a fin de mejorar la seguridad nacional.[41] El autor agrega datos cuantitativos y cualitativos de fuentes primarias y secundarias para fortalecer los argumentos en el estudio. En este estudio, se destacan las ciberamenazas prevalecientes que enfrenta Nigeria, así como el papel de la Política y Estrategia de Seguridad Nacional para abordarlas al subrayar sus deficiencias.[42] Sin embargo, dado que toda la población estaba definida y era accesible, una técnica de muestreo aleatorio probabilístico habría sido más apropiada que la técnica de muestreo intencional no probabilístico utilizada en el estudio. Esto habría aumentado la generalización del estudio, de ahí su validez externa. El investigador recomendó que el Gobierno Federal de Nigeria estableciera un cibercomando y patrocinara una resolución en la Asamblea General de la ONU a fin de lograr la promulgación de un tratado sobre ciberseguridad. Esencialmente, el estudio se concentró en gran medida en las ciberamenazas y no se centró en la ciberguerra y la seguridad nacional, que es el esfuerzo principal de este estudio.

---

[39] Osho O and Onoja, AD. ***National cyber security policy and strategy of Nigeria: A qualitative analysis", International journal of cyber criminology***, Vol.9, No.1, 2015, pp.120–143.

[40] Osho O and Onoja, AD. ***National cyber security policy and strategy of Nigeria: A qualitative analysis", International journal of cyber criminology***, Vol.9, No.1, 2015, pp.120–143.

[41] Alechenu, AA "***Cyber threats and national security in Nigeria: An assessment***", a research project submitted to National Defence College Nigeria, June 2017.

[42] Alechenu, AA "***Cyber threats and national security in Nigeria: An assessment***", a research project submitted to National Defence College Nigeria, June 2017.

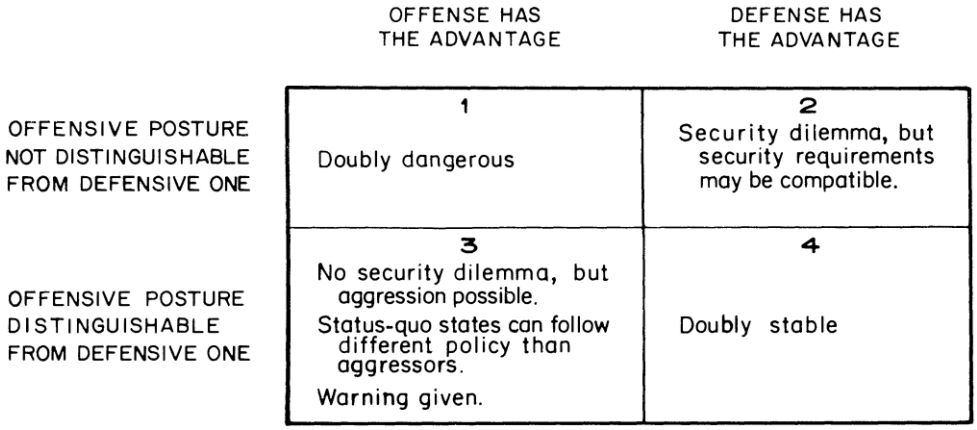
De lo antedicho, todos los estudios revisados hicieron contribuciones al conjunto de conocimientos en el campo de la ciberguerra y sus implicancias para la seguridad nacional. Algunos de los trabajos revisados se concentraron en las complejidades de la ciberguerra y cómo el fenómeno encaja en el esquema general de la guerra, mientras que otros consideraron las capacidades de las ciberarmas como un medio estratégico de guerra. Los estudios en el contexto nigeriano abordaron las deficiencias en la Política y Estrategia Nacional de Ciberseguridad, así como las ciberamenazas que enfrenta el país. Sin embargo, la mayoría de los estudios no se centraron expresamente en cuestiones, efectos, desafíos, perspectivas y estrategias a fin de incrementar las capacidades de las AFN para enfrentar las amenazas del ciberespacio para mejorar la seguridad nacional de Nigeria. Es sobre esta premisa que este estudio busca llenar los vacíos observados en los estudios anteriores al examinar cómo las AFN pueden incrementar sus capacidades para enfrentar las amenazas del ciberespacio necesarias para mejorar la seguridad nacional de Nigeria. Para abordar esto, el marco teórico sobre el que se situó el estudio se presentará en los párrafos posteriores.

MARCO TEÓRICO

Hay varios paradigmas teóricos que podrían ser utilizados con el fin de analizar las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria. Estas teorías incluyen la Teoría de la Ciberdominación, la Teoría de la Disuasión y la Teoría Ofensiva-Defensiva (ODT, por sus siglas en inglés), entre otras. Sin embargo, la teoría más adecuada para el estudio es la ODT según lo postulado por Robert Jervis debido a su naturaleza duradera y su amplia aplicación en diferentes formas de guerra y conflicto. La afirmación central de esta teoría es que la tecnología predominante en un momento dado es un factor crítico responsable del conflicto internacional, ya que los países están tentados a iniciar ataques cuando creen que las nuevas innovaciones y tecnologías favorecen el ataque más que la defensa.[43] Jervis articula este dilema de seguridad en 2 escenarios: si las armas ofensivas tienen ventajas sobre las armas defensivas y si las armas ofensivas se pueden distinguir de las armas defensivas.[44] Estos 2 escenarios se pueden combinar para formar 4 mundos posibles bajo la ODT como se ilustra esquemáticamente en la Figura 1.0

[43] Jervis, R. ***Cooperation under the security dilemma,*** **World politics**, Vol.30, No.2, 1978, p.10.
[44] Jervis, R. ***Cooperation under the security dilemma,*** **World politics**, Vol.30, No.2, 1978, p.11.

Figura 1.0: Diagrama de Resultados de Estabilidad Internacional basado en la Teoría Ofensiva-Defensiva de Jervis



Fuente: R Jervis, "Cooperación bajo el Dilema de Seguridad", **Política mundial**, Vol. 30, No.2, (1978).

En el modelo de "Cuatro mundos" en la Figura 1.0, Jervis postula que los estados pueden generalizar la estabilidad del sistema global en base a las combinaciones de estos 2 escenarios.[45] El Modelo retrata al mundo desde el punto de vista de un poder de status quo.

El primer cuadrante es el peor para los estados de status quo y postula que, dado que las armas ofensivas y defensivas son indistinguibles, los estados tienden a adquirir las armas buscadas por los agresores. Además, dado que la ofensa tiene ventajas sobre la defensa, los estados de status quo elegirán ofensivas sobre posturas defensivas. Esto los hace comportarse como agresores, creando así un mundo inestable y doblemente peligroso plagado de carrera armamentista.

El segundo cuadrante presenta un dilema de seguridad más favorable. Aunque las armas ofensivas y defensivas aún no se pueden distinguir, funciona con menos fuerza que el primer cuadrante, porque, dado que la defensa tiene la ventaja, un aumento en la postura de defensa de un estado aumenta su seguridad más que lo que disminuye la seguridad de otro estado.

En el tercer cuadrante, puede que no haya un dilema de seguridad, solo problemas. Como las armas ofensivas se distinguen de las armas defensivas, los estados pueden obtener armas

[45] Jervis, R. ***Cooperation under the security dilemma,*** **World politics**, Vol.30, No.2, 1978, p.12.

defensivas que no amenacen a otros estados. Sin embargo, dado que la ofensiva tiene la ventaja, es posible que los estados sean agresivos. Con una ventaja más significativa, los estados de status quo pueden incluso atacar de forma preventiva en lugar de arriesgarse a ser atacados. Por el contrario, si el delito tiene menos ventaja, habría más cooperación y estabilidad entre los estados, ya que los estados de status quo estarían invirtiendo más en armas defensivas. El cuarto cuadrante se considera un escenario doblemente seguro. Dado que las armas ofensivas pueden diferenciarse de las armas defensivas y la defensa tiene ventaja sobre la ofensa, los estados de status quo no están presionados para adquirir armas ofensivas. Además, debido a las posturas que adoptan, los estados agresivos involuntariamente significan sus intenciones. Entonces, si la defensa tiene suficiente ventaja, no hay problemas de seguridad.

Desde su publicación hace unos 40 años, la ODT de Jervis ha sido criticada por algunos académicos. Por ejemplo, Huntington afirma que es imposible establecer una distinción entre armas ofensivas y defensivas.[46] Argumenta que se pueden usar sistemas de armas específicos para acciones ofensivas y defensivas, por lo tanto, el equilibrio ofensivo-defensivo no se puede medir. Sin embargo, Lynn-Jones, un defensor de la ODT, postula que el equilibrio ofensa-defensa se mide por los costos relativos en la adquisición y el despliegue de armas.[47] Como resultado, los estados identifican las armas que son más ventajosas para la ofensa y las que son más ventajosas para la defensa.[48] La preocupación de Huntington, por lo tanto, no invalida la Teoría.

Debido a su poder explicativo y su importancia teórica, varios académicos han identificado a la ODT como una teoría apropiada para evaluar el efecto del poder de la ciberguerra en la seguridad nacional de un estado y cómo se relaciona con el sistema internacional. El estudio de Saltzman reflexiona sobre las capacidades de China, Estados Unidos, Rusia y la OTAN para enfrentar las amenazas del ciberespacio.[49] En su análisis, la ODT ofrece una clara idea respecto a la importancia de la ciberguerra en el equilibrio general del poder militar después de modificar las terminologías para reflejar las ciberarmas.[50] Del mismo modo, Malone usa la Teoría para

---

[46] Huntington, SP. ***US defence strategy: The strategic innovation of the Reagan years***", in Joseph Kruzel (ed.), **American defence mnnual, 1987–1988** (Massachusetts: Lexington Books, 1987), pp.23-43.

[47] SM Lynn-Jones, SM. ***Offense-Defense theory and its critics", Security studies***, Vol.4, No.4, (1995), pp.660–691

[48] SM Lynn-Jones, SM. ***Offense-Defense theory and its critics", Security studies***, Vol.4, No.4, (1995), pp.671.

[49] Saltzman, I ***Cyber posturing and the offence -defense balance, contemporary security policy***, 2013, < http://www.tandfonline.com/doi/abs/10.1080/13523260.2013.771031> accessed 17 Oct 19.

[50] Saltzman, I ***Cyber posturing and the offence -defense balance, contemporary security policy***, 2013, < http://www.tandfonline.com/

desarrollar un modelo que calcula las relaciones de costos de las acciones ofensivas y defensivas con el fin de proporcionar evidencia empírica sobre el equilibrio de las ciberarmas.[51] Los 2 estudios anteriores demuestran que la ODT puede aplicarse efectivamente a la ciberguerra a fin de indicar su impacto en la seguridad nacional.

La ODT se puede usar para predecir resultados probables sobre la relación entre ciberguerra y seguridad nacional en lo que se refiere a las AFN. Las capacidades de las AFN para enfrentar las amenazas del ciberespacio serían más viables cuando la ofensa es menos costosa que la defensa. El corolario de esto es que las AFN también necesitarían estar preparadas para la ciberdefensa, ya que otros países podrían librar una ciberguerra contra Nigeria. Esta situación se hace cada vez más probable a medida que las ciberarmas se vuelven más baratas y más alcanzables, en comparación con las armas cinéticas. Por lo tanto, es necesario que las AFN se esfuercen por lograr el equilibrio adecuado ofensivo-defensivo al enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional. En esta situación, si el escenario de la ciberguerra favorece un equilibrio apropiado entre la defensa y la ofensa, mejoraría la seguridad nacional. Sin embargo, si el equilibrio está sesgado en la dirección opuesta, la seguridad nacional podría verse afectada. El uso de la ODT ha estimulado la necesidad de examinar, a fin de extraer lecciones para el estudio, como el incremento de las capacidades para enfrentar las amenazas del ciberespacio condujeron a una mejora de la seguridad nacional en Estonia y Estados Unidos.

EJEMPLOS DE LA RELACIÓN ENTRE CIBERGUERRA Y SEGURIDAD NACIONAL EN ESTONIA Y ESTADOS UNIDOS

Con el fin de extraer lecciones, el estudio consideró la interacción entre ciberguerra y seguridad nacional en Estonia y EEUU. Estos países fueron seleccionados porque en ellos las capacidades para enfrentar las amenazas del ciberespacio se han incrementado con el fin de mejorar la seguridad nacional en ambos países. Esto se desarrollará en los párrafos siguientes.

CIBERGUERRA Y SEGURIDAD NACIONAL EN ESTONIA

En 2007, el Gobierno de Estonia retiró la estatua de bronce de un soldado que conmemoraba a

doi/abs/10.1080/13523260.2013.771031> accessed 17 Oct 19.

[51] Malone,PJ ***Offense-Defense balance in Cyberspace: A proposed model, institutional archive of the Naval Postgraduate School,*** 2012, < https://calhoun.nps.edu/bitstream/handle/10945/27863/12Dec_Malone_Patrick.pdf?sequence=1> accessed 17 Oct 19.

los soldados soviéticos.[52] Este acto enfureció a la minoría rusa que representaba el 26 por ciento de la población en Estonia y condujo a un ciberataque altamente coordinado de Rusia contra Estonia.[53] Los ciberataques se llevaron a cabo contra ministerios gubernamentales y sistemas financieros con efectos significativos. Esto se debía a que Estonia dependía en gran medida de las TIC para administrar sus asuntos. Por ejemplo, aunque es un país de solo 1.3 millones de personas, en 2007, era uno de los países más avanzados tecnológicamente con más del 86 por ciento de sus transacciones bancarias y el 31 por ciento de las votaciones en línea.[54] Los ataques mostraron la vulnerabilidad de las estructuras que dependen de Internet con un efecto negativo en la seguridad nacional de Estonia.

Después de los ataques, Estonia, a través de sus fuerzas armadas, instituyó varios cambios en sus políticas de ciberguerra. Lanzó una ciberestrategia basada en la protección de la infraestructura crítica, el ciberdelito y la defensa nacional y el establecimiento de la Liga de Ciberdefensa de Estonia.[55] La instauración de la Liga de Ciberdefensa significa una notable iniciativa de cooperación entre las fuerzas armadas y el sector privado en Estonia.[56] La Liga incluye a algunos de los mejores civiles del país con trabajos de TIC bien remunerados de los sectores público y privado que sirven sin tener que unirse formalmente al ejército.[57] Estonia también amplió su alianza con la OTAN con respecto a las capacidades para enfrentar las amenazas del ciberespacio. Esto dio como resultado el establecimiento del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN.[58] En virtud de sus esfuerzos concertados, Estonia tiene las mejores capacidades para enfrentar las amenazas del ciberespacio de Europa y es la quinta del mundo en la materia, según el Índice de la UIT 2017.[59] El incremento en estas capacidades ha mejorado la seguridad nacional de Estonia.

CIBERGUERRA Y SEGURIDAD NACIONAL EN ESTADOS UNIDOS

[52] Kozlowski A. ***Comparative analysis of cyber-attacks on Estonia, Georgia and Kyrgyzstan", European scientific journal***, Vol.3, (2014).

[53] Kozlowski A. ***Comparative analysis of cyber-attacks on Estonia, Georgia and Kyrgyzstan", European scientific journal***, Vol.3, (2014).

[54] **Blair, D "***Estonia recruits volunteer army of 'cyber warriors", The telegraph***, 26 Apr 15, <http://www.telegraph.co.uk/news/worldnews/europe.html> accessed 18 Oct 19.**

[55] **Brenner, SW.** *Cyber threats and the decline of the nation-state***, New York: Routledge, 2014, pp.205-211.**

[56] **Hsu, J.** *Cyber Warriors Need Not Be Soldiers***",** Discover**, 8 Mar 15, <http://blogs.discovermagazine.com/lovesick-cyborg/2015/03/08/cyber-warriors-need-not-soldiers/#.WjVKnd-nFPY> accessed 18 Oct 19.**

[57] **Hsu, J.** *Cyber Warriors Need Not Be Soldiers***",** Discover**, 8 Mar 15, <http://blogs.discovermagazine.com/lovesick-cyborg/2015/03/08/cyber-warriors-need-not-soldiers/#.WjVKnd-nFPY> accessed 18 Oct 19.**

[58] Taddeo M and Glorioso, L. **Ethics and policies for cyber operations**, (Italy: Springer, 2017), p.17.

[59] Taddeo M and Glorioso, L. **Ethics and policies for cyber operations**, (Italy: Springer, 2017), p.17.

Como país desarrollado, EEUU depende mucho de Internet y, por lo tanto, está significativamente expuesto a los ciberataques. A través de los años, se ha visto involucrado en varios incidentes de ciberguerra tanto en posiciones defensivas como ofensivas.[60] En 2009, Estados Unidos elevó sus capacidades para enfrentar las amenazas del ciberespacio al establecer un Cibercomando.[61] El Cibercomando fue creado bajo la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) para desplegar ciberarmas, defender las redes del Departamento de Defensa y proteger la infraestructura civil crítica.[62] Estos roles se ampliaron a lo largo de los años para mejorar sus capacidades para enfrentar las amenazas del ciberespacio y, por extensión, la seguridad nacional de los EEUU.

En agosto de 2017, el Cibercomando se actualizó a un comando independiente, liberándolo de las restricciones derivadas de trabajar junto con la NSA.[63] También hubo un aumento en la fuerza del personal involucrado en el enfrentamiento de las amenazas del ciberespacio pasando de 1.800 en 2014 a 6.000 en 2016.[64] Además, el presupuesto para el Cibercomando aumentó en casi un 100 por ciento pasando de US$ 190 millones en 2014 a US$ 365 millones en 2015, aparte de los U$S, billones de dólares que se destinaron al Departamento de Defensa, el Ejército, la Armada y la Fuerza Aérea, específicamente para el enfrentamiento de las amenazas del ciberespacio.[65] La Estrategia del Departamento de Defensa de 2015 para el enfrentamiento de las amenazas del ciberespacio estaba dirigida a mantener las fuerzas y capacidades con el fin de llevar a cabo operaciones en el ciberespacio, defender las redes de defensa y la infraestructura crítica de los EEUU de los ciberataques disruptivos de consecuencias significativas.[66] También incluyó disposiciones para la cooperación conjunta que comprende los sectores público y privado, así

---

[60] O Haizler, O.The United States. ***Cyber warfare history: Implications on modern cyber operational structures and policy making, Cyber intelligence and security,*** Vol.1, No.1, 2017.

[61] **Breene, K.** *Who are the cyberwar superpowers?"* World economic forum**, 4 May 16**, **<https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ > accessed 18 Oct 19.**

[62] **Breene, K.** *Who are the cyberwar superpowers?"* World economic forum**, 4 May 16**, **<https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ > accessed 18 Oct 19.**

[63] **Baldor, LC.** *U.S. to create the independent U.S. Cyber Command, split off from NSA***",** PBS**, 17 Jul 17, < https://www.pbs.org/newshour/politics/u-s-create-independent-u-s-cyber-command-split-off-nsa> accessed 18 Oct 19.**

[64] **Breene, K.** *Who are the cyberwar superpowers?"* World economic forum**, 4 May 16**, **<https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ > accessed 18 Oct 19.**

[65] Marks, J ***U.S. Cyber command funding nearly doubled this year — On your radar***: Budget's coming, State's got mail, CISA watch still on", **Politico**, 17 Mar 15, < https://www.politico.com/tipsheets/morning-cybersecurity/> accessed 19 Oct 19.

[66] "The Department of Defence Cyber Strategy", **Department of Defence**, April 2015, <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_ DoD_Cyber strategy _for_web.pdf> accessed 19 Oct 19.

como la cooperación internacional.[67] Estados Unidos ya está utilizando la ciberguerra en su lucha contra el terrorismo contra el Estado Islámico de Irak y Siria, y ha indicado su capacidad para responder a la supuesta intromisión electoral de Rusia.[68] Estas iniciativas, en gran medida, demuestran que las capacidades de Estados Unidos para enfrentar las amenazas del ciberespacio fueron incrementadas a fin de mejorar la seguridad nacional y, por lo tanto, presentan algunas lecciones para este estudio.

LECCIONES APRENDIDAS DE ESTONIA Y ESTADOS UNIDOS

Las lecciones aprendidas de los esfuerzos para enfrentar las amenazas del ciberespacio, llevados adelante por Estonia y Estados Unidos, con el fin de mejorar la seguridad nacional, son: la necesidad de tener una política efectiva para enfrentar las amenazas del ciberespacio, la necesidad de contar con instituciones especializadas en el enfrentamiento de las amenazas del ciberespacio y la necesidad de cooperación con el sector privado y los asociados internacionales. Estas lecciones se discuten en párrafos posteriores.

Necesidad de tener una política efectiva para enfrentar las amenazas del ciberespacio. Los gobiernos de Estonia y Estados Unidos establecieron políticas integrales que proporcionaron un marco para sus esfuerzos en una ciberguerra. Estas políticas ayudaron a guiar a sus Fuerzas Armadas, así como a otras ciberfuerzas, y centraron sus esfuerzos en el resguardo de sus operaciones de defensa e infraestructura crítica, así como en la realización de ciberoperaciones ofensivas cuando fuere necesario, para mejorar la seguridad nacional. La lección para el estudio es que los países necesitan desarrollar políticas integrales en el ciberespacio a fin de impulsar su postura de ciberdisuasión y preparar a sus fuerzas armadas para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional.

Necesidad de contar con instituciones especializadas en el enfrentamiento de las amenazas del ciberespacio. Tanto Estonia como EEUU entendieron la necesidad de tener una estructura dedicada a realizar operaciones ofensivas y defensivas en el ciberespacio. Estonia adoptó un enfoque que activa la integración de una liga de ciberdefensa de ciberexpertos con las Fuerzas Armadas para proteger su infraestructura en tiempos de ciberataques con consecuencias

[67] "The Department of Defence Cyber Strategy", **Department of Defence**, April 2015, <https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_Cyber strategy_for_web.pdf> accessed 19 Oct 19.

[68] Sanger, DE. ***USA Cyber attacks target ISIS in a new line of attacks***", **New York Times**, 24 Apr 16, < https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-sfirst-time.html> accessed 19 Oct 19.

importantes. Por otro lado, Estados Unidos estableció una organización independiente llamada Cibercomando, tripulada en gran medida por las Fuerzas Armadas para el enfrentamiento de las amenazas del ciberespacio. De cualquier manera, ambos países entendieron que era necesario tener protocolos y procedimientos establecidos para gobernar las ciberoperaciones manteniéndolo abierto para uso propio mientras se interrumpe el acceso del adversario. La escisión del Cibercomando de EEUU de la NSA en 2017 es instructiva, ya que le da al Cibercomando la libertad de acción para operar en el ciberespacio. Estonia y los EEUU usan la Liga de Ciberdefensa y el Cibercomando respectivamente para participar en el ciberespacio. La lección inherente a este estudio es que un país puede, en función de sus particularidades, establecer un organismo dedicado a través del cual sus fuerzas armadas protejan el ciberespacio con el fin de mejorar la seguridad nacional del país.

Necesidad de cooperación con el sector privado y los asociados internacionales. El Gobierno de Estonia tenía un amplio nivel de cooperación con la OTAN y aprovechó esta cooperación para tener instituciones vitales de ciberseguridad ubicadas en Estonia. Esto finalmente se tradujo en un incremento de las capacidades de Estonia para enfrentar las amenazas del ciberespacio. Del mismo modo, tanto Estonia como EEUU se relacionan con el sector privado en materias como ciberdefensa y protección de infraestructura crítica. Esto ayuda a garantizar una coordinación y armonización adecuadas de los procedimientos en caso de ciberataques. La lección clave para el estudio es que cuando los países cooperan con el sector privado y los asociados internacionales en materia de ciberseguridad, finalmente, logran un incremento de las capacidades para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional.

CAPÍTULO 3:
EVALUACIÓN DE LAS CAPACIDADES DE LAS AFN PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO A FIN DE MEJORAR LA SEGURIDAD NACIONAL

Este capítulo describe una visión general de la relación entre ciberguerra y seguridad nacional en Nigeria. Luego se presentan los datos de la investigación y se discuten los problemas e implicancias asociadas con las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria. Posteriormente, se identifican los desafíos asociados con las capacidades de las AFN para enfrentar las amenazas del ciberespacio en la mejora de la seguridad nacional en Nigeria. Finalmente, se presentan las perspectivas para incrementar las capacidades de las fuerzas armadas para enfrentar las amenazas del ciberespacio con el fin de mejorar la seguridad nacional de Nigeria, así como un resumen de los resultados de la investigación.

VISIÓN GENERAL DE LA RELACIÓN ENTRE CIBERGUERRA Y SEGURIDAD NACIONAL EN NIGERIA

Esta sección ofrece una perspectiva histórica de la relación entre ciberguerra y seguridad nacional en Nigeria. Esto se discutirá observando los desarrollos de las capacidades para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria en los siguientes segmentos de tiempo: 1990-2000, 2001-2010 y 2011-2018.

Desarrollo de las capacidades para enfrentar las amenazas del ciberespacio 1990-2000

Antes de la década de 1990, la infraestructura de las TIC en Nigeria se componía principalmente de sistemas informáticos independientes. La mayoría de los sistemas TIC financieros, de aviación o militares no estaban conectados en red. Como resultado, los datos no se compartieron entre los diversos sistemas independientes, lo que significaba que los sistemas de TIC enfrentaban ciberriesgos mínimos.[69] Sin embargo, a partir de la década de 1990, la infraestructura de TIC de Nigeria comenzó a evolucionar. A medida que las redes e Internet ganaron importancia y que más organizaciones en Nigeria adoptaron la informatización, las redes de computadoras aumentaron para permitir operaciones centralizadas.[70] Este desarrollo hizo que

[69] Cornick, M. **Health informatics: Transforming healthcare with technology**, Sidney: Cengage Learning, 2006, p.4.
[70] Robertazzi, TG.**Introduction to computer networking**, Stony Brook: Spinger international publishing, 2017, p.1

los sistemas de TIC fueran más vulnerables a los ciberataques, como virus informáticos, gusanos y otro software malicioso. Esta situación fue parcialmente mitigada por la oscuridad de las soluciones de TIC patentadas en ese momento.[71] Sin embargo, los ciberataques no alcanzaron el nivel que requería atención a gran escala por parte de las AFN, además de los esfuerzos necesarios para proteger los sistemas de las AFN. Por lo tanto, las políticas TIC vigentes en ese momento se centraron principalmente en el uso de computadora por parte de las 3 Fuerzas. Como las ciberoperaciones aún no habían evolucionado, no se previó para las AFN un marco de políticas de ciberguerra.

Desde mediados de la década de 1990, los avances en las TIC y el aumento de la conectividad de computadoras y otros dispositivos a Internet llevaron a un aumento en el número de usuarios de computadoras en Nigeria a casi 200.000 a fines de la década de 1990.[72] Varios de estos usuarios explotaron el medio para promover una actividad criminal existente conocida como Estafas de Pago por Adelantado (AFF, por sus siglas en inglés).[73] Las AFF están asociadas con la recepción fraudulenta de dinero con el pretexto de ofrecer un servicio. Con el aumento continuo de usuarios de Internet en todo el mundo de 26 millones en 1995 a más de 400 millones en 1999, los incidentes de cibercrimen en Nigeria como las AFF, robo de identidad y virus aumentaron geométricamente.[74] Estas fueron las principales ciberamenazas en el momento que tuvieron implicancias en la seguridad nacional de Nigeria.[75] Las AFN no tuvieron un papel clave en la lucha contra estas amenazas, ya que estas fueron abordadas principalmente por la Fuerza de Policía de Nigeria y otras agencias de aplicación de la ley en el país. Además, el marco institucional de las AFN no fue diseñado para combatir ciberdelitos o llevar a cabo ciberoperaciones, tal como sucede con la ciberguerra. En ese momento, las AFN no estaban adecuadamente preparadas para para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

Hacia fines de 1999, surgió otra amenaza conocida como el Efecto 2000, Problema del Año 2000

---

[71] Robertazzi, TG.**Introduction to computer networking**, Stony Brook: Spinger international publishing, 2017, p.1

[72] ***Nigeria internet usage and telecommunications reports***, <https://www. internetworldstats.com/af/ng.htm> accessed 19 Oct 19.

[73] Waziri, FM. **Advance fee fraud, National security and the law**, Ibadan: Book builders, 2005, p.2.

[74] **P Norris, P.** *Digital divide: Civic engagement, information poverty, and the internet worldwide*, **Boston: Cambridge university press, 2001, p.45.**

[75] Omodunbi BA et al., ***Cybercrimes in Nigeria: Analysis, detection and prevention***, **journal of engineering and technology**, Vol.1, No.1, 2016, p.1.

o Millennium Bug.[76] Esta fue una amenaza global que enfrentaron todos los dispositivos con circuitos de computadora integrados. Se esperababa que los dispositivos funcionaran mal en enero de 2000 debido a la incompatibilidad de las fechas programadas en ellos con los dígitos para el año 2000. Esto podría poner en peligro los sistemas basados en las TIC, como los utilizados en la banca, la red eléctrica y los sistemas militares.[77] En Nigeria, las medidas para abordar este desafío fueron multiagenciales, ya que los riesgos atravesaron sectores e involucraron a muchas partes interesadas. Por lo tanto, el enfoque requería la colaboración conjunta. Las AFN desempeñaron un papel activo en la coordinación de reuniones e instalación de soluciones recomendadas para los sistemas de TIC dentro de las fuerzas armadas para garantizar que cumplieran con el Año 2000.[78] Sin embargo, las AFN no fomentaron la colaboración conjunta, una iniciativa que podría aprovecharse en una futura ciberguerra con el fin de mejorar la seguridad nacional en Nigeria.

Desarrollo de las capacidades para enfrentar las amenazas del ciberespacio 2001-2010

A partir del año 2001, las tecnologías de redes informáticas proliferaron en Nigeria a medida que se redujo el costo de instalación, aumentando así el acceso para los nigerianos.[79] Como resultado de esta difusión, los sistemas de TIC se volvieron más vulnerables, requiriendo una capacidad técnica más especializada para protegerlos.[80] Cada una de las Fuerzas de las AFN iniciaron medidas para desarrollar la capacidad de las TIC de su personal. Por ejemplo, la NAF ordenó que su personal tuviera conocimientos de informática para fines de 2001.[81] El NA y la NN también tuvieron intervenciones similares para mejorar la capacidad técnica de su personal en las TIC.[82] Estos esfuerzos se tradujeron en un mayor uso de las TIC en las AFN que condujo a más cibervulnerabilidades, a medida que más sistemas en las AFN quedaron expuestos. En ese momento, la capacidad técnica para enfrentar estas cibervulnerabilidades no era adecuada. Necesitaba desarrollarse, particularmente las capacidades técnicas de las AFN para enfrentar las

[76] Bajak,F. ***Y2K bug's: World impact remains unpredictable***, **Amarillo journal of information technology**, Vol.9, No.3, 2000, p.17.

[77] Zittrain, J. **The Future of the internet--and how to stop it**, (Yale: Yale university press, 2008, p.18.

[78] Udoh, TV, Former Chief of Defence Space Administration, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 8 Nov 19.

[79] **Kizza, JM.** Guide to computer network security**, New York: springer science & business media, 2013, p.297.**

[80] **Kizza, JM.** Guide to computer network security**, New York: springer science & business media, 2013, p.297.**

[81] Ladan, D Director, Information Technology, Headquarters Nigerian Air Force, Interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at HQ NAF, Abuja 0n 1 Nov 19.

[82] Ladan, D Director, Information Technology, Headquarters Nigerian Air Force, Interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at HQ NAF, Abuja 0n 1 Nov 19.

amenazas del ciberespacio a fin de mejorar la seguridad nacional en el país.

Las AFN también realizaron esfuerzos concertados para garantizar que sus funciones operativas, logísticas y administrativas fueran informatizadas.[83] Los registros de personal de las diversas fuerzas se computarizaron entre 2002 y 2007. También se hicieron esfuerzos para adquirir infraestructura para enfrentar las amenazas del ciberespacio para proteger la infraestructura adquirida de 2008 a 2010.[84] Sin embargo, la infraestructura para enfrentar las amenazas del ciberespacio de las AFN era inadecuada en ese momento, ya que el proveedor de servicios de Internet clave para las AFN, Galaxy Backbone Limited, indicó que la infraestructura del lado del usuario era vulnerable. Más aún, la adquisición de infraestructura para enfrentar las amenazas del ciberespacio no fue armonizada por las 3 Fuerzas.

Por lo tanto, era necesario considerar formas de mejorar la infraestructura para enfrentar las amenazas del ciberespacio de las AFN a fin de mejorar la seguridad nacional en Nigeria.

Desarrollo de las capacidades para enfrentar las amenazas del ciberespacio 2011-2018

Para 2011, la ciberguerra se había convertido en una preocupación para los gobiernos de todo el mundo, particularmente después de los ciberataques contra Irán y Estonia en los años anteriores.[85] En las AFN, el enfoque en la ciberguerra se debió a la creciente dependencia del equipo con tecnologías informáticas como aeronaves, sistemas de conciencia de dominio y sistemas de comunicación. También se debió a las operaciones antiterroristas en el noreste en las que el BHT había infundido la ciberoperación en sus actividades. En agosto de 2012, el BHT presuntamente hackeó los registros del DSS y expuso la información personal de los agentes del DSS.[86] Para abordar las ciberamenazas en el país, las FGN promulgaron la Política y Estrategia Nacional de Ciberseguridad (NCSPS, por sus siglas en inglés) en 2014.[87] Este documento de política describió el marco de ciberseguridad de Nigeria.

---

[83] Daramola, A. Commander, 105 Communications Group, Shasha Lagos, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria, Lagos on 8 Nov 19.

[84] Daramola, A. Commander, 105 Communications Group, Shasha Lagos, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria, Lagos on 8 Nov 19.

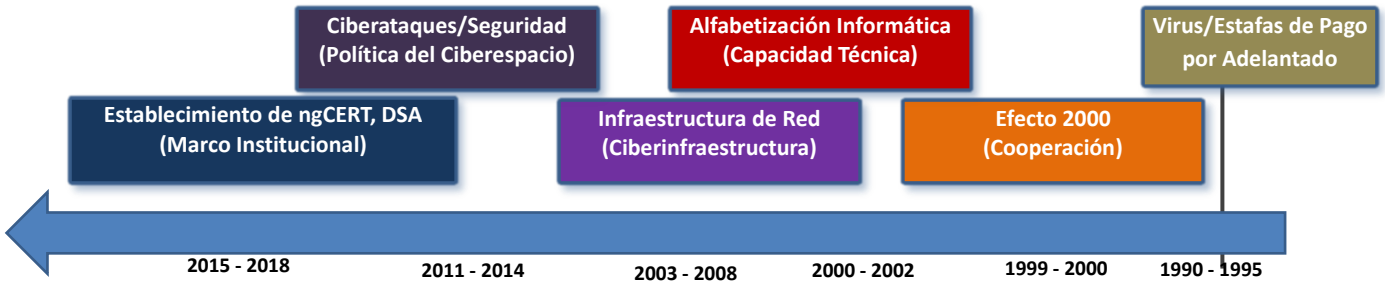
[85] Martin, G. Feature: Cyber and electronic warfare an increasing global challenge, **Defence Web**, 9 Nov 17, < http://www.defenceweb.co.za/index.php?option=com_ content& view=article &id=49817&catid=74&Itemid=30> accessed 20 Oct 19.

[86] Manrzikos, I. Exploring Nigeria's vulnerability in cyber warfare, Modern diplomacy, 22 Jul 13, < https://moderndiplomacy.eu/2013/07/22/exploring-nigerias-vulnerability-in-cyber-warfare/> accessed 20 Oct 19.

[87] National cyber security policy and strategy, 2014, <https://www2.cert.gov.ng/images/uploads/National_cybersecurity_policy.pdf> accessed 20 Oct 19.

En 2015, las FGN promulgaron la Ley de Cibercrimen (Prohibición, Prevención, etc.) de Nigeria.[88] La Sección 41 de la Ley autorizó a la ONSA a supervisar los esfuerzos de ciberseguridad de las AFN.[89] Un extracto de esta sección se encuentra en el Anexo 1. Como uno de sus mandatos, la ONSA estableció el Equipo de Respuesta a Emergencias Informáticas de Nigeria (ngCERT, por sus siglas en inglés) en mayo de 2015. El plan era que todos los sectores, incluidas las AFN, establecieran Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) para colaborar con el ngCERT en la lucha contra las ciberamenazas, formando así un sistema robusto para mejorar la seguridad nacional en Nigeria.[90] En 2015, el DHQ estableció una célula de ciberseguridad, mientras que la Ley DSA de 2016 convirtió la ciberseguridad en una parte integral de la DSA.[91] En la Figura 1.1 se encuentra una línea de tiempo que ilustra los desarrollos de las AFN para enfrentar las amenazas del ciberespacio.

Figura 1.2: Línea de tiempo que ilustra los desarrollos de las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio



Fuente: Diseño del investigador, 2019.

[88] CyberCrime (Prohibition,Prevention,etc) Act, 2015, < https://cert.gov.ng/images/ uploads/Cybercrime (Prohibition, Prevention, etc)_Act,_2015.pdf> accessed 20 Oct 19.

[89] CyberCrime (Prohibition,Prevention,etc) Act, 2015, < https://cert.gov.ng/images/ uploads/Cybercrime (Prohibition, Prevention, etc)_Act,_2015.pdf> accessed 20 Oct 19.

[90] **"NCC to establish computer security response teams for telecoms",** Nigeria communications week**, 28 Oct 16, <http://nigeriacommunicationsweek.com.ng/ncc-to-establish-computer-security-response-teams-for-telecoms/> accessed 20 Oct 19.**

[91] Defence space administration Act, 2016, < http://www.nassnig.org/document/ download/9421> accessed 20 Oct 19.

Las capacidades antes mencionadas de las AFN no fueron diseñadas para ciberoperaciones ofensivas, tal como sucede una ciberguerra. Por lo tanto, es necesario tomar medidas para posicionar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

Presentación de los Datos de Investigación

El objetivo de la encuesta utilizada en este estudio fue evaluar la relación entre las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria. Los datos generados a partir de la encuesta se presentan en esta sección de la siguiente manera:

Datos de la Muestra

Se administraron un total de 350 copias del cuestionario, de las cuales se devolvieron 308 copias completas, lo que indica una tasa de devolución del 88%. El diseño de la encuesta aseguró que solo se enviaran respuestas válidas, por lo tanto, se encontró que las 308 respuestas enviadas eran válidas para el análisis.

La alta tasa de respuesta es suficiente para generalizar los resultados a la población objetivo, afirmando así la validez externa del estudio.

Características de los Encuestados

Los encuestados que recibieron el cuestionario pertenecen a las especializaciones relacionadas con las TIC en las 3 Fuerzas. Los atributos clave y demográficos de estos encuestados se encuentran en el Apéndice 4.

Los atributos de los encuestados son similares a los parámetros de la población, lo que hace que la muestra sea una buena representación de la población. También se realizaron entrevistas no estructuradas con encuestados de las AFN, agencias gubernamentales y el sector privado.

Información y análisis de la Encuesta

En las respuestas de la encuesta en el Apéndice 5, las Preguntas 10 y 11 proporcionaron respuestas a las preguntas sobre el marco de políticas de ciberguerra, las Preguntas 12 y 13 respondieron a las preguntas sobre el marco institucional, mientras que las Preguntas 14 y 15 respondieron a las preguntas sobre la capacidad técnica. Además, las preguntas 16 y 17 respondieron a las preguntas sobre la infraestructura para enfrentar las amenazas del ciberespacio

y las preguntas 18 y 19 respondieron a las preguntas sobre la colaboración conjunta, mientras que las preguntas 20 a 22 fueron preguntas generales sobre la relación entre las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional. Por último, las preguntas 23 a 27 proporcionaron respuestas a preguntas sobre los alcances de las capacidades de las AFN para enfrentar las amenazas del ciberespacio en algunos atributos de la seguridad nacional.

Los aspectos más destacados del análisis de datos sobre las preguntas de la encuesta se incorporaron en la sección posterior de este capítulo. Además, también se presenta una explicación del análisis de correlación en una sección posterior del capítulo. Los datos presentados subrayan la necesidad de discutir temas asociados con las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria.

PROBLEMAS ASOCIADOS CON LAS CAPACIDADES DE LAS AFN PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO Y LA SEGURIDAD NACIONAL EN NIGERIA

Los problemas asociados con las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional incluyen el marco de políticas de ciberguerra, el marco institucional y la colaboración conjunta. Otros son la capacidad técnica y la infraestructura para enfrentar las amenazas del ciberespacio. Estos temas se discuten en párrafos posteriores.

Marco de Políticas de Ciberguerra

El Marco de Políticas de Ciberguerra en el contexto nigeriano, incorpora las pautas que proporcionan un curso de acción estandarizado para la conducción del enfrentamiento de las amenazas del ciberespacio por parte de las AFN con el fin de mejorar la seguridad nacional. Una Política para enfrentar la ciberguerra es esencial para la conducción eficiente de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Según Aguiyi, una política integral de ciberguerra describiría el protocolo y los procedimientos generales para llevar a cabo las ciberacciones de ofensivas y defensivas de las AFN a fin de mejorar la seguridad nacional en Nigeria.[92] La política existente que aborda las

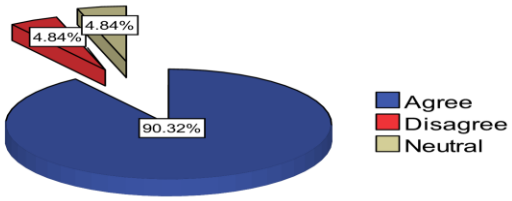
[92] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

amenazas y cibervulnerabilidades en Nigeria es la NCSPS 2014.[93] Este marco de políticas está dirigido a fortalecer la capacidad de Nigeria para responder a las ciberamenazas a fin de mejorar la seguridad nacional del país. La implementación de la NCSPS 2014 tuvo un impacto positivo en la clasificación de Nigeria en el Índice Global de Ciberseguridad (GCI, por sus siglas en inglés), que mide el nivel de compromiso de un país con la ciberseguridad.[94] El GCI clasificó a Nigeria 57 de un total de 165 países evaluados en 2018. Esto es un reflejo de que el país incluyó medidas en el marco de la UIT, la más importante de las cuales fue la promulgación de la NCSPS 2014. Sin embargo, la NCSPS 2014 no prevé ciberacciones ofensivas. La Sección 1.1.4 de la NCSPS 2014 especifica que la política es principalmente para la defensa contra las ciberamenazas que enfrenta el país.[95] Un extracto de esta Sección se encuentra en el Anexo 1. Udoh destacó la no disposición de una política para las ciberacciones ofensivas requeridas para llevar a cabo la ciberguerra. Hizo hincapié en que la ciberguerra es el nuevo dominio de la guerra después de la tierra, el mar, el aire y el espacio, en el que las naciones deben desarrollar no solo capacidades defensivas, sino también ofensivas.[96] El resultado de la encuesta sobre la opinión de los encuestados respecto a la importancia de una política para enfrentar las amenazas del ciberespacio para que las AFN lleven a cabo la ciberguerra a fin de mejorar la seguridad nacional en Nigeria se muestra en la Tabla 1.0 y la Figura 1.3.

Tabla 1.0: Opinión de los encuestados sobre la importancia de una Política de Ciberguerra para las Fuerzas Armadas de Nigeria

N°	Respuesta	Frecuencia	Porcentaje
(a)	(b)	(c)	(d)
1.	De Acuerdo	278	90.32
2.	Desacuerdo	15	4.84
3.	Neutral	15	4.84
4.	Total	308	100

Figura 1.3: Cuadro de opinión de los encuestados sobre la importancia de una Política de Ciberguerra para las Fuerzas Armadas de Nigeria



Fuente: Encuesta de campo de los investigadores, 2019.

[93] National cyber security policy and strategy, 2014, <https://www2.cert.gov.ng/images/uploads/National_cybersecurity_policy.pdf> accessed 20 Oct 19.
[94] Global Cybersecurity Index (GCI) 2019, **International Telecommunication Union**, <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2019-PDF-E.pdf> accessed 1 Nov 19.
[95] National cyber security policy and strategy, 2014, <https://www2.cert.gov.ng/images/uploads/National_cybersecurity_policy.pdf> accessed 20 Oct 19.
[96] Udoh, TV, Former Chief of Defence Space Administration, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 8 Nov 19.

La Figura 1.3 indica que el 90,32 por ciento de los encuestados estuvo de acuerdo en que una Política de Ciberguerra es necesaria para que las AFN lleven a cabo la ciberguerra a fin de mejorar la seguridad nacional, el 4,84 por ciento no estuvo de acuerdo, mientras que el 4,84 por ciento fue neutral. El resultado de la encuesta refuerza la posición de que un marco político para la ciberguerra llevada a cabo por las AFN es necesario. Esto está de acuerdo con Whyte, quien postuló que las AFN necesitan una política específica para la ciberguerra, ya que la NCSPS 2014 no preveía ciberacciones ofensivas.[97] Whyte señaló además que las pautas para los ciberataques ofensivos se detallan mejor en un documento de política para las AFN separado, en lugar de la NCSPS que se distribuye en los sectores público y privado del país.[98] Owolabi también enfatizó que la ciberguerra es una actividad significativa que podría conducir a actividades cinéticas en otros dominios y, como tal, tener una política de ciberguerra para las AFN es esencial.[99] Esta opinión también está de acuerdo con la ODT, ya que subraya la importancia de la ciberguerra en el equilibrio general del poder militar. En la actualidad, la capacidad de las AFN para emprender ciberataques ofensivos es limitada, debido a la ausencia de una Política de Ciberguerra. Una Política de Ciberguerra, entre otros beneficios, enumeraría las reglas de compromiso para el empleo de la ciberguerra por parte de las AFN, mejorando así la seguridad nacional en Nigeria. El marco de Política de Ciberguerra es, por lo tanto, una consideración importante si el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio mejoraría la seguridad nacional de Nigeria

Marco Institucional

La disponibilidad de un marco institucional de ciberguerra es vital para la conducción eficiente de la ciberguerra por parte de las AFN para mejorar la seguridad nacional en Nigeria. Según Saad, un marco institucional describiría los órganos de las AFN para llevar a cabo la ciberguerra y destacaría las responsabilidades específicas de cada uno.[100] La Sección 41 de la Ley Nacional de Ciberdelitos de 2015 autorizó a la ONSA como el organismo coordinador de los militares para

[97] Whyte, EG, Chief of Defence Space Administration, Abuja, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DSA Abuja on 1 Nov 19.

[98] Whyte, EG, Chief of Defence Space Administration, Abuja, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DSA Abuja on 1 Nov 19.

[99] AR Owolabi, Principal General Staff Officer to the Chief of Defence Staff, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19

[100] Saad, A, Head, Nigerian Computer Emergency Response Team, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 4 Nov 19.

defenderse de las ciberamenazas en Nigeria.[101] Del mismo modo, las Secciones 7 y 8 de la Ley DSA de 2016, establecieron la Dirección de Ciberseguridad (DCS, por sus siglas en inglés) y el Centro de Ciberoperaciones de Defensa, respectivamente, para llevar a cabo la ciberseguridad para las AFN.[102] Además, el DHQ y los Servicios tienen subdirecciones de ciberseguridad.[103] Todas estas medidas institucionales tenían como objetivo mejorar la ciberseguridad de las AFN a fin de mejorar la seguridad nacional en Nigeria.

Los esfuerzos de los diversos elementos de las AFN se centraron en gran medida en defender sus redes, sin ningún elemento de ciberacciones ofensivas. Además, los esfuerzos individuales se han llevado a cabo sin sinergia. Por lo tanto, a pesar de la mejora de Nigeria en el GCI, las AFN no ha registrado mejoras proporcionales en sus esfuerzos institucionales. Esto se debió a la ausencia de un equipo de ciberguerra a nivel de DHQ para coordinar o regular asuntos relacionados con los esfuerzos de las Fuerzas. Según Wambai, los esfuerzos institucionales descoordinados hacia la ciberguerra por parte de las AFN llevaron a un aumento de los ciberataques contra las AFN.[104] Por ejemplo, Uneanya señaló que entre enero y diciembre de 2018, Galaxy Backbone registró un total de 4.296 ataques contra redes de las AFN.[105] Fuera de esto, los ataques de 1980 fueron dirigidos a el NA, 396 a la NN y 1920 a la NAF. Uneanya declaró que las ciberdefensas de Galaxy Backbone bloquearon hasta el 97 por ciento de estos ciberataques, sin embargo, el 3 por ciento de los ataques aún podían penetrar las 3 Fuerzas. Un organismo dedicado de cibercoordinación de las AFN podría haber bloqueado el resto para mejorar la seguridad nacional en Nigeria.[106] El resultado de una encuesta de campo de la opinión de los encuestados sobre la necesidad de un marco institucional para la ciberguerra por parte de las AFN para mejorar la seguridad nacional en Nigeria se muestra en la Tabla 1.1 y la Figura 1.4.

[101] CyberCrime (Prohibition,Prevention,etc) Act, 2015, < https://cert.gov.ng/images/ uploads/Cybercrime (Prohibition, Prevention, etc)_Act,_2015.pdf> accessed 20 Oct 19.

[102] Defence Space Administration Act, 2016, < http://www.nassnig.org/document/ download/9421> accessed 4 Nov 19

[103] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

[104] YB Wambai, Director, Cyber Security, Defence Space Administration, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria", at DSA Abuja on 4 Nov 19.

[105] Uneanya ,M Manager, Network Security, Galaxy Backbone Limited, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria, at Abuja on 5 Nov 19.

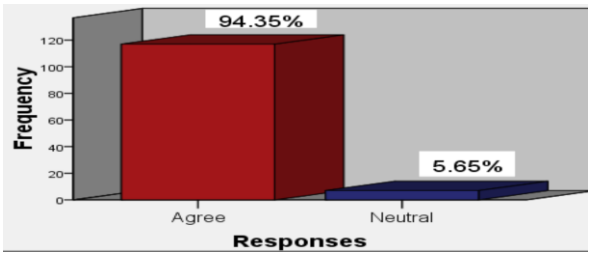
[106] Uneanya ,M Manager, Network Security, Galaxy Backbone Limited, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria, at Abuja on 5 Nov 19.

Tabla 1.1: Opinión de los encuestados sobre la necesidad de un marco institucional para la ciberguerra por parte de las Fuerzas Armadas de Nigeria

N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.	De Acuerdo	291	94.35
2.	Desacuerdo	0	0
3.	Neutral	17	5.65
4.	Total	308	100.00

Fuente: Encuesta de campo de los investigadores, 2019.

Figura 1.4: Gráfico que muestra la opinión de los encuestados sobre la necesidad de un marco institucional para la ciberguerra por parte de las Fuerzas Armadas de Nigeria



La Figura 1.4 indica que el 94,35 por ciento de los encuestados estuvo de acuerdo en que un marco institucional es relevante para llevar a cabo la ciberguerra por parte de las AFN, el 5,65 por ciento fue neutral, mientras que ninguno estuvo en desacuerdo. Esto refuerza el hecho de que el marco institucional es crítico para llevar a cabo una ciberguerra por parte de las AFN a fin de mejorar la seguridad nacional en Nigeria. Esta opinión también está de acuerdo con la ODT, que aboga por un marco para acciones ofensivas y defensivas en el ciberespacio para mejorar la seguridad nacional.[107] Petinrin corrobora este hallazgo, afirmando que, en lugar de subsumir la ciberguerra bajo la ONSA o la DSA, las AFN necesitan un organismo dedicado que le otorgue la estatura, los recursos y las capacidades para enfrentar las en Nigeria.[108] Sin embargo, esto no se ha logrado debido a la ausencia de un centro de coordinación de ciberguerra independiente para que las AFN impulsen la ciberguerra y esto mejore la seguridad nacional en Nigeria. Una institución independiente para la ciberguerra en las AFN ayudaría a integrar todas las ciberoperaciones en las AFN a fin de llevar a cabo una realización efectiva de la ciberguerra por parte de las AFN mejorando la seguridad nacional en Nigeria. El marco institucional es, por lo tanto, una consideración importante el enfrenamiento de las amenazas del ciberespacio, si las AFN van a mejorar la seguridad nacional en Nigeria.

[107] Saltzman,I, Cyber Posturing and the Offense-Defense Balance. **Contemporary Security Policy**, 2013, <http://www.tandfonline.com/doi/abs/10.1080/13523260.2013.771031> accessed 5 Nov 19.

[108] Petinrin,O, Former Chief of Defence Staff, DHQ, Interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 6 Nov 19

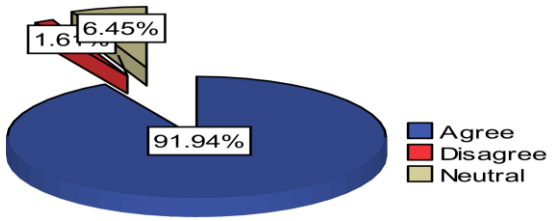
Colaboración Conjunta

La colaboración conjunta es esencial en la realización de una ciberguerra efectiva por parte de las AFN a fin de mejorar la seguridad nacional en Nigeria. Una colaboración conjunta bien coordinada involucraría alianzas entre agencias, asociaciones público-privadas y compromisos internacionales en ciberseguridad involucrando a las AFN para una lograr una mejora de la seguridad nacional en Nigeria. Según Ibrahim, la colaboración conjunta implicaría compartir información sobre posibles amenazas y mejores prácticas en ciberseguridad.[109] Aguiyi reveló que las AFN actualmente colaboran con cerca de 22 partes interesadas, incluidas 10 agencias gubernamentales y 12 organizaciones privadas como NITDA, Galaxy Backbone Limited y New Horizon Limited.[110] Además, señaló que las colaboraciones ayudaron a frustrar los ciberataques en las redes de las AFN, como las alertas sobre los ataques de Ransomware proporcionados por NITDA en 2017.[111] Ajayi también señaló que el DHQ colaboró con una empresa privada, Consultancy Support Services, para llevar a cabo una competencia de piratería para más de 35 nigerianos, de los cuales 15 fueron preseleccionados y 10 fueron empleados por el DSA.[112] El resultado de la encuesta sobre las opiniones de los encuestados sobre la necesidad de que las AFN participen en la colaboración conjunta en sus esfuerzos para enfrentar una ciberguerra a fin de mejorar la seguridad nacional se encuentra en la Tabla 1.2 y la Figura 1.5.

Tabla 1.2: Opinión de los encuestados sobre la necesidad de la colaboración conjunta de las fuerzas armadas de Nigeria en la ciberguerra.

	N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.		De Acuerdo	283	91.94
2.		Desacuerdo	5	1.61
3.		Neutral	20	6.45
4.		Total	308	100.00

Figura 1.5: Cuadro de opinión de los encuestados sobre la necesidad de la colaboración conjunta de las fuerzas armadas de Nigeria en la ciberguerra.



Source: Encuesta de campo de los investigadores, 2019.

[109] H Ibrahim, Director, Information Technology, Naval Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 1 Nov 19

[110] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

[111] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

[112] KC Ajayi, Director, Cyber Security, Defence Space Administration, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at DSA Abuja on 4 Nov 19.

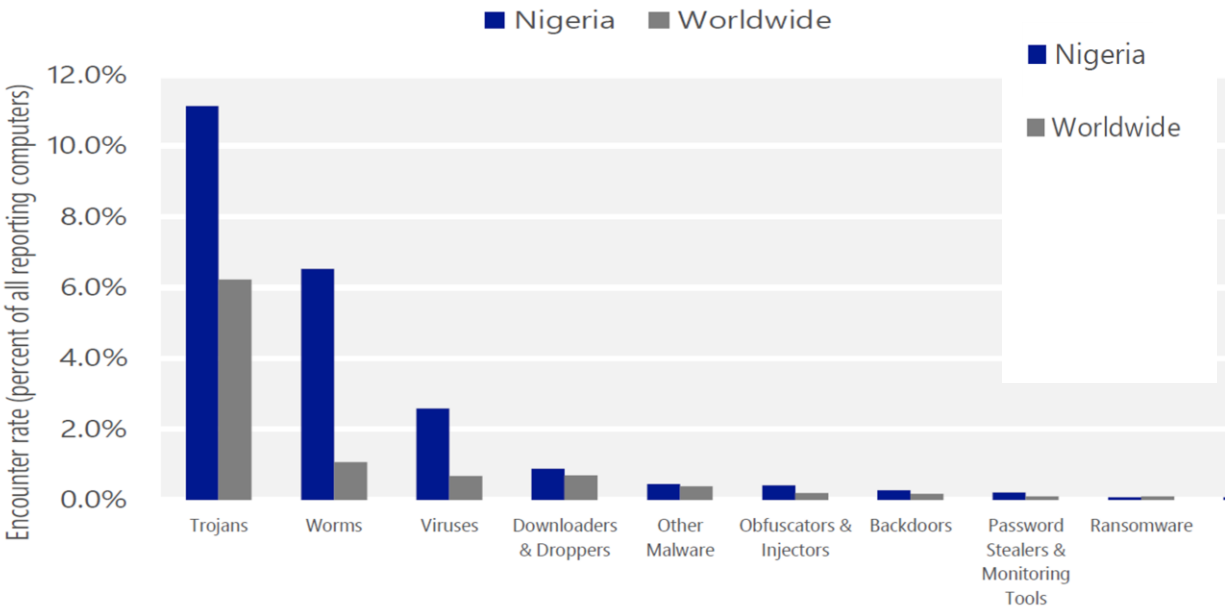
La Figura 1.5 indica que el 91,94 por ciento de los encuestados estuvo de acuerdo en que era necesario que las AFN participaran en la colaboración conjunta en sus esfuerzos ante la ciberguerra, el 1,61 por ciento no estuvo de acuerdo y el 6,45 por ciento fue neutral. Esto refuerza la necesidad de que las AFN colaboren conjuntamente en la ciberguerra. Este hallazgo fue validado por Wariowei, quien afirmó que los vínculos más vitales para la infraestructura de Nigeria están en manos del sector privado, ya que dirigen la mayoría de los sectores críticos.[113] Además, señaló que la colaboración entre ONSA, NITDA, las AFN y otros, mitigó los ciberataques ransomware de la variedad WannaCry de 2017, que afectaron a más de 200.000 computadoras en 150 países.[114] Esto también es consistente con la ODT que enfatiza la optimización de todos los recursos tanto para las ciberacciones defensivas como para las ofensivas. Sin embargo, las AFN no pueden optimizar los beneficios de la colaboración para sus esfuerzos en una ciberguerra debido a la falta de un marco de colaboración de ciberguerra que es esencial para mejorar el potencial de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de lograr una mejora de la seguridad nacional en Nigeria. Además, la falta de un marco institucional dificulta la realización de cualquier tipo de cooperación interinstitucional.

Infraestructura de la Ciberguerra

La infraestructura de la ciberguerra desempeña un papel importante en la conducción efectiva de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Según Ajijola, la infraestructura de la ciberguerra implica hardware, software y dispositivos de red capaces de defenderse contra ciberataques como malware y ataques DDoS, mientras que al mismo tiempo se utilizan para ciberoperaciones ofensivas.[115] La Figura 1.6 indica algunos ciberataques de malware en Nigeria en 2018.

[113] DS Wariowei, Head Cyber Security, National Information Technology Development Agency, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.
[114] DS Wariowei, Head Cyber Security, National Information Technology Development Agency, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.
[115] AH Ajijola, Executive Chairman, Consultancy Support Services Limited, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at Abuja on 7 Nov 19.

Figura 1.6: Gráfico que muestra los ciberataques de malware en Nigeria en 2018



Fuente: Informe de inteligencia de seguridad de Microsoft, 2018**.**

La Figura 1.6 muestra que en 2018, Nigeria experimentó ataques de Malware más altos que el promedio mundial, excepto Ransomware. Esto es un reflejo de la gama de posibles ataques contra las AFN, que exige una infraestructura efectiva de ciberguerra. El estado actual de la infraestructura que las AFN podrían utilizar para la ciberguerra comprende una combinación de conmutadores, enrutadores y dispositivos de firewall, distribuidos por toda las AFN, así como el software utilizado para la detección de intrusos y antimalware. Estos equipos, algunos de los cuales figuran en el Apéndice 6, son inadecuados para la ciberguerra, que incluye ciberacciones ofensivas y defensivas.

Ibrahim postula que aunque estos equipos brindan cierta protección para los sistemas de TIC en las AFN, ellos tienen capacidades limitadas para ciberoperaciones ofensivas, lo que es crucial para la ciberguerra.[116] Este argumento es consistente con la ODT que argumenta que los países confían más en la ofensiva que en la defensa cuando creen que las tecnologías favorecen más el

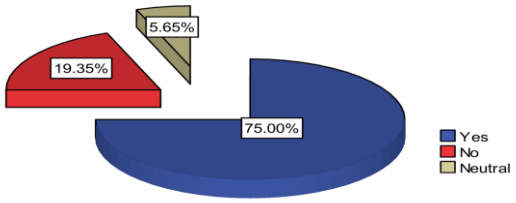
[116] H Ibrahim, Director, Information Technology, Naval Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 1 Nov 19

ataque que la defensa.[117] El resultado de la encuesta sobre si el estado de la infraestructura de la ciberguerra en las AFN obstaculiza la participación en una ciberguerra por parte de las AFN se encuentra en la Tabla 1.3 y la Figura 1.7.

Tabla 1.3: Opinión de los encuestados sobre si el estado de la infraestructura de ciberguerra obstaculiza la participación en una ciberguerra.

N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.	Yes	231	75.00
2.	No	60	19.35
3.	Neutral	17	5.65
4.	Total	308	100.00

Figura 1.7: Cuadro de opinión de los encuestados sobre si el estado de la infraestructura de ciberguerra obstaculiza la participación en una ciberguerra.



Fuente: Encuesta de campo de los investigadores, 2019.

La Figura 1.7 indica que el 75 por ciento de los encuestados creía que el estado de la infraestructura de ciberguerra de las AFN dificulta la realización de una ciberguerra, el 19,35 por ciento no estuvo de acuerdo, mientras que el 5,65 por ciento fue neutral. Esto refuerza el hecho de que la infraestructura contemporánea de ciberguerra de las AFN es crítica para la ciberguerra. El hallazgo fue corroborado por Edet, quien argumentó que poseer capacidades para enfrentar las amenazas del ciberespacio efectivas implica tener fuertes capacidades ofensivas y defensivas, y las AFN carecen de la infraestructura para ambos, particularmente para la acción ofensiva.[118] Sin embargo, Edet señaló que el mal estado de la infraestructura de ciberguerra de las AFN podría atribuirse a centrarse en la adquisición de cibertecnología a expensas de la producción autóctona a través de Investigación y Desarrollo (I + D).[119] En esencia, la escasez de infraestructura de ciberguerra de las AFN se debe en gran parte a la escasa I + D en cibertecnologías en Nigeria. Por lo tanto, la infraestructura de ciberguerra es una consideración vital si se busca incrementar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria

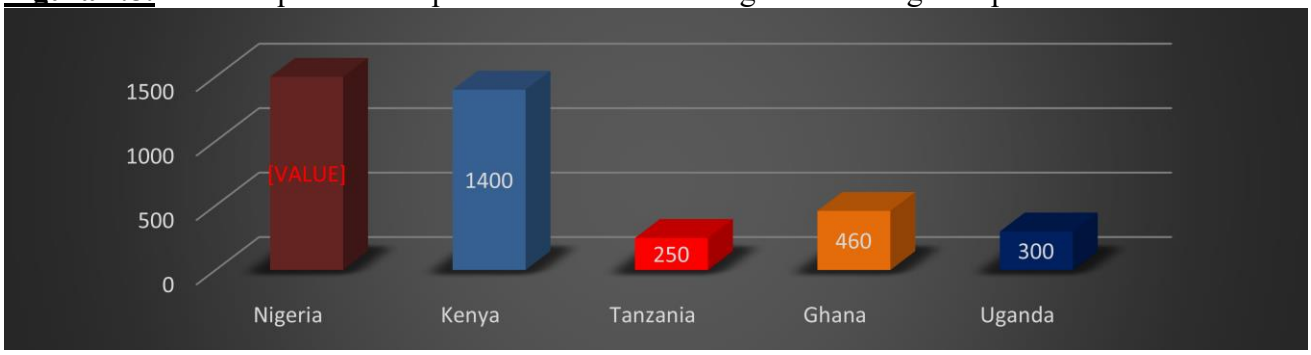
[117] R Jervis, Cooperation under the Security Dilemma, **World Politics**, Vol.30, No.2, (1978)**.**
[118] E Edet, **Op.Cit**.
[119] E Edet, **Op.Cit**.

Capacidad Técnica

La capacidad técnica es esencial para una conducción eficiente de la ciberguerra por parte de las AFN a fin mejorar la seguridad nacional en Nigeria. Según Udoh, la capacidad técnica para la ciberguerra implica tener personal con la capacitación y experiencia necesarias en actividades relacionadas con la ciberguerra.[120] Además de la formación de pregrado o posgrado, algunas certificaciones aplicables a la ciberguerra incluyen Certified Ethical Hacker (CEH) y Certified Penetration Tester (CPT).[121] Una lista de las certificaciones de ciberseguridad se encuentra en el Apéndice 7.

A partir de 2018, de los 6.892 profesionales de ciberseguridad en África, Nigeria tenía 1.500, lo que representa el 21,8 por ciento de los profesionales de ciberseguridad de África.[122] Para Nigeria, con una población de aproximadamente 97 millones de usuarios de Internet, esto representa un profesional de ciberseguridad por cada 65.000 usuarios de Internet.[123] En comparación, Kenia tiene un profesional de ciberseguridad por cada 26.000 usuarios de Internet.[124] El desglose de los profesionales de ciberseguridad en algunos países africanos se muestra en la Figura 1.8.

Figura 1.8: Gráfico que muestra profesionales de ciberseguridad en algunos países africanos



Fuente: Banco Mundial, 2018.

En las AFN, la capacidad técnica para la ciberguerra se basa en las TIC, las señales, las comunicaciones y las especialidades relacionadas en las Fuerzas, que fueron el grupo de los

[120] Udoh, TV, Former Chief of Defence Space Administration, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 8 Nov 19.

[121] E Tittel and K Lindros, "Best Information Security Certifications 2018", Toms IT Pro, 12 Dec 17, <http://www.tomsitpro.com/articles/information-security-certifications. html> accessed 5 Nov 19.

[122] Nigeria Cyber Security Report 2017, **Serianu**, <http://www.serianu.com/ downloads/NigeriaCyberSecurityReport2017.pdf> accessed 5 Nov 19.

[123] Nigeria Cyber Security Report 2017, **Serianu**, <http://www.serianu.com/ downloads/NigeriaCyberSecurityReport2017.pdf> accessed 5 Nov 19.

[124] Nigeria Cyber Security Report 2017, **Serianu**, <http://www.serianu.com/ downloads/NigeriaCyberSecurityReport2017.pdf> accessed 5 Nov 19.

encuestados. La tabla 1.4 muestra la disposición de las certificaciones de ciberseguridad de los encuestados. Indica que el 33 por ciento de los encuestados tienen certificaciones de ciberseguridad. Esto comprende 24 por ciento en el NA y 38 por ciento cada uno en la NN y la NAF. De acuerdo con la ODT, una fuerte capacidad técnica es vital para que las AFN lleven a cabo una ciberofensa y una ciberdefensa efectiva a fin de mejorar la seguridad nacional en Nigeria. Estas estadísticas son consistentes con la sociedad en general, ya que Aladenusi postuló que una gran proporción de doctorados en cursos relacionados con la informática en Nigeria no eran expertos en ciberseguridad.[125] Esto también es consistente con la opinión de Wambai de que la escasa capacidad técnica en ciberseguridad en las AFN ha dificultado llenar los espacios de ciberseguridad en el DSA.[126]

Tabla 1.4: Disposición de las certificaciones de ciberseguridad de los encuestados

N°	Fuerza	Tienen una Certificación en Ciberseguridad	No tienen una Certificación en Ciberseguridad	Total	Porcentaje
(a)	(b)	(c)	(d)	(e)	(f)
1.	Nigerian Army	30	92	122	24 per cent
2.	Nigerian Navy	13	19	32	38 per cent
3.	Nigerian Air Force	59	95	154	38 per cent
4.	Total	102	206	308	33 per cent

Fuente: Encuesta de campo de los investigadores, 2019.

Ladan está de acuerdo con Wambai y sugiere que la insuficiencia podría atribuirse a una capacidad de formación inadecuada para cursos relacionados con la ciberguerra en las AFN.[127] La capacidad de formación adecuada en cursos relacionados con la ciberguerra estimularía el desarrollo de la capacidad técnica para enfrenar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Por lo tanto, la capacidad técnica es un factor clave en el enfrenamiento de las amenazas del ciberespacio, si las AFN van a mejorar la seguridad nacional

[125] *Aladenusi,T, Cyber haram: can Nigeria prepare for the next generation of terrorists?,* ***Deloitte****, <https://www2.deloitte.com/ng/en/pages/risk/articles/cyberharam-can-nigeria-prepare-for-the-next-generation-of-terrorists.html> accessed 5 Nov 19.*

[126] YB Wambai, Director, Cyber Security, Defence Space Administration, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria", at DSA Abuja on 4 Nov 19.

[127] Ladan, D Director, Information Technology, Headquarters Nigerian Air Force, Interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at HQ NAF, Abuja 0n 1 Nov 19.

en Nigeria. Los temas discutidos y analizados pusieron de manifiesto la necesidad de examinar los alcances de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

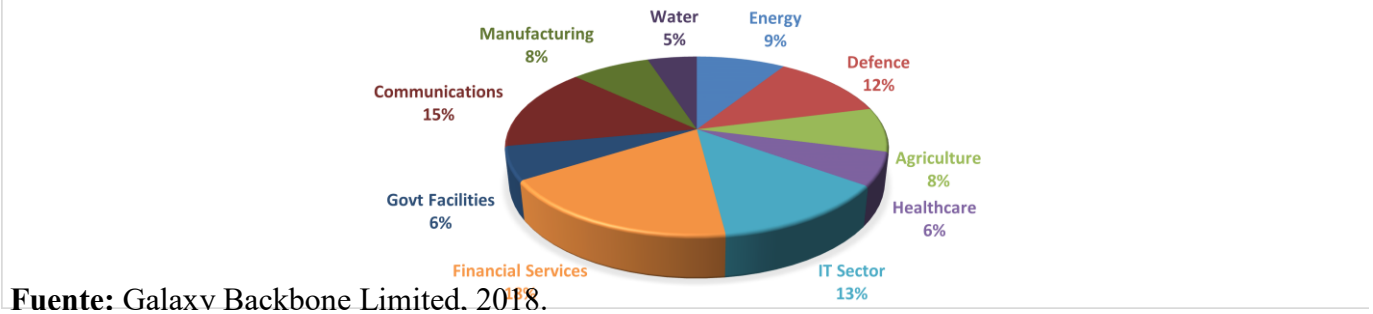
ALCANCES DE LAS CAPACIDADES DE LAS AFN PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO EN LA SEGURIDAD NACIONAL EN NIGERIA

Los alcances de las capacidades para enfrentar las amenazas del ciberespacio en la seguridad nacional de Nigeria incluyen: la Infraestructura Nacional Crítica (CNI, por sus siglas en inglés), las operaciones militares, el comercio electrónico y el contraterrorismo (CT). Estos alcances se discuten posteriormente.

Infraestructura Nacional Crítica

La CNI encapsula activos, sistemas e instalaciones cuya destrucción o incapacidad causaría un impacto debilitante en el bienestar socioeconómico y la seguridad nacional de una nación.[128] La protección efectiva de la CNI es, por lo tanto, parte integral de la seguridad nacional. En Nigeria, la Sección 6.6.4 de la NCSPS 2014 identificó 15 sectores de CNI. Estos sectores, que incluyen energía y servicios financieros, entre otros, se ejecutan utilizando la Infraestructura Nacional de Información Crítica (CNII, por sus siglas en inglés). Para atender los desarrollos futuros en la CNI, la Sección 3 (1) de la Ley de Ciberdelitos, 2015 faculta al Presidente para designar otros activos como CNII. Por ejemplo, Ajijola argumenta que el sistema de registro de votantes podría ser designado como CNII para priorizar la protección del sistema electoral a fin de mejorar la seguridad nacional.[129] La figura 1.9 indica los eventos contra la CNII en Nigeria capturados por Galaxy Backbone a diciembre de 2018.

Figura 1.9: Gráfico que muestra los eventos contra la Infraestructura Nacional de Información Crítica



Fuente: Galaxy Backbone Limited, 2018.

[128] Amoroso **Cyber Attack: Protecting National Infrastructure**, (Maryland: Elsevier Inc, 2011), p.22.

[129] AH Ajijola, Executive Chairman, Consultancy Support Services Limited, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at Abuja on 7 Nov 19.

La Figura 1.9 indica que de aproximadamente 20.000 eventos sobre CNII, el servicio financiero y el sector de TI tuvieron el más alto con 18 y 13 por ciento respectivamente, mientras que el sector del agua fue menor con 5 por ciento. Los firewalls o barreras de protección de Galaxy pudieron defenderse contra aproximadamente el 93 por ciento de estos ataques y aproximadamente el 7 por ciento llegó a los objetivos finales.[130] Estas CNII fueron evaluadas como vulnerables en el Índice de Impacto Global de Amenazas 2017, que calificó a Nigeria en segundo lugar en África y entre los 10 principales a nivel mundial en términos de exposición al ciberriesgo.[131] Según Wariowei, debido a este nivel de vulnerabilidad, alrededor de 2.175 sitios web nigerianos fueron pirateados en 2016, de los cuales 585 eran propiedad del gobierno, incluidas las CNI, lo que convierte a Nigeria en el decimoséptimo país más atacado del mundo.[132] Estos ciberataques contra las CNI muestran la necesidad de contar con capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de proteger la CNI y mejorar la seguridad nacional en Nigeria. Según Begho, a través del desarrollo de capacidades para enfrentar las amenazas del ciberespacio, como las capacidades de programación autóctona contra la piratería, las AFN podrían proteger mejor la CNI.[133] Por lo tanto, las capacidades de las AFN para enfrentar las amenazas del ciberespacio tienen alcances positivos significativos para la protección de la CNI, a fin de lograr una mayor seguridad nacional en Nigeria.

Operaciones Militares

El ciberespacio ha revolucionado las operaciones militares de muchas maneras, como la mejora de la capacidad de ISR (Inteligencia, vigilancia y reconocimiento) que permite una toma de decisiones precisa y oportuna.[134] También ha mejorado las comunicaciones militares y la gestión logística.[135] La creciente dependencia de las operaciones militares en el ciberespacio genera más vulnerabilidades a los ciberataques y destaca la necesidad de proteger los sistemas militares. Por ejemplo, las AFN tenían un rango de más de 100 tipos de armas y plataformas que estaban

[130] Uneanya ,M Manager, Network Security, Galaxy Backbone Limited, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria, at Abuja on 5 Nov 19.

[131] "Check Point's Latest Cyber-Attack Index Includes Five Countries in Africa", **Africa.com**, <https://www.africa.com/five-worlds-highest-risk-countries-africa-according-check-points-latest-threat-index/> accessed 6 Nov 19.

[132] DS Wariowei, Head Cyber Security, National Information Technology Development Agency, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.

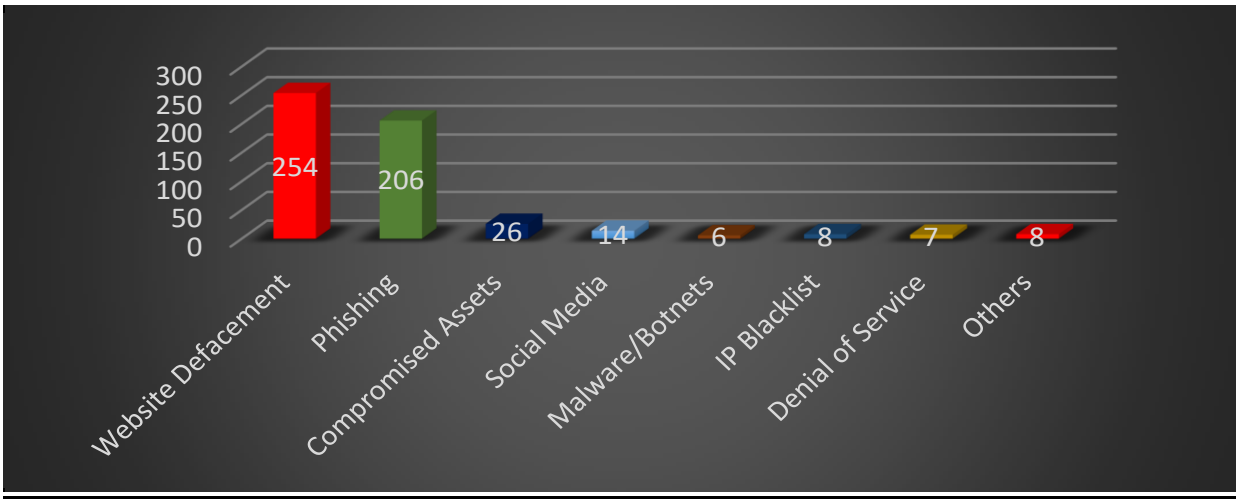
[133] N Behgo, Chief Executive Officer, Futures Software Resources Ltd, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.

[134] Alberts DS and Papp, DS, **Information age anthology: The information age military**, (New York: CCCR, 2001), pp: 199-213..

[135] Alberts DS and Papp, DS, **Information age anthology: The information age military**, (New York: CCCR, 2001), pp: 199-213.

integrados con direcciones IP y, por lo tanto, eran vulnerables a los ciberataques.[136] Los ciberataques pueden impedir el funcionamiento de estas plataformas, de ahí la necesidad de contar con buenas ciberdefensas para protegerlas. Los ataques a las redes de las AFN capturados por el ngCERT desde 2015-2018 se muestran en la Figura 2.0.

Figura 2.0: Gráfico que muestra los tipos de ciberataques contra las fuerzas armadas de Nigeria



Fuente: Oficina del Asesor de Seguridad Nacional del ngCERT, 2018.

La Figura 2.0 indica que de 529 ataques detectados por el ngCERT, 254 fueron desfiguraciones de la web, mientras que 206 fueron ataques de phishing. También hubo 6 ataques de botnet, así como 7 ataques de denegación de servicio, entre otros. Estos ataques respaldan la noción de Ladan de que los adversarios podrían usar ciberataques para explotar las plataformas y redes de las AFN para obtener una ventaja operativa y, por lo tanto, subrayan la urgencia de que las AFN necesiten incrementar sus capacidades para enfrentar las amenazas del ciberespacio a fin de salvaguardarlos.[137] Las capacidades de las AFN para afrontar las amenazas del ciberespacio, por lo tanto, tienen alcances positivos significativos para salvaguardar las operaciones militares, a fin de mejorar la seguridad nacional en Nigeria.

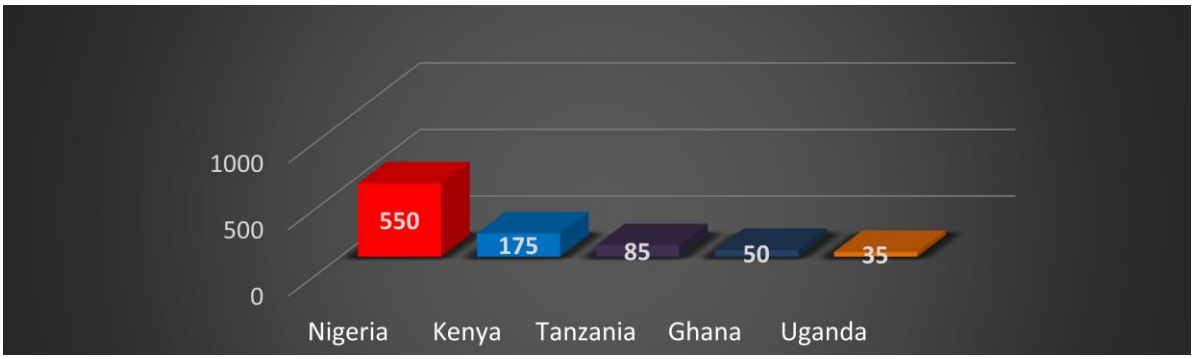
[136] Lot, EC, Former Head of NAWANI, Headquarters Nigerian Army, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 7 Nov 19

[137] Ladan, D Director, Information Technology, Headquarters Nigerian Air Force, Interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at HQ NAF, Abuja 0n 1 Nov 19.

Comercio Electrónico

El comercio electrónico connota una amplia gama de actividades en línea que cubren la transferencia de fondos o datos para la compra de bienes o servicios realizados a través de redes mediadas por computadora.[138] Una consideración importante para el comercio electrónico es la capacidad de proteger todas las transacciones electrónicas de los ciberataques. Según Pantami, Nigeria perdió US$ 450 millones en ciberataques en 2016 y US$ 550 millones en 2017, con más de 3.500 ciberataques en 2017, de los cuales más del 75 por ciento tuvieron éxito.[139] En la Figura 2.1 se muestra un gráfico que muestra las pérdidas por incidentes de cibercrimen en algunos países africanos en 2017.

Figura 2.1: Gráfico que muestra las pérdidas por ciberdelitos en algunos países africanos en 2017



Fuente: Banco Mundial, 2018.

La Figura 2.1 muestra que se perdieron más de US$ 2 mil millones en 2017 en África, Nigeria tuvo la mayor cifra con US$ 550 millones, Kenia perdió US$ 175 millones y Tanzania US$ 85 millones. Ghana y Uganda perdieron US$ 50 millones y US$ 35 millones respectivamente. Esto indica que Nigeria fue más vulnerable a las pérdidas en el comercio electrónico debido a los ciberataques, lo que podría afectar negativamente la seguridad nacional. Fakandu postula que aunque el papel principal de las capacidades de las AFN para enfrentar las amenazas del ciberespacio era proteger sus redes y plataformas, también era proteger y responder a los ciberataques de consecuencias significativas en otros sectores, incluido el comercio

[138] Chander, H, **Cyber laws and IT protection**, (New Delhi: PHI Learning Pvt, 2012), p.5.

[139] **Adaramola, Z, Nigeria: Cyber-attacks - '₦150 Billion depositors' monies at risk",** Daily Trust**, 12 Feb 18, < http://allafrica.com/stories/201802120464.html> accessed 5 Nov 19.**

electrónico.[140] Por lo tanto, es importante que las AFN incrementen sus capacidades para enfrentar las amenazas del ciberespacio a fin de frenar los ciberataques significativos al comercio electrónico y mejorar la seguridad nacional en Nigeria.[141] Por lo tanto, las capacidades de las AFN para enfrentar las amenazas del ciberespacio tienen alcances positivos significativos para el comercio electrónico, a fin de mejorar la seguridad nacional en Nigeria.

Contraterrorismo

Las operaciones de contraterrorismo (CT) se refieren a los esfuerzos coordinados del gobierno destinados a prevenir el terrorismo o mitigar sus efectos, con miras a salvar vidas y propiedades. Las AFN están actualmente involucradas en operaciones de CT contra el BHT en el noreste de Nigeria y el ciberespacio es clave para rastrear y monitorear a los terroristas.[142] Asegurar y explotar este dominio fue, por lo tanto, crítico para mejorar la seguridad nacional en Nigeria. La NCC calcula el número de usuarios de teléfonos GSM en el país en 173.749.601 a junio de 2019, con alrededor de 91 millones de usuarios de Internet.[143] Según Eteng, los integrantes del BHT aprovechan este dominio para reclutar, radicalizar, recaudar fondos y avanzar en sus operaciones.[144] Por lo tanto, es necesario que las AFN supervisen constantemente el dominio para controlar las actividades del BHT y mejorar así la seguridad nacional. Por ejemplo, en 2013, las AFN dirigieron el cierre de las redes GSM en los 3 estados del noreste de Nigeria de Adamawa, Borno y Yobe.[145] Esto ayudó a evitar la coordinación entre el BHT para mejorar la seguridad nacional en Nigeria. El resultado de la encuesta de opinión sobre si el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, posicionaría mejor a las AFN para realizar operaciones de CT a fin de mejorar la seguridad nacional se muestra en la Tabla 1.5 y la Figura 2.2.

---

[140] Fakandu, B, Head Cyber security. Office of the National Security Adviser, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 7 Nov 19.

[141] DS Wariowei, Head Cyber Security, National Information Technology Development Agency, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.

[142] Ladan, D Director, Information Technology, Headquarters Nigerian Air Force, Interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at HQ NAF, Abuja 0n 1 Nov 19.

[143] "Internet Subscriber Statistics**", Nigerian Communication Commission**, <https://www.ncc.gov.ng/stakeholder/statistics-reports/subscriber-data#internet-service-operator-data> accessed 5 Nov 19.

[144] Eteng, G, Director of Operations, Department of State Services, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria." at Abuja on 7 Nov 19.

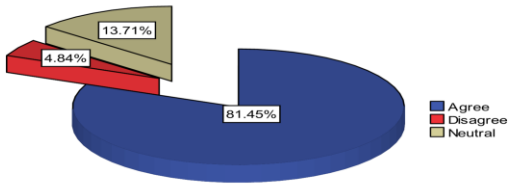
[145] Ezeugo,I Cyber Security Experts Association of Nigeria (CSEAN)", **Cyber Secure Nigeria Conference**, 2016, <https://www.cybersecurenigeria.org/wp-content/ uploads/2015/11/Cyber-terrorism-threats-to-critical-infrastructures-Iyke-Ezeugo.pdf> accessed 6 Nov 19.

Tabla 1.5: Opinión de los encuestados sobre si el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, posicionaría mejor a las AFN para realizar operaciones de CT

N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.	De Acuerdo	251	81.45
2.	Desacuerdo	15	4.84
3.	Neutral	42	13.71
4.	Total	308	100.00

Fuente: Encuesta de campo de los investigadores, 2019.

Figura 2.2: Visión de los encuestados sobre si el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, posicionaría mejor a las AFN para realizar operaciones de CT



La Figura 2.2 indica que el 81,45 por ciento de los encuestados estuvo de acuerdo en que el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, posicionaría mejor a las AFN para realizar operaciones de CT, el 4,84 por ciento no estuvo de acuerdo, mientras que el 13,71 por ciento fue neutral. Este hallazgo respalda la opinión de Ajijola de que las capacidades de las AFN para enfrentar las amenazas del ciberespacio pueden desplegarse efectivamente en las operaciones de CT para mejorar la seguridad nacional en Nigeria.[146] Por lo tanto, las capacidades de las AFN para enfrentar las amenazas del ciberespacio tienen alcances positivos significativos para las operaciones de CT, a fin de mejorar la seguridad nacional de Nigeria.

Los alcances de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional de Nigeria, resaltaron la necesidad de considerar la correlación entre ciberguerra y seguridad nacional.

Correlación entre Ciberguerra y Seguridad Nacional

Los datos obtenidos de la encuesta se evaluaron para tener una distribución normal, por lo tanto, se utilizó un análisis bi-variado para determinar la correlación entre las variables; ciberguerra y seguridad nacional. Para las variables generales de ciberguerra y seguridad nacional, el coeficiente de correlación de Pearson (p) que se obtuvo del análisis es 0,701. Además, cada uno

[146] AH Ajijola, Executive Chairman, Consultancy Support Services Limited, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at Abuja on 7 Nov 19.

de los 5 problemas de la ciberguerra fueron evaluados frente a los atributos clave de la seguridad nacional mediante el análisis de correlación de Pearson y se encontró que todos tenían una relación positiva fuerte con p = 0.000 <0.05 en un nivel de significancia de 0,05 en todos los casos.

Tabla 1.6: Tratamiento de los alcances de la ciberguerra y la seguridad nacional

N°	Problemas de Ciberguerra y Seguridad Nacional	Atributos de la Seguridad Nacional	Resultado del análisis bi-variado
(a)	(b)	(c)	(d)
1.	Política de Ciberguerra	Infraestructura Nacional Crítica	Implicación Positiva Fuerte
2.	Marco Institucional	Operaciones Militares	Implicación Positiva Fuerte
3.	Colaboración Conjunta	Comercio Electrónico	Implicación Positiva Fuerte
4.	Capacidad Técnica	Contraterrorismo	Implicación Positiva Fuerte
5.	Infraestructura de Ciberguerra	Infraestructura Nacional Crítica	Implicación Positiva Fuerte

Fuente: Análisis de los investigadores, 2019.

El resultado que se muestra en la Tabla 1.6 indica una relación fuerte y directa entre la ciberguerra y la seguridad nacional. A partir de este análisis, es evidente que cualquier incremento en las capacidades de las AFN para enfrentar las amenazas del ciberespacio mejorarían la seguridad nacional en Nigeria. Esto confirma la relación directa entre las variables conceptualizadas anteriormente en el Capítulo 2. La correlación plantea la necesidad de destacar los desafíos de las capacidades de las AFN para enfrentar las amenazas del ciberespacio en la mejora de la seguridad nacional en Nigeria.

DESAFÍOS DE LAS CAPACIDADES DE LAS AFN PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO EN LA MEJORA DE LA SEGURIDAD NACIONAL EN NIGERIA

Los desafíos que enfrentan las capacidades de las AFN para enfrentar las amenazas del ciberespacio en la mejora de la seguridad nacional en Nigeria, incluyen la ausencia de una política de ciberguerra, la ausencia de un centro de coordinación de ciberguerra independiente y la falta de un marco colaborativo de ciberseguridad para las AFN. Otros son la pobre

investigación y desarrollo (I+D) en cibertecnologías y el inadecuado desarrollo de capacidad técnica en campos relacionados a la ciberguerra. Estos desafíos se discuten posteriormente.

Ausencia de una Política de Ciberguerra

La ausencia de una política de ciberguerra para las AFN ha limitado la capacidad de las AFN para coordinar la respuesta a los ciberincidentes de naturaleza significativa en Nigeria. Según Aguiyi, el 23 de enero de 2015, el sitio web del DHQ fue pirateado y manipulado durante casi 24 horas, mientras que el 28 de marzo de 2015, el sitio web de la Comisión Electoral Nacional Independiente también fue manipulado, con efectos adversos en la seguridad nacional de Nigeria.[147] Ambos incidentes no fueron contrarrestados por las AFN debido a la falta de una política de ciberguerra para proporcionar un marco para las ciberacciones ofensivas.

Según Ajijola, con el crecimiento de los usuarios de Internet en Nigeria de 23.9 millones en 2008 a 91.6 millones en 2019, Nigeria está en mayor riesgo de ciberataques y es solo cuestión de tiempo antes de que se vuelva catastrófico.[148] El autor, lamenta la insuficiencia de la NCSPS 2014 para afrontar una ciberguerra por parte de las AFN.[149] Whyte también ve la ausencia de una política de ciberguerra como la razón para no delinear la responsabilidad y no saber cuándo las AFN ofrecerán asistencia de ciberseguridad a otros sectores.[150] La opinión de los encuestados sobre si la ausencia de una política de ciberguerra para las AFN obstaculiza sus capacidades para enfrentar las amenazas del ciberespacio y afecta la seguridad nacional en Nigeria se encuentra en la Tabla 1.7 y la Figura 2.3.

[147] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

[148] AH Ajijola, Executive Chairman, Consultancy Support Services Limited, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at Abuja on 7 Nov 19.

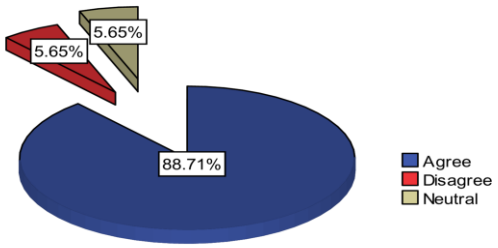
[149] AH Ajijola, Executive Chairman, Consultancy Support Services Limited, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria in Perspective", at Abuja on 7 Nov 19.

[150] Whyte, EG, Chief of Defence Space Administration, Abuja, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DSA Abuja on 1 Nov 19.

Tabla 1.7: Opinión de los encuestados sobre si la ausencia de una política de ciberguerra para las AFN obstaculiza sus capacidades para enfrentar las amenazas del ciberespacio

N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.	De Acuerdo	274	88.71
2.	Desacuerdo	17	5.65
3.	Neutral	17	5.65
4.	Total	308	100.00

Figura 2.3: Cuadro de opinión de los encuestados sobre sobre si la ausencia de una política de ciberguerra para las AFN obstaculiza sus capacidades para enfrentar las amenazas del ciberespacio



Fuente: Encuesta de campo de investigadores, 2019

La Figura 2.3 indica que el 88,71 por ciento de los encuestados estuvo de acuerdo en que la ausencia de una política de ciberguerra para las AFN obstaculiza sus capacidades para enfrentar las amenazas del ciberespacio, el 5,65 por ciento no estuvo de acuerdo, mientras que el 5,65 por ciento fue neutral. Esto indica que la ausencia de una política de ciberguerra para las AFN obstaculiza sus capacidades para enfrentar las amenazas del ciberespacio para mejorar la seguridad nacional en Nigeria. Obidake corroboró este punto de vista, quien argumentó que la falta de una política de ciberguerra para las AFN había resultado en acciones descoordinadas por parte de las Fuerzas que llevaron a la incapacidad de las AFN para explotar completamente el ciberespacio para la guerra.[151] Owolabi también opinó que la falta de una política de ciberguerra impide el desarrollo de una misión, infraestructura y recursos humanos para la participación en una ciberguerra llevada a cabo por las AFN, con efectos adversos sobre la seguridad nacional en Nigeria.[152] La falta de una política de ciberguerra para las AFN es, por lo tanto, un impedimento para sus capacidades para enfrentar las amenazas del ciberespacio, lo que afecta la seguridad nacional en Nigeria.

Ausencia de un Centro de Coordinación de Ciberguerra Independiente

La ausencia de un centro de coordinación de ciberguerra independiente ha llevado a la disipación de esfuerzos por parte de ONSA, DHQ, DIA, DSA y las 3 Fuerzas, lo que es contrario a las mejores prácticas mundiales. Por ejemplo, más de 90 países tienen actualmente capacidades de

[151] Obidake, KK, Director, Technical Services, Defence Intelligence Agency, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DIA Abuja on 8 Nov 19.

[152] AR Owolabi, Principal General Staff Officer to the Chief of Defence Staff, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19

ciberataque ofensivo, y al menos 20 ya tienen comandos de ciberguerra.[153] Estos países, algunos de los cuales se encuentran en el Apéndice 8, comprenden posibles adversarios que Nigeria necesita para tener una institución de ciberguerra fuerte para enfrentar. Por ejemplo, en 2016, China, Turquía e India generaron el 27%, el 10% y el 7% de los ciberataques globales, respectivamente, y ese año se experimentaron más de 3.500 ataques en Nigeria.[154] Aunque la Ley de Ciberdelitos de 2015 designa a la ONSA como el punto focal para la ciberseguridad, según Abdullahi, la ONSA está sobrecargada con muchos otros roles y, como agencia asesora, no tiene el mandato de llevar a cabo la guerra.[155] También está sujeta a influencia política, razón por la cual los países están designando una institución separada para llevar a cabo una ciberguerra como lo hicieron EEUU y Alemania en 2017.[156] En la Figura 2.4 se muestra un gráfico que muestra el nivel de ciberataques globales, mientras que la Figura 2.5 muestra países con comandos y su parte de ciberataques globales en 2018.

Figura 2.4: Gráfico de un mapa mundial que ilustra el nivel de ciberataques en todos los países

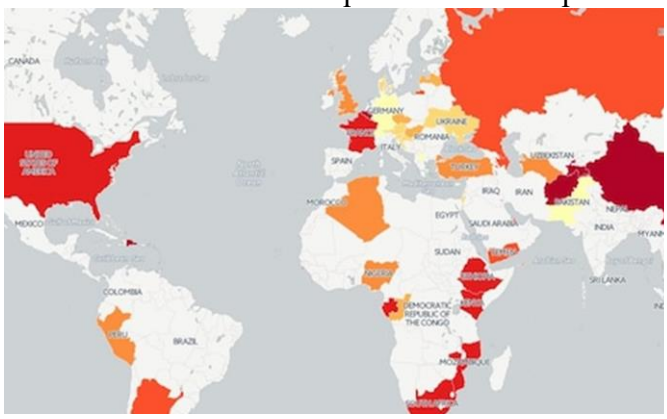
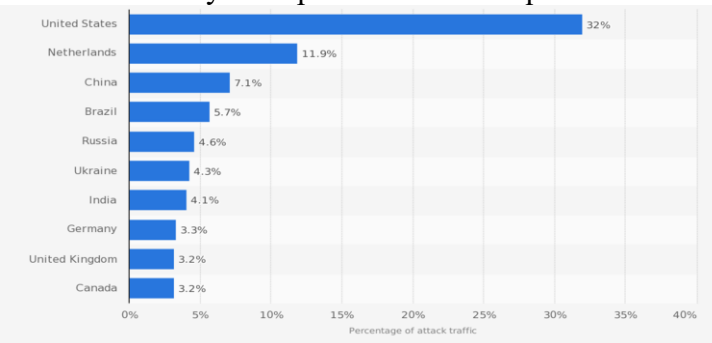


Figura 2.5: Gráfico que muestra algunos países con cibercomandos y su reporte de ciberataques en 2018



Fuente: Statista, 2019

Las Figuras 2.4 y 2.5 indican que los países que experimentan ciberataques significativos como Nigeria, tienen cibercomandos. Sin embargo, aparte de la DSA que tiene una subunidad para la ciberseguridad, no hay una institución designada exclusivamente para la ciberguerra en Nigeria. La ausencia de un cuerpo dedicado a la ciberguerra inhibe así a las AFN para confrontar ciberataques a fin de mejorar la seguridad nacional. Esta opinión fue apoyada por Eteng, quien

---

[153] **"Turkey Launched Cyber Warfare Command",** Israel Defense**, 13 Apr 14, < http://www.israeldefense.co.il/en/content/turkey-launched-cyber-warfare-command> accessed 8 Nov 19.**

[154] T Chandran, "Revealed: 10 countries From Where Most Cyber-Attacks Originate" **Gulf Business**, 17 Jul 16, < http://gulfbusiness.com/revealed-10-countries-from-where-most-cyber-attacks-originate/> accessed 8 Nov 19.

[155] Abdullahi,GS, Commander 56 Signals, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 8 Nov 19.

[156] K Beene, **Op.Cit**.

postuló que la tasa de ciberataques en el país requería que un organismo de las AFN dedicado operara en el ciberespacio.[157] La ausencia de un centro independiente de coordinación de la ciberguerra es, por lo tanto, una barrera para el incremento de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, lo que tiene un impacto negativo en la seguridad nacional en Nigeria.

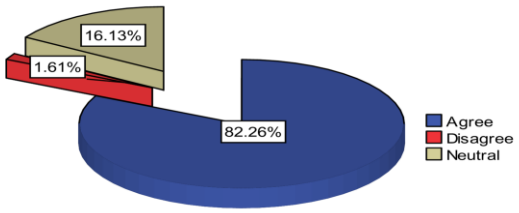
Falta de un Marco Colaborativo de Ciberseguridad para las AFN

La falta de un marco colaborativo de ciberseguridad priva a las AFN de las mejores prácticas en ciberseguridad, que podrían aprovecharse para desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional. Por ejemplo, los ciberataques de Ransomware de mayo de 2017 afectaron a más de 230.000 computadoras en aproximadamente 150 países y requirió esfuerzos concertados de los sectores público y privado, así como la colaboración internacional para mitigar sus efectos en Nigeria.[158] Según Aguiyi, la falta la colaboración en ciberseguridad entre las AFN y los asociados internacionales, que con los organismos públicos y privados es solo sobre una base ad hoc, no es lo suficientemente robusta como para impulsar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional.[159] El resultado de la encuesta de opiniones sobre si la falta de un marco de colaboración de ciberseguridad impide que las AFN puedan participar en una ciberguerra se encuentra en la Tabla 1.8 y la Figura 2.6.

Tabla 1.8: Opinión de los encuestados sobre si la falta de un marco de colaboración de ciberseguridad impide que las AFN puedan participar en una ciberguerra

N°	Respuesta	Frecuencia	Porcentaje
(a)	(b)	(c)	(d)
1.	Acuerdo	253	82.26
2.	Desacuerdo	5	1.61
3.	Neutral	50	16.13
4.	Total	308	100.00

Figura 2.6: Cuadro de opinión de los encuestados sobre si la falta de un marco de colaboración de ciberseguridad impide que las AFN puedan participar en una ciberguerra.



Fuente: Encuesta de campo de los investigadores, 2019.

[157] G Eteng, **Op.Cit**.

[158] "S.Africa's Model for Cybersecurity", **Cybersecurity Intelligence**, 18 Sep 17, < https://www.cybersecurityintelligence.com/blog/s-africas-model-for-cybesecurity2762. html> accessed 8 Nov 19.

[159] Aguiyi, NV, Deputy Director, Cyber Security, Directorate of Electronic Warfare, Defence Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at DHQ Abuja on 1 Nov 19.

La Figura 2.6 muestra que el 82,26 por ciento de los encuestados estuvo de acuerdo en que la falta de un marco de colaboración de ciberseguridad impide que las AFN puedan participar en una ciberguerra, el 1,61 por ciento no estuvo de acuerdo, mientras que el 16,13 fue neutral. Esto refuerza la importancia de la colaboración en ciberseguridad para impulsar la ciberguerra por parte de las AFN a fin de mejorar la seguridad nacional en Nigeria. Esta opinión fue respaldada por Musa, quien afirmó que Nigeria tenía alrededor de 173.749.601 usuarios de teléfonos móviles en junio de 2019 de una población de más de 200 millones, de los cuales alrededor del 52 por ciento usaba Internet.[160] Por lo tanto, es necesario colaborar con operadores y reguladores de estos medios para mejorar la seguridad nacional en Nigeria.[161] La falta de un marco colaborativo de ciberseguridad para las AFN es, por lo tanto, una barrera para la conducción de la ciberguerra por parte de las AFN, lo que tiene un impacto negativo en la seguridad nacional en Nigeria.

Pobre Investigación y Desarrollo en Cibertecnologías

La pobre I + D en el campo de las cibertecnologías en Nigeria disuade la innovación nacional, lo que lleva a una dependencia excesiva en las cibertecnologías extranjeras por parte de las AFN. Las AFN participan en una serie de proyectos de I + D que abarcan las 3 Fuerzas a fin de mejorar la seguridad nacional. Por ejemplo, entre enero de 2016 y el 30 de junio de 2019, el NA participó en 27 proyectos de I + D, mientras que la NN y la NAF llevaron a cabo 24 y 35 proyectos, respectivamente.[162] Estos proyectos de I + D estaban relacionados principalmente con la ingeniería, sin ningún esfuerzo visible en el área de cibertecnologías ofensivas como el software malicioso. Esto es consistente con la tendencia de I + D en el país. La I + D coordinada por el Ministerio Federal de Ciencia y Tecnología entre 2016 y 2018 tiene más de 80 años y carece de enfoque en cibertecnologías.[163] Esto socava la innovación y la producción locales y conduce a la situación en la que se importa alrededor del 90 por ciento de las tecnologías relacionadas con el ciberespacio utilizadas en el país.[164] Según Begho, para los ciberataques ofensivos que

[160] Musa,YEM, Coordinator, Counter Terrorism Centre, Office of the National Security Adviser, Interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria", at Abuja on 8 Nov 19

[161] Musa,YEM, Coordinator, Counter Terrorism Centre, Office of the National Security Adviser, Interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria", at Abuja on 8 Nov 19

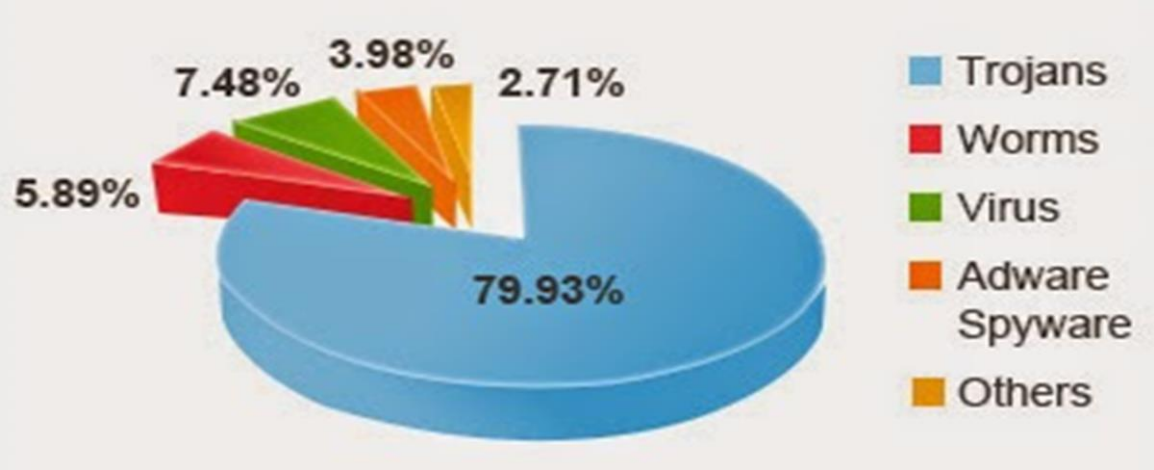
[162] Abbe, EO, Research Officer, Defence Research and Development Bureau, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria at Abuja on 8 Nov 19.

[163] "Nigeria's dependence on foreign technologies", **Business day Online**, 14 Dec 15, < http://www.businessdayonline.com/nigerias-dependence-on-foreign-technologies-2/> accessed 8 Nov 19.

[164] Ogunfuwa, I, "90% of technologies used in Nigeria are imported – DG, NOTAP", **Punch Online**, 12 Nov 17, < http://punchng.com/90-of-technologies-used-in-nigeria-are-imported-dg-notap/ >accessed 9 Nov 19.

involucran en gran medida software malicioso (malware), el enfoque correcto en la I + D autóctona podría hacer que las AFN sean autosuficientes en el desarrollo de software que podría usarse como ciberarma.[165] Algunos ejemplos de malware son virus y gusanos.[166] Estos, así como su frecuencia de uso, se muestran en el cuadro de la Figura 2.7.

Figura 2.7: Ejemplos de algunos programas maliciosos que podrían usarse para la ciberguerra.



Fuente: ViralInfection.Info, 2019.

La Figura 2.7 muestra un rango de malware que las AFN podrían estar produciendo a través de I + D en cibertecnologías para producir un grupo de ciberarmas que se utilizarán para la ciberguerra. Edet alude al hecho de que la dependencia actual de las cibertecnologías importadas en lugar de llevar a cabo I + D en cibertecnologías autóctonas dificulta el desarrollo de la ciberguerra por parte de las AFN.[167] Afirma que las cibertecnologías importadas podrían diseñarse con instalaciones dudosas que socavan la seguridad nacional en Nigeria.[168] Esta situación se ve exacerbada por la escasa capacidad de ingeniería inversa en Nigeria. La pobre I + D en cibertecnologías en Nigeria es, por lo tanto, un impedimento para la realización de la ciberguerra por parte de las AFN, con el consiguiente impacto adverso sobre la seguridad nacional en Nigeria.

[165] N Behgo, Chief Executive Officer, Futures Software Resources Ltd, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.
[166] N Behgo, Chief Executive Officer, Futures Software Resources Ltd, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at Abuja on 7 Nov 19.
[167] Edet,E, **Op.Cit**.
[168] Edet,E, **Op.Cit**.

Inadecuado Desarrollo de Capacidad Técnica en Campos Relacionados a la Ciberguerra

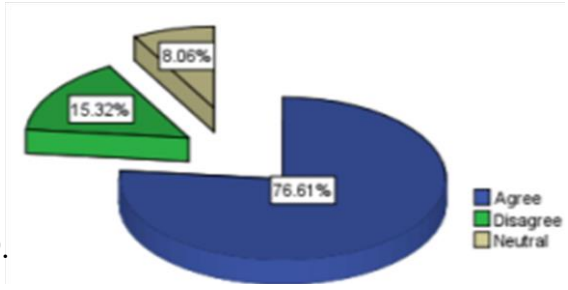
El inadecuado desarrollo de capacidad técnica en campos relacionados a la ciberguerra en Nigeria lleva a opciones limitadas para que las AFN capaciten a su personal calificado en habilidades relacionadas con la ciberguerra. Según la Comisión Nacional de Universidades, solo hay 3 universidades que ofrecen ciberseguridad como un curso de grado, lo que socava la creación de capacidad técnica en el país y para las AFN. Esto representa solo el 2 por ciento de las 160 universidades en Nigeria que comprenden 40 universidades federales, 46 estatales y 74 privadas.[169] Las universidades que ofrecen cursos de ciberseguridad incluyen la NDA, la Universidad Federal de Tecnología de Minna y la Universidad Estatal de Nassarawa. Según Aguiyi, además de la NDA que comenzó un curso de licenciatura en ciberseguridad en 2017, no hay ninguna institución visible en las AFN que ofrezca capacitación detallada sobre la ciberguerra a fin de ayudar a desarrollar la capacidad técnica de las AFN para enfrentar las amenazas del ciberespacio. La opinión de los encuestados sobre si el bajo número de instituciones que ofrecen cursos relacionados con la ciberguerra inhibe el desarrollo de las capacidades de las AFN para enfrentar las amenazas del ciberespacio se encuentra en la Tabla 1.9 y la Figura 2.8.

Tabla 1.9: Opinión de los encuestados sobre si el bajo número de instituciones que ofrecen cursos relacionados con la ciberguerra inhibe el desarrollo de las capacidades de las AFN para enfrentar las amenazas del ciberespacio.

N° (a)	Respuesta (b)	Frecuencia (c)	Porcentaje (d)
1.	Agree	236	76.61
2.	Disagree	47	15.32
3.	Neutral	25	8.06
4.	Total	308	100.00

Fuente: Encuesta de campo de los investigadores, 2019.

Figura 2.8: Cuadro de opinión de los encuestados sobre si el bajo número de instituciones que ofrecen cursos relacionados con la ciberguerra inhibe el desarrollo de las capacidades de las AFN para enfrentar las amenazas del ciberespacio.



La Figura 2.8 indica que el 76,61 por ciento de los encuestados estuvo de acuerdo en que el bajo número de instituciones educativas que ofrecen cursos relacionados con la ciberguerra inhibe el desarrollo de la capacidades de las AFN para enfrentar las amenazas del ciberespacio, el 15,32

[169] National Universities Commission <http://nuc.edu.ng/contact-us/> accessed 10 Nov 19.

por ciento no estuvo de acuerdo, mientras que el 8,06 por ciento fue neutral. Esto indica que la escasez de instituciones educativas que ofrecen cursos relacionados con la ciberguerra en Nigeria es perjudicial para los esfuerzos por desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Esta opinión fue respaldada por Ladan, quien afirmó que las instituciones inadecuadas para los cursos relacionados con la ciberguerra son en gran parte responsables del bajo nivel de profesionales especializados en la ciberguerra en las AFN. [170]Por lo tanto, la capacitación técnica inadecuada para los cursos relacionados con la ciberguerra en Nigeria ha inhibido las capacidades de las AFN para enfrentar las amenazas del ciberespacio, con el consiguiente impacto adverso sobre la seguridad nacional en Nigeria. Habiendo discutido los desafíos, es esencial evaluar la ODT ante las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

Evaluación de la Teoría Ofensiva-Defensiva en las Capacidades de las Fuerzas Armadas de Nigeria para Enfrentar las Amenazas del Ciberespacio

La ODT afirma que la tecnología que prevalece en un momento dado es un factor crítico en el conflicto internacional, ya que los países inician ataques cuando creen que las tecnologías favorecen más el ataque que la defensa.[171] Esta teoría depende de si las armas ofensivas tienen ventajas sobre las armas defensivas y si las armas ofensivas se pueden distinguir de las armas defensivas. El Gobierno Federal de Nigeria promulgó la NCSPS 2014, que es en gran medida un marco defensivo. Para las ciberacciones ofensivas, una política de ciberguerra, marco institucional, marco de colaboración, infraestructura y capacidad técnica para la ciberguerra se consideraron y discutieron anteriormente en los párrafos anteriores.

La teoría también describió los alcances de las capacidades de las AFN para enfrentar las amenazas del ciberespacio en la mejora de la seguridad nacional. Esto indica que la ODT describe acertadamente cómo se puede optimizar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional. Basado en el modelo de "Cuatro mundos" de la ODT, dado que las armas ofensivas son indistinguibles de las armas defensivas en el tercer cuadrante, las AFN necesitarían invertir mucho en ambas capacidades

[170] H Ibrahim, Director, Information Technology, Naval Headquarters, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 1 Nov 19

[171] R Jervis, “Cooperation under the Security Dilemma”, **World Politics**, Vol.30, No.2, (1978).

(ciberdefensa y ciberofensa), para permitirle defenderse adecuadamente y lanzar preventivamente ataques cuando sea necesario. La base teórica de la ODT es así válida para la aplicación práctica a las capacidades para enfrentar las amenazas del ciberespacio de las AFN a fin de mejorar la seguridad nacional en Nigeria. Tras el análisis de la ODT, existen algunas perspectivas para maximizar las capacidades de las AFN para enfrentar las amenazas del ciberespacio con el fin de mejorar la seguridad nacional de Nigeria.

PERSPECTIVAS PARA INCREMENTAR LAS CAPACIDADES DE LAS AFN PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO CON EL FIN DE MEJORAR LA SEGURIDAD NACIONAL DE NIGERIA

Las perspectivas para desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria son la Ley de Administración del Espacio de Defensa del 2016, el Programa de Inteligencia y Ciberseguridad en la NDA y la Ley de Prohibición y Prevención de Ciberdelitos del 2015. Estos se discuten posteriormente.

Ley de Administración del Espacio de Defensa del 2016

La Ley de Administración del Espacio de Defensa de 2016, que creó el Centro de Ciberoperaciones de Defensa (DCOC, por sus siglas en inglés), tenía la intención de desarrollar tecnología satelital y garantizar la seguridad de las ciberactividades de Nigeria, entre otros mandatos relacionados. La Sección 2d de la Ley, estableció el DCOC para proporcionar capacidades de ciberespacio resistentes y asequibles para las AFN.[172] El Centro podría servir como un punto focal para armonizar las ciberoperaciones de las AFN a fin de avanzar en sus capacidades para enfrentar las amenazas del ciberespacio, lo que conduciría hacia una mayor seguridad nacional en Nigeria.

Según Wambai, el objetivo principal del DCOC es defender las redes y operaciones del MOD y de las AFN, así como los ataques de importancia contra la CNII en Nigeria a fin de mejorar la seguridad nacional.[173] En cuanto a la capacidad de lanzar ciberataques ofensivos, Wambai señala que el DCOC estaba considerando una cibercapacidad ofensiva que se etiqueta tentativamente como ciberrespuesta.[174] Sin embargo, Lawal opinó que para generar especialización, el DCOC

[172] Defence space administration Act, 2016, < http://www.nassnig.org/document/ download/9421> accessed 20 Oct 19.

[173] YB Wambai, Director, Cyber Security, Defence Space Administration, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria", at DSA Abuja on 4 Nov 19.

[174] YB Wambai, Director, Cyber Security, Defence Space Administration, interviewed on "Cyber Warfare and National Security: Analysis of the

podría ser eliminado de la Ley, por lo que la Ley podría centrarse en actividades espaciales, mientras que las ciberoperaciones podrían ser independientes.[175] Sin embargo, en este momento, la Ley de Administración del Espacio de Defensa de 2016, si se implementa bien, podría ser una buena perspectiva para desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio, para una mayor seguridad nacional en Nigeria.

Programa de Inteligencia y Ciberseguridad en la Academia de Defensa Nigeriana

El Programa de Inteligencia y Ciberseguridad (ICSP, por sus siglas en inglés) en la NDA es un curso de licenciatura que se introdujo en la Facultad de Ciencias Militares y Estudios Interdisciplinarios de la NDA en 2016. Según Ogwueleka, el objetivo general del programa es producir oficiales militares capacitados con buenos conocimientos en ciberseguridad e inteligencia militar que ayudarán a enfrentar los desafíos de las operaciones de las AFN en términos de ciberguerra y lucha contra el terrorismo, entre otros.[176] Para lograr esto, el departamento cuenta actualmente con 18 profesores especializados y el contenido del curso cubre ingeniería social, penetración de redes e inteligencia artificial, entre otros.[177] El primer ICSP comenzó en la sesión académica 2017/2018 y el programa actualmente tiene 21 cadetes oficiales inscriptos.[178] Al graduarse, se espera que los oficiales contribuyan positivamente al avance de las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Por lo tanto, el ICSP en la NDA, si está bien sostenido, podría ser una buena perspectiva para proporcionar la capacidad técnica requerida para desarrollar las capacidades de las AFN para realizar operaciones ofensivas en el ciberespacio, mejorando así la seguridad nacional en Nigeria.

Ley de Prohibición y Prevención de Ciberdelitos 2015

La Ley de prohibicación y prevención de ciberdelitos de 2015, se promulgó para proporcionar un marco para la regulación del ciberespacio. Se ocupa de la prohibición, prevención, detección, respuesta, investigación y enjuiciamiento de delitos informáticos en Nigeria. La Sección 44 de la

---

Capabilities of the Armed Forces of Nigeria", at DSA Abuja on 4 Nov 19.

[175] Lawal, MS, Acting Director of Communications, Office of the National Security Adviser, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 11 Nov 19.

[176] FN Ogwueleka, Dean, Faculty of Military Science and Interdisciplinary Studies, Nigerian Defence Academy, Kaduna, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at NDA Kaduna on 1 Nov 19.

[177] FN Ogwueleka, Dean, Faculty of Military Science and Interdisciplinary Studies, Nigerian Defence Academy, Kaduna, interviewed on "Cyber Warfare and National Security: Analysis of the Capabilities of the Armed Forces of Nigeria" at NDA Kaduna on 1 Nov 19.

[178] Jallo, IM, Registrar, Nigerian Defence Academy, Kaduna, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at NDA, Kaduna on 1 Nov 19.

Ley estableció el Fondo de Ciberseguridad.[179] Un extracto de esta sección de la Ley se encuentra en el Anexo 2. El Fondo, que está domiciliado en el Banco Central de Nigeria, debe ayudar a proporcionar los fondos necesarios para las actividades relacionadas con la ciberguerra en Nigeria, ya que las asignaciones presupuestarias legales generalmente son insuficientes.[180] La cuenta está financiada por un impuesto del 0,005 por ciento en todas las transacciones de las empresas mencionadas en el Segundo Anexo de la Ley.[181] Estas empresas incluyen proveedores GSM, proveedores de servicios de Internet y bancos, entre otros.

Abdullahi confirmó que al 1 de marzo de 2018, la ONSA había abierto la cuenta del Fondo con el Banco Central.[182] El Fondo proporcionará el ímpetu necesario para alcanzar los objetivos de ciberseguridad, lo que impulsaría las capacidades de las AFN para enfrentar las amenazas del ciberespacio, mejorando así la seguridad nacional en Nigeria. Por lo tanto, la Ley de prevención y prohibición de ciberdelitos de 2015, si se implementa bien, podría ser una buena perspectiva para generar los fondos necesarios que podrían incrementar las capacidades de las AFN para enfrentar las amenazas del ciberespacio, mejorando así la seguridad nacional en Nigeria. Las perspectivas discutidas subrayan la necesidad de resaltar un resumen de los resultados de la investigación.

Resumen de los Resultados de la Investigación

La investigación se propuso llevar a cabo una evaluación de las capacidades de las AFN para enfrentar las amenazas del ciberespacio sobre la seguridad nacional. Un resumen de los resultados de la investigación son los siguientes.

a. Existe una relación directa entre ciberguerra y seguridad nacional.

b. La ciberguerra ha sido reconocida como el nuevo dominio de la guerra. Sin embargo, el estado de las capacidades de las AFN para enfrentar las amenazas del ciberespacio es baja debido a los problemas de la política de ciberguerra, el marco institucional y el marco colaborativo de ciberguerra. Otros son la infraestructura de ciberguerra y la capacidad técnica.

[179] Cyber Crimes (Prohibition, Prevention, Etc) Act, 2015, Office of the National Security Adviser.
[180] Cyber Crimes (Prohibition, Prevention, Etc) Act, 2015, Office of the National Security Adviser.
[181] Cyber Crimes (Prohibition, Prevention, Etc) Act, 2015, Office of the National Security Adviser.
[182] Abdullahi, MT, Director, Nigerian Computer Emergency Response Team, interviewed on Cyber warfare and national security: Analysis of the capabilities of the Armed Forces of Nigeria at Abuja on 1 Nov 19.

c. El estudio muestra que el desarrollo de las capacidades de las AFN para enfrentar las amenazas del ciberespacio, incrementaría su capacidad para proteger la CNI, las operaciones militares, el comercio electrónico y realizar operaciones de CT, a fin de lograr una mayor seguridad nacional en Nigeria.

d. Los desafíos identificados en el estudio incluyen la ausencia de una política de ciberguerra, la ausencia de un organismo coordinador de la ciberguerra, la falta de un marco de colaboración para la ciberseguridad, la pobre I + D en cibertecnologías y el desarrollo inadecuado de capacidades técnicas en campos relacionados con la ciberguerra.

e. Las perspectivas para desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio son la Ley de Administración del Espacio de Defensa de 2016, el Programa de Inteligencia y Ciberseguridad en la Academia de Defensa Nigeriana y la Ley de Prohibición y Prevención de Cibercrímenes 2015.

f. Los hallazgos anteriores le dan crédito a la ODT. Esto se debe a que el marco de la política de ciberguerra, la capacidad técnica, el marco institucional y la infraestructura de ciberguerra están dirigidos a ciberacciones ofensivas y defensivas para mejorar la seguridad nacional.

CAPITULO 4:
CONCLUSIÓN Y RECOMENDACIONES

La conclusión resume todo el estudio, proporcionando un resumen de los principales hallazgos y deducciones. Posteriormente, se presentarán las recomendaciones para el estudio y una serie de estrategias para desarrollar las capacidades de las AFN para enfrentar las amenazas del ciberespacio con el fin de mejorar la seguridad nacional de Nigeria.

CONCLUSIÓN

El ciberespacio se ha sido identificado como uno de los dominios de la guerra, además de los dominios de tierra, mar, aire o espacio exterior. Las AFN podrían explotar este dominio mediante la realización de una ciberguerra a fin de mejorar la seguridad nacional en Nigeria. Muchos países han aprovechado las ventajas de este dominio y han desarrollado sus capacidades para enfrentar las amenazas del ciberespacio a fin de ser utilizadas de forma independiente o en concierto con actividades cinéticas para mejorar su seguridad nacional. A pesar de la difusión del ciberespacio en Nigeria, la creciente dependencia de la infraestructura crítica en el ciberespacio y la creciente dependencia de las plataformas militares y las operaciones en el ciberespacio, Nigeria carece de la capacidad suficiente para proteger sus infraestructuras y operaciones de los ataques en este dominio. Más aún, las AFN, que son las responsables de defender la seguridad nacional, incluida la respuesta a los ataques al país, carece de la capacidad de defender al país contra ciberataques significativos o de lanzar ciberataques preventivos, lo que afecta la seguridad nacional en Nigeria. En consecuencia, el objetivo de esta investigación fue evaluar las capacidades de las AFN para enfrentar las amenazas del ciberespacio y sugerir formas de desarrollarla a fin de mejorar la seguridad nacional en Nigeria.

El estudio examinó la relación entre ciberguerra y seguridad nacional y estableció que existe una relación directa entre las 2 variables. Luego se utilizó una combinación de métodos cuantitativos y cualitativos para la recopilación de datos de fuentes primarias y secundarias. Se administró un cuestionario a una muestra de especialistas en TIC de las AFN que fueron seleccionados mediante muestreo aleatorio estratificado. Además, se realizaron entrevistas no estructuradas con otros expertos en el campo de las TIC, utilizando el método de muestreo intencional no probabilístico. Los problemas identificados en el estudio fueron el marco de políticas de ciberguerra, el marco institucional, la colaboración conjunta, la infraestructura de ciberguerra y

la capacidad técnica. Algunos alcances de la ciberguerra en la seguridad nacional incluyen la CNI, las operaciones militares, el comercio electrónico y la lucha contra el terrorismo.

Los hallazgos clave de la investigación se obtuvieron de los problemas y alcances de las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria. Se descubrió que la política nacional de ciberseguridad existente se centraba principalmente en la ciberdefensa, por lo que era necesario que las AFN tuvieran una política de ciberguerra que proporcionara pautas sobre el aspecto ofensivo de las ciberoperaciones. Del mismo modo, para mejorar la coordinación y la eficacia en la ciberguerra, se requirió un organismo coordinador dedicado como el Cibercomando de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio. Además, dado que la ciberseguridad conlleva un enfoque integral de la sociedad, es necesario que exista un marco de ciberseguridad para que las AFN compartan la inteligencia de los ciberataques y el conocimiento sobre las mejores prácticas en ciberseguridad. La infraestructura de la ciberguerra, así como la capacidad técnica para la ciberguerra también fueron inadecuadas en Nigeria. La infraestructura debe ser cada vez más autóctona para garantizar un suministro adecuado de ciberarmas. También debe haber suficiente acceso a la capacitación en ciberguerra en las AFN para desarrollar la capacidad técnica para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

Un análisis de los datos primarios y secundarios generados por el estudio reveló que las capacidades de las AFN para enfrentar las amenazas del ciberespacio tienen alcances positivos en la seguridad nacional en Nigeria. Podría ayudar a mejorar la protección de la CNI al colaborar con otras agencias para defender a la CNII contra ataques de consecuencias importantes a fin de conducir a una mayor seguridad nacional en Nigeria. Además, las capacidades de las AFN para enfrentar las amenazas del ciberespacio ayudarían a asegurar y mejorar las operaciones militares al proporcionar salvaguardas para todas las redes, plataformas y activos de las AFN que tienen direcciones IP y, por lo tanto, son vulnerables a los ciberataques. Del mismo modo, las capacidades de las AFN para enfrentar las amenazas del ciberespacio podrían ayudar a mejorar las salvaguardas necesarias para llevar a cabo el comercio electrónico a fin de mejorar la seguridad nacional en Nigeria. Además, dado que grupos terroristas como el BHT han intensificado sus operaciones al ciberespacio, las capacidades de las AFN para enfrentar las amenazas del ciberespacio podrían llevarse a cabo para contrarrestar a los terroristas en el

ciberespacio y también realizar operaciones ofensivas en el dominio a fin de mejorar la seguridad nacional en Nigeria.

Aplicando la ODT y extrayendo lecciones de otros países, se descubrió que las AFN tenían el potencial de desarrollar efectivamente sus capacidades para enfrentar las amenazas del ciberespacio y explotar las ventajas de la guerra que existen en el dominio. Además de estos problemas y alcances, se identificaron algunos desafíos de las capacidades de las AFN para enfrentar las amenazas del ciberespacio y la seguridad nacional en Nigeria. Los desafíos incluyen la ausencia de una política de ciberguerra, la ausencia de un organismo coordinador de la ciberguerra y la falta de un marco de colaboración de ciberguerra. Otros son una pobre I + D en cibertecnologías y una capacidad técnica inadecuada para los campos relacionados con la ciberguerra.

La ausencia de una política de ciberguerra para las AFN se atribuyó a la falta de un documento de política que proporcione pautas para la acción ofensiva en el ciberespacio. La no designación de una institución dedicada a la ciberguerra para las AFN se había aducido a la necesidad de tener un organismo en las AFN con la estatura requerida para la ciberguerra, mientras que la falta de un marco de colaboración de ciberguerra se debió a la falta de un estructura para colaborar con el sector público y privado, así como con asociados internacionales. La pobre I + D en cibertecnologías se ha atribuido a la falta de enfoque de investigación en la ciberguerra, mientras que el pobre desarrollo de capacidades para los campos relacionados con la ciberguerra se atribuyó a la escasez de capacitación relacionada con la ciberguerra en las AFN.

A pesar de los desafíos identificados, las AFN tienen perspectivas de incrementar sus capacidades para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria. Estas perspectivas incluyen la Ley de Administración del Espacio de Defensa del 2016 que dio origen al Centro de Ciberoperaciones de Defensa, que se centrara en las ciberoperaciones para las AFN. Otra perspectiva es la creación del Programa de Inteligencia y Ciberseguridad en la Academia de Defensa Nigeriana, que ayudaría a desarrollar la capacidad técnica de las AFN para enfrentar las amenazas del ciberespacio. La tercera perspectiva para contribuir al desarrollo de las capacidades de las AFN para enfrentar las amenazas del ciberespacio es la ley de prevención y prohibición de ciberdelitos de 2015, que estableció el Fondo de ciberseguridad que puede ayudar a proporcionar fondos para contribuir al desarrollo de

las capacidades de las AFN para enfrentar las amenazas del ciberespacio y, por lo tanto, mejorar la seguridad nacional en Nigeria.

RECOMENDACIONES

Se recomienda que el DHQ debería:

a. Promulgar una política de ciberguerra para la AFN.

b. Establecer un Cibercomando AFN como una institución autónoma de tres servicios.

c. Establecer un Centro de fusión de ciberseguridad en el Cibercomando de AFN.

d. Dirija a la DRDB para que comience la I + D en cibertecnologías.

e. Desarrollar una Doctrina de Capacitación en Ciberseguridad para la AFN.

ESTRATEGIAS PARA DESARROLLAR LAS CAPACIDADES DE LAS FUERZAS ARMADAS DE NIGERIA PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO CON EL FIN DE MEJORAR SU SEGURIDAD NACIONAL

Las AFN ofrecen algunas estrategias para incrementar sus capacidades para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en el país. La promulgación de una política de ciberguerra por parte del DHQ proporcionaría un marco para la conducción efectiva de la ciberguerra por parte de las AFN. El establecimiento de un Cibercomando de las AFN aseguraría que hubiera una organización central para la ciberguerra en el país. Además, el establecimiento de un centro de fusión de ciberseguridad en el Cibercomando de las AFN proporcionaría un punto focal para la colaboración en ciberseguridad. Además, la realización de I + D en cibertecnologías garantizaría que las AFN realicen suficiente investigación en cibertecnologías, como el desarrollo de malware y la ingeniería inversa. Por último, el desarrollo de la doctrina de capacitación en ciberseguridad para las AFN resultaría en una doctrina estandarizada para todos los niveles de capacitación en ciberseguridad en las AFN. Estas estrategias, si se implementan bien, mejorarían la conducción de la ciberguerra por parte de las AFN lo que conduciría a mejorar la seguridad nacional en Nigeria.

Promulgación de una Política de Ciberguerra para las Fuerzas Armadas de Nigeria

La promulgación de una política de ciberguerra para las AFN abordaría el desafío de la ausencia

de una política de ciberguerra. El objetivo de la política sería tener un marco que garantice la conducción coordinada y efectiva de la ciberguerra por parte de las AFN. La política también proporcionaría los principios rectores sobre los roles y responsabilidades de todos los elementos que participan en la ciberguerra y describiría las acciones que se tomarán durante las ciberacciones ofensivas o defensivas. También proporcionaría las normas y reglas de participación en la ciberguerra por parte de las AFN.

Al formular la política, el DHQ necesitaría consultar ampliamente con ONSA, DSA, NITDA y otros departamentos y agencias ministeriales relevantes, así como con el sector privado. Esto sería para garantizar que la política fuera integral, detallada y abordara todos los componentes que representan la ciberguerra para mejorar la seguridad nacional en Nigeria. El DHQ podría establecer un comité para redactar la política de ciberguerra y el proceso de formulación de políticas podría financiarse con la asignación presupuestaria del DHQ.

Establecimiento del Cibercomando de las Fuerzas Armadas de Nigeria

El establecimiento de un Cibercomando de las AFN abordaría el desafío de la ausencia de un centro coordinador independiente para la ciberguerra en comparación con las unidades y el ciberdepartamento de cada Fuerza. El objetivo del Cibercomando de las AFN sería tener una institución independiente y dedicada que sirviera como punto focal para la ciberguerra en el país. El Cibercomando de las AFN integraría todas las ciberoperaciones de las AFN y colaboraría con otras agencias gubernamentales y el sector privado. Tendría la capacidad de prevenir ciberataques contra la CNI de Nigeria, así como contra la infraestructura de las AFN y también realizar ciberoperaciones ofensivas. Un centro de fusión de ciberseguridad, así como un centro de capacitación, podrían estar domiciliados en el Cibercomando.

El Cibercomando de las AFN sería una institución autónoma de las 3 Fuerzas que se establecería mediante una Ley de la Asamblea Nacional como DSA, DIA y DICON. Esto le daría la estatura requerida y le permitiría atraer los fondos necesarios del Gobierno Federal de Nigeria. El DHQ podría establecer un comité para comenzar a redactar un proyecto de ley para el establecimiento y la financiación del Cibercomando de las AFN. El DHQ garantizaría que el comité colabore con ONSA, DIA, NITDA y otras agencias que tienen responsabilidades de ciberseguridad. El DHQ podría enviar un proyecto de ley sobre el establecimiento del Cibercomando de las AFN al MOD para su revisión y para su posterior aprobación a la Asamblea Nacional.

Establecimiento del Centro de Fusión de Ciberseguridad en las Fuerzas Armadas de Nigeria

El establecimiento de un centro de fusión de ciberseguridad en las AFN abordaría el desafío de la falta de un marco de colaboración de ciberseguridad. El objetivo del centro de fusión sería tener un punto focal en el que las AFN colaborarían con agencias gubernamentales, el sector privado y asociados internacionales en asuntos relacionados con la ciberseguridad. El enfoque utilizado en la ciberseguridad y, de hecho, en la ciberguerra es un enfoque que abarca a toda la sociedad y a toda la nación, que requiere que cada elemento esté vinculado a la alerta temprana, el intercambio de datos y todos los demás aspectos de colaboración. Los expertos en ciberseguridad altamente remunerados y experimentados se encuentran principalmente en el sector privado y su experiencia solo se puede obtener a través de un marco de colaboración eficaz utilizando un centro de fusión, para mejorar la seguridad nacional en Nigeria.

El DHQ podría establecer un comité para establecer un centro de fusión de ciberseguridad. El comité podría incorporar a ONSA, MOD, NIA, NITDA DSS, NP, DIA, DSA, NA, NN, NAF, otras agencias gubernamentales relevantes y actores clave en el sector privado. Específicamente, los departamentos de ciberseguridad de estas instituciones podrían participar plenamente en el comité.

Realización de Investigación y Desarrollo en Cibertecnologías

La realización de I + D en cibertecnologías abordaría el desafío de la pobre I + D en cibertecnologías. El objetivo sería asegurar que las AFN pudieran concentrar sus esfuerzos de investigación en áreas de cibertecnología que incluirían el desarrollo de software malicioso, así como el desarrollo y configuración de hardware utilizado para proteger redes, entre otros. También se centraría en realizar investigaciones en ingeniería inversa para acelerar la transferencia de tecnología y la innovación a fin de mejorar la seguridad nacional.

El DHQ y las Fuerzas ya tienen marcos para la investigación. En consecuencia, el recién creado Buró de Investigación y Desarrollo de Defensa (DRDB) podría encabezar esta iniciativa.

Desarrollo de la Doctrina de Capacitación en Ciberseguridad

El desarrollo de la doctrina de capacitación en ciberseguridad para las AFN abordaría el desafío de la creación de capacidad técnica inadecuada para campos relacionados con la ciberguerra en

Nigeria. El objetivo de la doctrina de capacitación es tener un marco de referencia estándar para todos los niveles de capacitación en ciberseguridad y ciberguerra en las AFN. Esto incluiría capacitación para usuarios y especialistas en ciberguerra desde niveles principiantes hasta expertos. El objetivo sería garantizar la estandarización en las operaciones de ciberguerra y facilitar un enfoque común de las ciberoperaciones en general. También garantizaría que las AFN pudieran desarrollar personal que pudiera defender la infraestructura militar y la CNI en Nigeria, al tiempo que desarrollaría una fuerza laboral de personal con conciencia de ciberseguridad para mejorar la seguridad nacional.

Al desarrollar la doctrina de la capacitación, el DHQ podría consultar ampliamente con el sector privado y también embarcarse en el programa inicial de instruir a los capacitadores para asegurar que haya suficiente capacidad en términos de personal técnico. El DHQ podría establecer un comité para desarrollar la doctrina de capacitación, mientras que los fondos para el desarrollo y la circulación de la doctrina, así como los programas iniciales de instrucción para capacitadores podrían incluirse en el presupuesto del DHQ.

Plan de Implementación de las Estrategias

A continuación se describe un plan de implementación de las estrategias propuestas para impulsar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria.

a. Fase 1 (0–12 meses). La fase 1 es la fase a corto plazo o preliminar. Implicaría las siguientes actividades:

(1) Articulación de un marco para un proyecto de política sobre ciberguerra por parte de las AFN que incluye amplias consultas con todas las partes interesadas.

(2) Articulación de modalidades para el establecimiento de un Cibercomando de las AFN.

(3) Inicio de consultas sobre la creación de un centro de fusión de ciberseguridad en las AFN.

(4) Establecimiento de asociaciones y comenzar el desarrollo de la capacidad de I + D en cibertecnologías.

(5) Articulación de modalidades para el desarrollo de una doctrina de capacitación en ciberseguridad para las AFN.

b. Fase 2 (13-24 meses). La fase 2 es la fase a mediano plazo. Implicaría las siguientes actividades:

(1) Comienzo de la I + D preliminaren cibertecnologías, por parte del DRDB, para el primer trimestre de 2021.

(2) Establecimiento de un comité para formular la política de ciberguerra para el primer trimestre de 2021.

(3) Notificación al MOD sobre la configuración del Comité para formular la política de ciberguerra para el primer trimestre de 2021.

(4) Establecimiento de un comité para comenzar a redactar un proyecto de ley para el establecimiento y la financiación del Cibercomando de las AFN para el segundo trimestre de 2021.

(5) Envío de un proyecto de ley sobre el establecimiento del Cibercomando de las AFN al MOD para su revisión y para su posterior aprobación a la Asamblea Nacional para el segundo trimestre de 2021.

(6) Desarrollo de la doctrina de capacitación en ciberseguridad para el segundo trimestre de 2021.

(7) Eliminación del DCOC de la DSA para formar el componente inicial del Cibercomando de las AFN para el tercer trimestre de 2021.

(8) Continuación de la I + D detallada en cibertecnologías, por parte del DRDB, para el tercer trimestre de 2021.

(9) Promulgación de la política de ciberguerra para el tercer trimestre de 2021.

(10) Comienzo de instrucción a los capacitadores en ciberseguridad, a través de un programa, para el tercer trimestre de 2021.

(11) Comienzo de las operaciones en el centro de fusión de ciberseguridad para el cuarto trimestre de 2021.

c. Fase 3 (más de 25 meses). La fase 3 es la fase de consolidación. Implicaría la implementación y el monitoreo de la política de ciberguerra para las AFN. Además, la aprobación de la Ley para establecer el Comando de ciberguerra de las AFN y el monitoreo de las actividades del Centro de Fusión de Ciberseguridad para las AFN se realizarían en esta fase. La I + D del DRDB se coordinaría en esta fase, así como la implementación de la doctrina de capacitación en ciberseguridad. El efecto global de las medidas tomadas para incrementar las capacidades de las AFN para enfrentar las amenazas del ciberespacio a fin de mejorar la seguridad nacional en Nigeria se evaluaría durante esta fase.

BIBLIOGRAFÍA

LIBROS

Alberts DS y Papp DS, Information age anthology: The information age military. Nueva York: CCCR, 2001.

Amoroso E, Cyber attack: Protecting national infrastructure. Maryland: Elsevier Inc, 2011.

Brenner SW, Cyber threats and the decline of the nation-state, Nueva York: Routledge, 2014.

Carr J, Inside cyber warfare: Mapping the cyber underworld. Cambridge, O'Reilly, 2011.

Chander H, Cyber laws and IT protection. Nueva Delhi: PHI Learning Pvt, 2012.

Cornick M, Health informatics: Transforming healthcare with technology. Sidney: Cengage Learning, 2006.

Dyke VV, Security and sovereignty in international politics. Nueva York: Appleton-Century-Crofts, 1966.

Green JA, Cyber warfare: A multidisciplinary analysis. Nueva York: Routledge, 2015.

Howard PN and Hussain MM, Democracy's fourth wave?: Digital media and the Arab spring. Nueva York: Oxford Press, 2013.

Huntington SP, US defence strategy: The strategic innovation of the Reagan years", in Joseph Kruzel (ed.), American defence annual, 1987–1988. Massachusetts: Lexington Books, 1987.

Kizza JM, Guide to computer network security. Nueva York: Springer Science & Business Media, 2013.

Mullan D, Scamming the scammers. Dublin: Paper books, 2014.

Norris P, Digital divide: Civic engagement, information poverty, and the internet worldwide. Boston: Cambridge University Press, 2001.

Reardon RJ, Containing Iran: Strategies for addressing the Iranian nuclear challenge. Santa Monica: Rand Corporation, 2012.

Robertazzi TG, Introduction to computer networking. Stony Brook: Spinger International Publishing, 2017.

Romm JJ, Defining national security: The non-military aspects. Nueva York: Council on Foreign Relations Press, 1993.

Schmitt et al. MN, Tallinn manual on the international law applicable to cyber warfare. Nueva York: Cambridge University Press, 2013.

Singer PW and Friedman A, Cybersecurity: What everyone needs to know. Nueva York, Oxford University Press, 2014.

Taddeo M and Glorioso L, Ethics and policies for cyber operations. Italia: Springer, 2017.

Valeriano B and Maness RC, Cyber war versus cyber realities: Cyber conflict in the international system. Nueva York: Oxford University Press, 2015.

Vogt WP, Quantitative research methods for professionals. Boston: Pearson Education Inc, 2010.

Waziri FM, Advance fee fraud, National security and the law. Ibadan: Bookbuilders, 2005.

Zetter K, Countdown to zero day: Stuxnet and the launch of the world's first digital weapon. Boston: Crown Archetype, 2014.

Zittrain J, The future of the internet and how to stop it. Yale: Yale University Press, 2008.

PERIÓDICOS/REVISTAS ESPECIALIZADAS

Alexander K, Warfighting en Cyberspace, Joint Force Quarterly, Vol.3, No.46, (2007).

Bajak F, “Y2K Bug's: World impact remains unpredictable, Amerilo Journal of Information Technology, Vol.9, No.3, (2000).

Cronbach LJ, Coefficient alpha and the internal structure of tests, Psychometrika, Vol.16, No.3, (1951).

Haizler O, The United States’ Cyber warfare history: Implications on modern cyber operational structures and policymaking, cyber intelligence and security, Vol.1, No.1, (2017).

Ibrahim AM, y Azubuike AS, A review on the security challenges in northern Nigeria and its implications for business survival and sustainable development, Journal of management and corporate governance, Vol.6, No.2, (2004).

Jervis R, Cooperation under the security dilemma, World politics, Vol.30, No.2, (1978).

Kozlowski A, Comparative Analysis of Cyber-attacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal, Vol.3, (2014).

Lynn-Jones SM, Offense-Defense theory and its critics, Security Studies, Vol.4, No.4, (1995).

Omodunbi et al. BA, "Cybercrimes in Nigeria: Analysis, detection and prevention, Journal of Engineering and Technology, Vol.1, No.1, (2016).

Osho O y Onoja AD, "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis, International Journal of Cyber Criminology, Vol.9, No.1, (2015).

YS Eun y JS Abmann, "Cyberwar: Taking Stock of Security and Warfare in the Digital Age", International Studies Perspectives, Vol.17, (2016).

PUBLICACIONES OFICIALES

Oficina del Asesor de Seguridad Nacional, Ley de Ciberdelitos (Prohición, Prevención, etc), 17 de Enero de 2018.

Administración del Espacio de Defensa, Ley de Administración del Espacio de Defensa 2016, 23 de Diciembre de 2017.

Ministerio de Asuntos Económicos y Comunicación, Estrategia de Ciberseguridad de Estonia 2014, 25 de diciembre de 2017.

Unión Internacional de Telecomunicaciones, Índice Global de Seguridad Cibernética 2018.

Comisión de Comunicación de Nigeria, Estadísticas de suscriptores de Internet 2019.

Oficina del Asesor de Seguridad Nacional, Política y Estrategia Nacional de Ciberseguridad 2014, Comisión Nacional de Universidades, 2018.

Departamento de Defensa de los Estados Unidos, Ciberestrategia 2015 del Departamento de

Defensa de los Estados Unidos.

INTERNET/MEDIOS ELECTRÓNICOS

Aladenusi T, "Cyberharam': can Nigeria prepare for the next generation of terrorists?", Deloitte, <https://www2.deloitte.com/ng/en/pages/risk/articles/cyberharam-can-nigeria-prepare-for-the-next-generation-of-terrorists.html> consultado el 5 de Noviembre de 2019.

Blair D, "Estonia recruits volunteer army of 'cyber warriors", The Telegraph, 26/04/2015, <http://www.telegraph.co.uk/news/worldnews/europe/ estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html> consultado el 18 de Octubre de 2019.

Baldor LC, "U.S. to create the independent U.S. Cyber Command, split off from NSA", PBS, 17/07/2017, <https://www.pbs.org/newshour/politics/u-s-create-independent-u-s-cyber-command-split-off-nsa> consultado el 18 de Octubre de 2019.

Billo CG y Chang W, "Cyber Warfare an Analysis of the Means and Motivations of Selected Nation State", Institute For Security Technology Studies, <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf> consultado el 15 de Octubre de 2019.

Breene K, "Who are the cyberwar superpowers?", World Economic Forum, 04/05/2016, <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/> consultado el 18 de Octubre de 2019.

Brunner J, "Iran Has Built an Army of Cyber-Proxies", The Tower, 29/08/2015, < http://www.thetower.org/article/iran-has-built-an-army-of-cyber-proxies/> consultado el 2 de Octubre de 2019..

Chandran T, "Revealed: 10 countries From Where Most Cyber-Attacks Originate" Gulf Business, 17/07/2016, < http://gulfbusiness.com/revealed-10-countries-from-where-most-cyber-attacks-originate/> consultado el 8 de Noviembre de 2019..

"Check Point's Latest Cyber-Attack Index Includes Five Countries in Africa", Africa Online, <https://www.africa.com/five-worlds-highest-risk-countries-africa-according-check- points-latest-threat-index/> consultado el 6 de Noviembre de 2019.

Ezeugo I, "Cyber Security Experts Association of Nigeria (CSEAN)", Cyber Secure Nigeria

Conference, 2016, <https://www.cybersecurenigeria.org/wp-content/ uploads/2015/11/ Cyber-terrorism-threats-to-critical-infrastructures-Iyke-Ezeugo.pdf> consultado el 6 de Noviembre de 2019.

Hadjizenonos D, "Africa in the cyber war", Hi-Tech Security Solutions, 03/02/2016, < http://www.securitysa.com/53798n> consultado el 2 de Octubre de 2019.

Hsu J, "Cyber Warriors Need Not Be Soldiers", Discover, 08/03/2015, <http://blogs.discovermagazine.com/lovesick-cyborg/2015/03/08/cyber-warriors-need-not-soldiers/#.WjVKnd-nFPY> consultado el 18 de Octubre de 2019.

Holloway M, "Stuxnet Worm Attack on Iranian Nuclear Facilities" Stanford University, 16/07/2015, <http://large.stanford.edu/courses/2015/ph241/ holloway1/> consultado el 2 de Octubre de 2019.

"Internet Users Statistics for Africa", Internet World Stats, Junio/2017, <http://www.internetworldstats.com/stats1.htm> consultado el 5 de Noviembre de 2019.

"List of Common Malware Types", <http://www.viralinfections.info/ article/231846211/list-of-common-malware-types/> consultado el 20 de Octubre de 2019.

Malone PJ, "Offense-Defense Balance in Cyberspace: A Proposed Model", Institutional Archive of the Naval Postgraduate School, 2012, <https://calhoun.nps.edu/bitstream/handle/10945/27863/12Dec_Malone_Patrick.pdf?sequence=> consultado el 17 de Octubre de 2019.

Manrzikos I, "Exploring Nigeria's Vulnerability in cyber warfare", Modern Diplomacy, 22/07/2013, <https://moderndiplomacy.eu/2013/07/22/exploring-nigerias-vulnerability-in-cyber-warfare/> consultado el 20 de Octubre de 2019.

Marks J, "U.S. Cyber Command funding nearly doubled this year — On your radar: Budget's coming, State's got mail, CISA watch still on", Politico, 17/03/2015, < https://www.politico.com/tipsheets/morning-cybersecurity/2015/03/us-cyber-command-funding-nearly-doubled-this-year-on-your-radar-budgets-coming-states-got-mail-cisa-watch-still-on-212543> consultado el 19 de Octubre de 2019.

Martin G, “Feature: Cyber and electronic warfare an increasing global challenge”, Defence Web, 09/11/2017, http://www.defenceweb.co.za/index.php?option=com_ content&view=article&id=49817&catid=74&Itemid=30> consultado el 10 de Octubre de 2019.

National Security Policy for Change and Well-being of the Filipino People (2017 - 2022), National Security Council of the Republic of Philippines, <http://www.nsc. gov.ph/attachments/article/NSP/NSP-2017-2022.pdf> consultado el 15 de Octubre de 2019.

“NCC to Establish Computer Security Response Teams for Telecoms”, Nigeria Communications Week, 28/10/2016, <http://nigeriacommunicationsweek.com.ng/ncc-to-establish-computer-security-response-teams-for-telecoms/> consultado el 20 de Octubre de 2019.

“Nigeria’s dependence on foreign technologies”, Business Day Online, 14/12/2015, <http://www.businessdayonline.com/nigerias-dependence-on-foreign-technologies-2/> consultado el 20 de Octubre de 2019.

Nigeria Internet Usage and Telecommunications Report <internetworldstats.com/af/ng.htm> consultado el 19 de Octubre de 2019.

“Nigeria Cyber Security Report 2017”, Serianu, <http://www.serianu.com/ downloads/NigeriaCyberSecurityReport2017.pdf> consultado el 20 de Octubre de 2019.

Ogunfuwa I, “90% of technologies used in Nigeria are imported – DG, NOTAP”, Punch Online, 12/11/2017, <http://punchng.com/90-of-technologies-used-in-nigeria-are-imported-dg-notap/> consultado el 20 de Octubre de 2019.

“S.Africa’s Model for Cybersecurity”, Cybersecurity Intelligence, 18/09/2017, <https://www.cybersecurityintelligence.com/blog/s-africas-model-for-cybesecurity2762.html> consultado el 8 de Noviembre de 2019.

Saltzman I, “Cyber Posturing and the Offense-Defense Balance”, Contemporary Security Policy, 2013, <http://www.tandfonline.com/ doi/abs/10.1080/13523260. S2013.771031> consultado el 5 de Noviembre de 2019.

Sanger DE, “USA Cyber Attacks Target ISIS in a new Line of Attacks”, New York Times, 24/04/2016, <https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-

for-first-time.html> consultado el 20 de Octubre de 2019.

Saltzman I, "Cyber Posturing and the Offense-Defense Balance", Contemporary Security Policy, 2013, <http://www.tandfonline.com/doi/abs/10.1080/ A13523260.2013.771031> consultado el 17 de Octubre de 2019.

Tittel E and Lindros K, "Best Information Security Certifications 2018", Toms IT Pro, 12/12/2017, <http://www.tomsitpro.com/articles/information-security- certifications, 2-205-7. html> consultado el 25 de Octubre de 2019.

"Turkey Launched Cyber Warfare Command", Israel Defense, 13/04/2014, <http://www.israeldefense.co.il/en/content/turkey-launched-cyber-warfare-command> consultado el 8 de Noviembre de 2019.

Varga G, "Building Partnerships in Challenging Times: The Defence Arrangements of Tunisia" European Institute of the Mediterranean, <http://www.iemed.org/publicacions-en/historic-de-publicacions/papersiemed-euromesco/34.-building-partnerships-in-challenging-times-the-defence-arrangements-of-tunisia> consultado el 2 de Octubre de 2019.

MATERIAL SIN PUBLICAR

Alechenu AA, Cyber Threats and National Security in Nigeria: An Assessment", un proyecto de investigación presentado al Colegio de Defensa Nacional de Nigeria, junio de 2017.

Obisco M, Global Cyber Security Agenda, documento presentado en un seminario organizado por la Unión Internacional de Comunicación sobre Protección Infantil en línea, Hotel Bristol, Amman, Jordania 15 de julio de 2015.

Olu KL, "Nigerian Cyber Security Project in the Twenty First Century, documento presentado en la Conferencia AFRINET, Accra, 16-19 de septiembre de 2016.

ENTREVISTAS NO ESTRUCTURADAS

Abbe EO, Oficial de investigación, Buró de Investigación y Desarrollo de Defensa, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 8 de noviembre de 2019.

Abdullahi GS, Comandante del Batallón 56, entrevistado sobre "Ciberguerra y Seguridad

Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" el 8 de Noviembre de 2019.

Abdullahi MT, Director, Equipo nigeriano de respuesta ante emergencias informáticas, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 1 de Noviembre de 2019.

Adesewo R, Agregado, Embajada de Nigeria en Túnez, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 8 de Noviembre de 2019.

Aguiyi NV, Subdirector, Ciberseguridad, Cuartel General de Defensa, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 1 de Noviembre de 2019.

Ajayi KC, Director de Ciberseguridad, Administración Espacial de Defensa, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 4 de Noviembre de 2019.

Ajijola AH, Director Ejecutivo, Consultancy Support Services Limited, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 7 de Noviembre de 2019.

Akwaja C, Miembro del personal, Nigeria Computer Society, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 8 de Noviembre de 2019.

Behgo N, Director Ejecutivo, Futures Software Resources Ltd, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 7 de Noviembre de 2019.

Daramola A, Comandante, Grupo de Comunicaciones 105, Shasha, Lagos, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Lagos el 1 de Noviembre de 2019.

Ekeh, Director, Zinox Technologies, entrevistado sobre "Ciberguerra y Seguridad Nacional:

Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 10 de Noviembre de 2019.

Eteng G, Director de Operaciones, Departamento de Servicios del Estado, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 7 de Noviembre de 2019.

Fakandu B, Jefe de Ciberseguridad, Oficina del Asesor de Seguridad Nacional, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 7 de Noviembre de 2019.

Ibrahim H, Director, Tecnología de la Información, Cuartel General de la Armada de Nigeria, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 1 de Noviembre de 2019.

Jallo IM, Registrador, Academia de Defensa de Nigeria, Kaduna, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 1 de Noviembre de 2019.

Ladan, Director, Tecnología de la Información, Sede de la Fuerza Aérea de Nigeria, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 1 de Noviembre de 2019.

Lawal MS, Director Interino de Comunicaciones, Oficina del Asesor de Seguridad Nacional, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 11 de Noviembre de 2019.

Lot EC, Ex jefe de NAWANI, Cuartel General del Ejército Nigeriano, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 7 de Noviembre de 2019.

Musa YEM, Coordinador, Centro Contra el Terrorismo, Oficina del Asesor de Seguridad Nacional, entrevistado sobre "Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria" en Abuja el 8 de Noviembre de 2019.

Obidake KK, Director, Servicios Técnicos, Agencia de Inteligencia de Defensa, entrevistado

sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 8 de Noviembre de 2019.

Ogwueleka FN, Decano, Facultad de Ciencias Militares y Estudios Interdisciplinarios, Academia de Defensa de Nigeria, Kaduna, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 1 de Noviembre de 2019.

Owolabi AR, Oficial Principal de Estado Mayor del Jefe del Estado Mayor de Defensa, Cuartel General de Defensa, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 1 de Noviembre de 2019.

Petinrin O, Ex jefe de personal de defensa, DHQ, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 6 de Noviembre de 2019.

Saad A, Jefe, Equipo de respuesta a emergencias informáticas de Nigeria, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 4 de Noviembre de 2019.

Shittu, Ministro de Comunicaciones, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 8 de Noviembre de 2019.

Udoh TV, Ex Jefe, Agencia de Administración Espacial de Defensa, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 8 de Noviembre de 2019.

Uneanya M, Gerente, Seguridad de Red, Galaxy Backbone Limited, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 5 de Noviembre de 2019.

Wambai YB, Director, Ciberseguridad, Administración del Espacio de Defensa, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 4 de Noviembre de 2019.

Wariowei DS, Jefe de Seguridad Cibernética, Agencia Nacional de Desarrollo de Tecnología de

la Información, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 1 de Noviembre de 2019.

Whyte EG, Jefe de Administración Espacial de Defensa, Administración Espacial de Defensa, entrevistado sobre “Ciberguerra y Seguridad Nacional: Análisis de las capacidades de las Fuerzas Armadas de Nigeria” en Abuja el 1 de Noviembre de 2019.

TESIS ARE:
APÉNDICE 1

LISTADO DE PERSONAS ENTREVISTADAS

N°	Rango Militar / Título	Nombre	Designación	Observa-ciones
(a)	(b)	(c)	(d)	(e)
1.	Air Mshl	OO Petinrin	Ex jefe de personal de defensa	
2.	Maj Gen	EG Whyte	Jefe de Administración Espacial de Defensa	
3.	Maj Gen	AR Owolabi	Oficial Principal de Estado Mayor del Jefe del Estado Mayor de Defensa, Cuartel General de Defensa	
4.	AVM	B Chiobi	Director de Operaciones DHQ	
5.	AVM (rtd)	TV Udoh	Ex Jefe de la Agencia de Administración Espacial de Defensa	
6.	AVM	MA Mohammed	Jefe de Políticas y Planes, NAF	
7.	Brig Gen	GS Abdullahi	Comandante, Signals Group	
8.	Brig Gen	MT Abdullahi	Director de Comunicaciones, ONSA	
9.	Cdre	Wambai	Ex Director de Ciberseguridad, DSA	
10.	Cdre	KC Ajayi	Director de Ciberseguridad, DSA	
11.	Cdre	H Ibrahim	Director de Informática, Cuartel General de la Armada	
12.	Air Cdre	Aguiyi	Director Adjunto de Ciberseguridad, DHQ	
13.	Air Cdre	D Ladan	Director de Informática, HQ NAF	
14.	Air Cdre	Obidake	Director de Servicios Técnicos, DIA	
15.	Cdre	H Ibrahim	Director de Informática, HQ NN	
16.	Brig Gen	IM Jallo	Registrador, NDA	
17.	Brig Gen	MT Abdullahi	Director de Ciberseguridad, ONSA	
18.	Col	RI Hedima	Oficial de Personal Principal, DSA	
19.	Col	Amubikanhun	Jefe de Informática, Cuartel General de la Fuerza Aérea	
20.	Col	Makintosh	MA de CDSA, DSA	
21.	Col	B Fakandu	Jefe de Ciberseguridad, ONSA	
22.	Wg Cdr	EO Abbe	Oficial de Investigación, DRDB	
23.	Flt Lt	Ekoro	CERT, ONSA	
24.	Professor	F Ogwueleka	Responsible del Programa de Ciberseguridad, NDA	
25.	Dr	Wawere	Jefe de Ciberseguridad, NITDA	
26.	Dr	Max Martins	Jefe de Ciberseguridad, Galaxy Backbone	
27.	Mr	AH Ajijola	Fundador, Cyber Institute Ltd	
28.	Mr	E Edet	Director de Asuntos Jurídicos, NITDA	
29.	Mr	U Igboanugo	Departamento de Ciberseguridad, NITDA	
30.	Mr	Y Ahmed	Seguridad Informática, Galaxy Backbone	
31.	Mr	Abubakar Sa'ad	Gerente ngCERT, ONSA	
32.	Mrs	Nkem Behgo	CEO Futures Software Resources Ltd	
33	Mr	Eno Hanson	Director, Acct Management, Mastercard	
34	Mr	R Eteng	Director of Operation, DSS	

Fuente: Recopilación del investigador, noviembre de 2019.

CUESTIONARIO SOBRE EL PROYECTO DE CIBERGUERRA

1. Un marco de políticas de ciberguerra para las Fuerzas Armadas de Nigeria es relevante para mejorar la seguridad nacional de Nigeria.

2. La ausencia de una política de ciberguerra para las Fuerzas Armadas de Nigeria obstaculiza el incremento de las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio a fin de lograr una mejora de la seguridad nacional en Nigeria.

3. Es esencial tener un marco institucional para optimizar las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio a fin de lograr una mejora de la seguridad nacional en Nigeria.

4. La inexistencia de una institución dedicada únicamente para coordinar la ciberguerra, como un Cibercomando, obstaculiza el incremento de las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio.

5. ¿Usted cree que la capacidad humana o el conocimiento técnico de las Fuerzas Armadas de Nigeria en ciberguerra es adecuado?

6. ¿Las instituciones educativas que ofrecen cursos relacionados con la ciberguerra en Nigeria son inadecuadas?

7. ¿Usted cree que el estado de la infraestructura de tecnología de Fuerzas Armadas de Nigeria impide el empleo de una ciberguerra en Nigeria?

8. ¿Las inversiones inadecuadas en infraestructura tecnológica de ciberguerra limitan las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio?

9. ¿Es necesario que las Fuerzas Armadas de Nigeria cooperen con otras agencias, organizaciones privadas y asociados internacionales en sus esfuerzos para enfrentar las amenazas del ciberespacio?

10. ¿El nivel de cooperación entre las Fuerzas Armadas de Nigeria y el sector privado con respecto a la ciberguerra es pobre?

11. ¿Cómo calificaría la implicación de las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio en la seguridad nacional en Nigeria?

12. ¿El desarrollo de las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio mejoraría las operaciones de las Fuerzas Armadas de Nigeria?

13 ¿Las capacidades de las Fuerzas Armadas de Nigeria para enfrentar las amenazas del ciberespacio contribuirían a mejorar la seguridad nacional en Nigeria?

14. Con el incremento de sus capacidades para enfrentar las amenazas del ciberespacio, las Fuerzas Armadas de Nigeria serían más capaces de proteger la infraestructura crítica de Nigeria.

15. Con el incremento de sus capacidades para enfrentar las amenazas del ciberespacio, las Fuerzas Armadas de Nigeria serían más capaces de proteger y mejorar sus operaciones militares.

16. Con el incremento de sus capacidades para enfrentar las amenazas del ciberespacio, las Fuerzas Armadas de Nigeria serían más capaces de proteger el comercio electrónico en Nigeria.

17. Con el incremento de sus capacidades para enfrentar las amenazas del ciberespacio, las Fuerzas Armadas de Nigeria serían más capaces de conducir operaciones de contraterrorismo.

DETALLES DEL CÁLCULO DE TAMAÑO DE MUESTRA

Se calculó un tamaño de muestra apropiado para el estudio utilizando la fórmula Taro Yamane.

La fórmula para el cálculo del tamaño de la muestra con un nivel de confianza del 95% y un margen de error del 5% viene dada por:

n = N / (1 + N (e) 2)

Donde n = Tamaño de la muestra, N = Población y e= es el margen de error

Para este estudio, N = 1,930 y e = 0.05

Por lo tanto, n = 1,930 / (1 + 1,930 (0.05) 2)

= 1,930 / (1 + 1,930 (0.0025)

= 1,930 / (1 + 4.825)

= 1,930 / 5.825

= 331

Tamaño de la muestra (n) = **331**

Fuente: Análisis del investigador, noviembre de 2019.

ALGUNOS EQUIPAMIENTOS DE LA CAPACIDAD DE LAS FUERZAS ARMADAS DE NIGERIA PARA ENFRENTAR LAS AMENAZAS DEL CIBERESPACIO

N°	Equipamiento	Observaciones
(a)	(b)	(c)
1.	Servidores Blade	
2.	Routers Cisco	
3.	Routers de Puerta de Enlace Predeterminada	
4.	Interruptor de Núcleo	
5.	Cortafuegos	
6.	Dispositivos de detección de intrusiones	
7.	Dispositivos de protección de intrusiones	
8.	Programas Anti-Malware	

Fuente: recopilación de la investigación, 2019.

LISTADO DE ALGUNAS CERTIFICACIONES EN CIBERSEGURIDAD

Serial	Certificación	Observaciones
(a)	(b)	(c)
1.	Certified Ethical Hacker (CEH)	
2.	Certified Information Security Manager (CISM)	
3.	Security+	
4.	Certified Information Systems Security Professional (CISSP)	
5.	GSEC: SANS GIAC Security Essentials.	
6.	Offensive Security Certified Professional (OSCP)	
7.	SysAdmin, Networking, and Security (SANS) Institute	
8.	Certified Information Systems Auditor (CISA)	
9.	Certified in the Governance of Enterprise IT (CGEIT)	
10.	Certified in Risk and Information Systems Control (CRISC)	
11.	Computer Hacking Forensic Investigator	
12.	Licensed Penetration Tester	
13.	Certified Incident Handler	
14.	Certified Disaster Recovery Professional	
15.	GIAC Information Security Professional	
16.	GIAC Certified Incident Handler	
17.	GIAC Reverse Engineering Malware	

Fuente: New Horizon Limited, noviembre de 2019.

LISTADO DE ALGUNOS PAÍSES QUE TIENEN CIBERCOMANDOS

N°	País	Año del Establecimiento	Observaciones
(a)	(b)	(c)	(d)
1.	EEUU	2008	
2.	Alemania	2017	
3.	China	2010	
4.	Corea del Sur	2009	
5.	Corea del Norte	2010	
6.	Taiwan	2017	
7.	Iran	2010	
8.	Francia	2016	
9.	Turquía	2014	
10.	Vietnam	2018	
11.	Rusia	2013	
12.	Filipias	2012	
13.	Suecia	2011	
14.	Suiza	2005	
15.	Países Bajos	2011	
16.	Estonia	2018	
17.	Australia	2018	
18.	Arabia Saudita	2017	

Fuente: Recopilación del investigador, 19 de noviembre de 2019.

EXTRACTO DE LA SECCIÓN 44 DE LA LEY SOBRE CIBERDELITOS DE 2015 (PROHIBICIÓN, PREVENCIÓN, ETC.)

Establishment of National Cyber Security Fund.

44. (1) There is established a Fund, which shall be known as the National Cyber security Fund (in this Act referred to as "The Fund").

(2) There shall be paid and credited into the Fund established under subsection (1) of this section and domiciled in the Central Bank of Nigeria:

(a) A levy of 0.005 of all electronic transactions by the businesses specified in the second schedule to this Act.

(b) grants-in-aid and assistance from donor, bilateral and multilateral agencies;

(c) all other sums accruing to the Fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organizations: Provided that the terms and conditions attached to such gifts, endowments, bequest or contributions will not jeopardize the functions of the Agency;

(d) such monies as may be appropriated for the Fund by the National Assembly; and

(e) all other monies or assets that may, from time to time accrue to the Fund.

(3) All monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.

(4) The levy imposed under subsection 2(a) shall be remitted directly by the affected businesses or organizations into the Fund domiciled in the Central Bank within a period of 30 days.

(5) An amount not exceeding 40 percent of the Fund may be allocated for programs relating to countering violent extremism.

(6) Accounts and records of the Fund -

(a) The Office of the National Security Adviser shall keep proper records of the accounts;

(b) The account of the Fund shall be audited in accordance with guidelines provided by the Auditor General of the Federation.

Fuente: Ley sobre ciberdelitos de 2015 (prohibición, prevención, etc.)