

O tempero que faltava na educação cibernética na Nigéria: a perspectiva da segurança nacional

The missing spice in cyber education in Nigeria: national security perspective

Resumo: Desde o advento da internet, o cibercrime tornou-se uma dízima periódica na Nigéria. Muitas nações estão lutando para proteger seu espaço cibernético dos criminosos, pela segurança nacional e integração. Como resultado disso, os governos estão encaminhando esforços para proteger os seus cidadãos e a sua imagem do crime online. Alguns destes esforços incluem a educação para a cibersegurança, que implica programas de conscientização do público geral, a fim de sensibilizá-los sobre a cibercriminalidade. Diversos programas de conscientização foram realizados em universidades e outras instituições de ensino e instituições públicas e privadas. No entanto, observou-se que tais programas nunca foram conduzidos ao clero, que são agentes fundamentais e talvez uma dos temperos mais importantes que podem influenciar a vida da maioria dos nigerianos. É neste contexto que esta pesquisa busca utilizar dados quantitativos para revelar como o clero na Nigéria foi deixado de fora na propagação da consciência da cibersegurança entre o público geral. O objetivo do estudo foi analisar o papel e a influência que o clero tem em sua congregação e sugerir maneiras de usar essa influência para melhorar a conscientização sobre a cibersegurança na Nigéria, a fim de aumentar a segurança nacional no país.

Abstract: Since the advent of the internet, cybercrime has become a recurring decimal in Nigeria. Many nations are battling to protect their cyber space from criminals, for national security and integration. As a result of this, efforts are being made by governments to protect their citizens and image from online crime. Some of these efforts include cybersecurity education which entails awareness raising programmes to the general public in order to sensitize them about cybercrime. Several awareness raising programmes have been conducted to universities and other educational institutions and public and private institutions. However, it was observed that such programmes have never been conducted to the clergy who are fundamental agent, perhaps one of the most important spice that tends to create influence in the life of most Nigerians. It is against this backdrop that this research seek to utilize quantitative data to reveal how the clergy in Nigeria have been left out in the propagation of cybersecurity awareness among the general public. The objective of the study was to analyze the role and influence the clergy have on their congregation and suggest ways such influence can be utilized to improve cybersecurity awareness in Nigeria for enhanced national security in the country.

Shehu Saidu Shehu 

Nigerian Army.

Abuja, Nigeria.

saidisco@yahoo.com

Recebido: 04 de abril de 2020

Aprovado: 12 de julho de 2020

COLEÇÃO MEIRA MATTOS

ISSN on-line 2316-4891 / ISSN print 2316-4833

<http://ebrevistas.eb.mil.br/index.php/RMM/index>



1 Introdução

Um dos fenômenos tecnológicos mais significativos que afetou positivamente o modo de vida dos seres humanos ao redor do mundo é o surgimento do ciberespaço. O ciberespaço é um domínio global virtual que vem cada vez mais impactando quase todos os aspectos da vida diária. O domínio está moldando rapidamente a comunicação, a aprendizagem, bem como a colaboração entre indivíduos e organizações. Também está transformando nações, eliminando barreiras ao comércio e criando oportunidades para inovações (OMODUNBI et al., 2016). No entanto, os novos riscos e vulnerabilidades que ameaçam a economia e segurança nacionais estão por trás da crescente dependência do ciberespaço (TIIRMAA-KLAAR, 2016). Ter o conhecimento necessário sobre as ameaças existentes, o que levará ao gerenciamento dos riscos e à criação de capacidades adequadas de prevenção e recuperação, são os elementos essenciais da segurança cibernética. Hoje em dia, a segurança cibernética é crucial para o desenvolvimento econômico e a segurança nacional do país, já que os criminosos cibernéticos estão usando o ciberespaço para perpetuar atos nefastos (TIEMO; NELLY, 2016).

O termo “cibercrime” simboliza a insegurança e o risco online, sendo amplamente usado hoje para descrever os crimes ou danos que são cometidos usando tecnologias em rede (OSHO; ONOJA, 2015). Inversamente, a cibersegurança é a proteção dos sistemas e redes do ciberespaço contra danos, uso não autorizado ou exploração. É também o método utilizado para proteger a confiabilidade das redes e sistemas contra as ameaças cibernéticas fundamentais, como o ciberterrorismo e o cibercrime. Como os Estados-nação são dependentes de uma vasta gama de redes e sistemas de ciberespaço para o desenvolvimento econômico, a violação dessas redes pode ter implicações terríveis para a segurança nacional (HILTS, 2018). Além disso, considerando que a segurança nacional é a principal responsabilidade de cada governo, as nações estão desenvolvendo seus esforços de cibersegurança, a fim de proporcionar um ciberespaço seguro e resistente para o desenvolvimento econômico. Mais ainda, o aumento das capacidades cibernéticas dos criminosos para realizar crimes certamente colocou em risco a segurança nacional dos estados (HARE, 2010).

Em outubro de 2008, autoridades de inteligência dos EUA revelaram que as autoridades policiais europeias descobriram uma rede de fraude de cartões de crédito altamente sofisticada que usou uma tecnologia altamente avançada para enviar dados de contas para o Paquistão a partir de centenas de máquinas de cartões de supermercado em toda a Europa (SIOBHAN, 2018). Da mesma forma, no início de 2016, um grupo atacante chamado “Lazarus”, localizado na Coreia do Norte, roubou um total de mais de US\$100 milhões, principalmente do Bangladesh Bank através da penetração do Alliance Access software usado pela rede da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (SWIFT), que transporta transações financeiras mundiais de forma segura e padronizada. Na mesma linha, um ataque contra Maersk pelo NotPetyransomware mais tarde em 2017 custou ao gigante de transporte até US\$300 milhões (KOCH; GOLLING, 2018).

Na África, a África do Sul experimentou o maior número de ciberataques de criminosos. De acordo com Dahir (2018), a África do Sul registra um elevado número de ciberataques

anualmente, já que 67% das corporações foram alegadamente atacadas. Estima-se que estes ataques tenham custado à economia sul-africana 242 milhões de dólares, aumentando assim a taxa de desemprego no país e afetando os meios de subsistência (VERMUELEN, 2016). Estimar a perda líquida gerada pelo cibercrime é uma tarefa desafiadora. Os números oficiais publicados por organismos governamentais ou não governamentais são indicadores fracos, uma vez que apenas estão incluídos os casos que lhes foram apresentados. No entanto, o relatório mais recente indica que o custo global da cibercriminalidade é de cerca de US\$600 bilhões, incluindo os ganhos para os criminosos e os custos de recuperação e defesa para as empresas (LEWIS, 2018).

A Nigéria tem mais de 120 milhões de usuários de internet, representando 24% de todos os usuários de Internet na África (INTERNET WORLD STATS, 2019). Este uso da Internet consiste predominantemente no uso da Internet móvel em oposição ao uso de banda larga fixa por assinatura. No entanto, esta crescente dependência do uso da internet vem com uma maior exposição às ameaças e vulnerabilidades, especialmente em um país popularmente conhecido pelo “yahooyahoo”¹ (TADE; ALIYU, 2011). A pesquisa revelou que 80% desses “yahooyahoo” são jovens e às vezes estudantes de diversas instituições superiores (ARANSIOLA; ASINDEMADE, 2011). Desde agências governamentais até ao público geral já se tornaram vítimas deste grupo de pessoas.

Este grupo de criminosos continua a prosperar, apesar de vários esforços, severos e brandos, empreendidos pelo governo nigeriano para conter a terrível ameaça no país. O esforço severo refere-se ao uso de várias legislações de crimes cibernéticos que podem levar os infratores presos, enquanto o esforço brando envolve educação, treinamento e habilidades em segurança cibernética. A convite do escritório do Conselheiro de Segurança Nacional (ONSA) em outubro de 2018, o Centro Global de Segurança Cibernética (GCSCC) realizou uma revisão da maturidade da capacidade de Segurança Cibernética na Nigéria utilizando o Modelo de Maturidade da Cibersegurança (CMM)² que é composto por 5 dimensões distintas de capacidade de cibersegurança. Na terceira dimensão, o GCSCC analisa a disponibilidade do programa de sensibilização para a cibersegurança, tanto para o público como para os executivos. No entanto, observou-se que o Centro não considerou programas de sensibilização para o clero que são um tempero importante³ do tecido cultural das comunidades e, como tal, pode influenciar a tomada de decisões, ideologias e comportamentos morais e éticos das pessoas (PINTER et al., 2016).

O objetivo desta pesquisa é, portanto, revelar como o clero na Nigéria foi deixado de fora na propagação da consciência da ciber segurança para o público geral, o grupo mais atingido pela ciber criminalidade. O objetivo do estudo foi analisar o papel e a influência que os líderes religiosos têm em sua congregação e sugerir maneiras de utilizar essa influência para melhorar a conscientização sobre a segurança cibernética na Nigéria a fim de aumentar a segurança nacional no país. O estudo é significativo, uma vez que o resultado pode ajudar a melhorar as políticas e acrescentar ao corpo de conhecimento existente na cibersegurança.

1 “Yahoo Yahoo” é uma expressão usada na Nigéria referindo-se ao cibercrime.

2 Ver Modelo de Maturidade da Capacidade de Cibersegurança para as Nações (CMM), edição revista em: <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition>. Acesso em: 21 set. 2019.

3 Tempero é usado aqui para significar “um atributo que torna algo atraente, interessante ou envolvente”.

A pesquisa foi aplicada e utilizou dados empíricos que foram coletados e analisados. Foi utilizado o método de campo da coleta de dados utilizando entrevistas e questionários, analisando-os quantitativamente. Além disso, o dimensionamento da amostra do estudo foi feito utilizando a Fórmula do Tamanho da Amostra de Taro Yamane. O estudo adotou a amostragem aleatória de clusters e os dados gerados foram apresentados usando gráficos para ilustrar as relações entre as variáveis do estudo. O estudo é limitado ao clero, bem como ao limite de 6000 a 8000 palavras.

2 Revisão da literatura

2.1 Contexto

O uso da Internet e o número de assinantes têm crescido exponencialmente na Nigéria nos últimos anos. Em conformidade com a Seção 89, Subseção 3(d), da Lei de Comunicações da Nigéria de 2003 (NCA, 2003) ⁴ o relatório da Comissão Nigeriana de Comunicações (NIGERIAN COMMUNICATIONS COMMISSION, 2019) afirma que o número de assinantes ativos de telefonia móvel e internet fixa na Nigéria é de cerca de 175 milhões e mais de 120 milhões, respectivamente. O elevado número de assinantes da internet são na sua maioria jovens que procuram emprego produtivo, engajamento social e maior conectividade global. No entanto, com esta crescente prosperidade e digitalização, surgem ameaças, riscos, vulnerabilidades e cibercrimes que podem minar a segurança nacional. Os cibercrimes são essencialmente atividades criminosas em que computadores, redes ou dispositivos eletrônicos de Tecnologia da Informação são a fonte, a ferramenta, o alvo ou o local do crime. Os cibercrimes são realizados através do acesso ilegal à base de dados de outra pessoa, interceptação ilegal, interferência de dados, interferência em sistemas, uso indevido de dispositivos, falsificação e fraudes eletrônicas (BAIDEN, [s. d.]).

2.2 Cibercrime

Na Nigéria, a cibercriminalidade tornou-se uma das principais vias para roubar dinheiro e praticar espionagem comercial. Dentro do ciberespaço nigeriano, Serianu (2016) revelou que o custo do cibercrime na Nigéria é de cerca de US\$649 milhões, com 81% dos incidentes cibernéticos causados pela proliferação de notícias falsas, ransomwares e fraudes na internet, sendo o público geral a categoria mais atingida. Em agosto de 2019, as autoridades dos EUA descobriram e acusaram 80 pessoas, a maioria das quais são "yahooyahoo" nigerianos em um esquema na internet de US\$46 milhões (FARIVAR, 2019). Os golpistas teriam supostamente vitimizado indivíduos de pequenas e grandes empresas usando uma tática chamada "Business EmailCompromise (BEC)" ⁵ O FBI e a Agência Anticorrupção

4 A lei obrigou a NCC a monitorar e relatar o estado da indústria de telecomunicações nigeriana, fornecer análises estatísticas e identificar tendências da indústria em relação a serviços, tarifas, operadoras, tecnologia, assinantes, questões de concorrência, domínio, entre outros, com o objetivo de identificar áreas onde a intervenção regulatória seria necessária.

5 BEC é uma exploração em que o invasor obtém acesso a uma conta de e-mail corporativa e falsifica a identidade do proprietário para fraudar a empresa ou seus funcionários, clientes ou parceiros de dinheiro.

da Nigéria, a EFCC⁶ revelou que 167 pessoas na Nigéria e 74 nos Estados Unidos tinham sido vítimas, semanas depois de autoridades dos EUA divulgarem uma lista de suspeitos nigerianos por trás do golpe online. Tais criminosos cibernéticos presos e vários outros são geralmente processados pela EFCC de acordo com as leis existentes, para servir de dissuasão aos outros. Por isso, além da prisão e perseguição penal dos criminosos, o governo possui uma iniciativa robusta de educação cibernética focada no programa de conscientização sobre riscos e ameaças de segurança cibernética, e como enfrentá-los, para o público geral e partes interessadas do governo e o setor privado.

2.3 Educação Cibernética

Enxerga-se que a falta de conscientização sobre as melhores práticas de segurança, a baixa educação do usuário e ausência dos programas de sensibilização podem ser os principais fatores atribuídos à exposição da maioria dos nigerianos às ameaças cibernéticas. No entanto, percebeu-se a existência de muitas iniciativas de conscientização sobre segurança cibernética organizadas por algumas instituições em colaboração com a ONSA, Agência Nacional de Desenvolvimento de Tecnologia da Informação (NITDA), EFCC, Banco Central da Nigéria (CBN) e NCC, entre outros, destinadas a aumentar a conscientização dos executivos e do público geral sobre a importância da cibersegurança. Tais iniciativas incluem o Mês da Conscientização da Segurança Cibernética (NCSAM), organizado pelo Centro Internacional para o Desenvolvimento da Liderança da Nigéria (ICLDNG). A última NCSAM foi realizada em outubro de 2018. Outras iniciativas são a oferta de cursos acadêmicos especializados em segurança cibernética na Universidade Estadual de Nasarawa (CENTER FOR CYBERSPACE STUDIES, 2019), Primeira Universidade Técnica (TECH-U, [201-]), Universidade Federal de Tecnologia (SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY, c2016) e Academia Nigeriana de Defesa Kaduna (NIGERIAN DEFENSE ACADEMY, [201-]).

Também existe uma conferência anual de segurança cibernética denominada Cyber SecureNigeriaConference organizada pela Associação de Especialistas em Segurança Cibernética da Nigéria (CSEAN). A associação tem como objetivo reunir pesquisas de segurança cibernética tanto da indústria quanto da academia (CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA, 2019). Além disso, prestadores de serviços como a Associação de Provedores de Pagamentos Eletrônicos da Nigéria (E-PPAN) também participou de campanhas de conscientização pública, particularmente em torno do uso de plataformas de pagamento eletrônico. Além disso, foi observada uma aceitação da certificação profissional internacional de segurança, como a ISACA e a série da Organização Internacional de Normalização (ISO) 27000 (GCSCC, 2018). Fora dos estabelecimentos acadêmicos e oficiais, existem alguns programas comunitários relacionados com a cibersegurança para crianças. Este programa faz parte da escola de verão oferecida aos alunos do ensino primário e secundário (DIGITAL PEERS INTERNATIONAL, 2019).

Os referidos programas de sensibilização parecem ter sido abrangentes. No entanto, GCSCC, que foi convidado pela ONSA para realizar uma revisão da maturidade da capaci-

⁶ EFCC significa Comissão de Crimes Econômicos e Financeiros.

dade de segurança cibernética da Nigéria com o objetivo de compreender sua capacidade de segurança cibernética a fim de priorizar o investimento em capacidades de segurança cibernética estrategicamente, observando que há uma necessidade de maior cooperação entre a academia e a indústria na pesquisa de segurança cibernética. O Centro observou ainda que recursos adequados para facilitar a educação em segurança cibernética nas universidades precisam ser fornecidos e a adesão ao CSEAN está aberta apenas para estudantes, graduados, profissionais de TI e aqueles sem treinamento em TI mas que trabalham em instituições relacionadas. Foi observado ainda que, em vez de um mês completo, a NCSAM foi conduzida apenas por dois dias devido às restrições de outras iniciativas que ocorreram. Na sequência do diagnóstico da maturidade da educação para a cibersegurança, o GCSCC fez algumas recomendações destinadas a fornecer aconselhamento e passos a serem seguidos para o aumento da capacidade de cibersegurança existente na Nigéria. Uma leitura atenta da revisão feita pelo GCSCC revelou que não houve menção de qualquer campanha de conscientização organizada para os líderes religiosos nas mesquitas e igrejas entre a lista de todos os lugares onde a campanha de conscientização sobre segurança cibernética foi enumerada. Observou-se também que a composição dos stakeholders no diagnóstico feito pelo GSCSS não incluía o clero e nem foram citados nas recomendações do Centro.

2.4 Influência do Clero na População Nigeriana

A Nigéria é um país dividido aproximadamente pela metade entre cristãos, que vivem principalmente na parte sul do país e muçulmanos na parte norte, com uma minoria da população praticante da religião indígena da Nigéria. O escritor e romancista BCC (LETTER..., 2014) revelou que na Nigéria, um país que afirma possuir grande parte das celebridades e intelectuais mais aclamados da África, as páginas do Facebook e do Twitter com maior número de seguidores são as do clero. Ela revelou ainda que muitos líderes religiosos na Nigéria são considerados superstars e desempenham um papel positivo no país. Ela acrescentou que se os líderes das cinco maiores igrejas da Nigéria dessem algum indício de que ninguém deveria ler obras do renomado romancista Chinua Achebe, a base de fãs do autor e as vendas do livro na Nigéria instantaneamente afundariam, independentemente de quão aclamado ele é em todo o mundo. Na Nigéria, a maioria dos que pertencem a uma religião ou a outra entendem a espiritualidade como parte da religião. Sobre esta questão, Aja (2019) destacou que:

Eles tendem a definir espiritualidade de várias maneiras, incluindo acreditar ou ter fé no transcendente, ter esperança no transcendente, ter uma relação com o transcendente e ser religioso, abrir o coração para o transcendente, ir à igreja, ir à mesquita, apaziguando o transcendente, fazendo tudo o que o transcendente manda, observando os princípios religiosos. Alguns podem definir a espiritualidade usando uma combinação de duas ou mais destas definições. O transcendente aqui pode ser Deus, Jesus, Alá, ou deuses, dependendo da tradição religiosa. Os adeptos da religião islâmica, assim como os da religião tradicional, acreditam na supremacia de Deus.

A paixão pela religião penetrou profundamente em todas as facetas da vida dos nigerianos e dificilmente pode ser relegada para segundo plano. A proibição religiosa do planejamento familiar foi atribuída como principal fator que inibiu o sucesso do programa na Nigéria (LAWANI; IYOKE; EZEONU, 2015). Da mesma forma, Nwaubani (LETTER..., 2014) revelou que quando os nigerianos foram convencidos de que seus votos não contariam nas eleições gerais de 2007, a menos que fossem registrados, as pessoas ficaram na fila por horas simplesmente porque seus pastores os ordenaram a fazê-lo. O repórter da BBC acrescentou que os líderes religiosos também desempenharam papéis-chave em batalhas contra a pólio, o HIV e o enfrentamento do surto de Ebola na Nigéria, transmitindo informações relevantes e enfatizando a urgência da situação a partir de seus púlpitos. Portanto, o clero poderia se tornar o maior recurso da Nigéria na campanha de conscientização cibernética se sua imensa influência fosse aproveitada de formas mais estruturadas e focadas.

3 Metodologia

O método de coleta de dados adotado neste estudo foi o método de campo. Este método utiliza uma combinação de entrevistas e questionários. Os dados primários para o estudo foram coletados de profissionais de cibersegurança que estão alocados em agências como ONSA, NITDA, NCC, EFCC, Administração de Defesa do Espaço (DSA) e Centro de Cibersegurança do Exército Nigeriano. Outros são do clero em vários locais de culto. Uma vez que a maior parte da população de nigerianos são muçulmanos e cristãos, o clero estudado eram aqueles das mesquitas e igrejas. Foram enviados dois conjuntos de questionários. Um tinha o foco no público profissional a fim de descobrir se eles já haviam considerado o clero como parte de seu programa de conscientização. O segundo questionário foi destinado ao clero, a fim de conhecer o seu nível de consciência cibernética e se eles já tinham recebido qualquer forma de campanha de conscientização. Os Questionários cuja fiabilidade era $\alpha = 0,94$ e $0,73$ para o clero e as profissões de cibersegurança, respectivamente, em relação ao Alfa recomendado por Cronbach $\alpha = .70$ (UNIVERSITY OF CALIFORNIA, [201 -]) foi utilizado para gerar dados e os dados recolhidos foram analisados quantitativamente utilizando o Microsoft Excel. Como os entrevistados estavam na Nigéria, o pesquisador enviou os questionários através do WhatsApp para o líder de esquadrão Ngulde e o tenente de voo Akintunde que ajudaram com a distribuição, supervisão e recuperação (BASSIC- RESEARCH, 2019)⁷

Os dados secundários foram obtidos em revistas, seminários, conferências e revistas relevantes. Outros são jornais online, pesquisas não publicadas e outros materiais relevantes da internet. A fórmula do tamanho da amostra de Taro Yamane com um erro de margem de 5% e um nível de confiança de 95% foi usada para calcular o tamanho da amostra do estudo (WHAT..., [2017?]). Isto resultou em uma amostra de 98 e 65 para os profissionais do clero e da cibersegurança, respectivamente. O estudo adotou a amostragem aleatória por conglomerados, visto que o clero considerado era apenas aqueles que administravam dentro da área de residência dos serviços de segurança. Do mesmo modo, os entrevistados da

⁷ Os questionários podem ser consultados em: <https://drive.google.com/open?id=1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR>. Acesso em: 21 set. 2019.

perspectiva profissional foram considerados aqueles que profissionalmente lidavam com cibersegurança. Isto porque todas as organizações que planejam e executam as campanhas de conscientização o fazem em colaboração com as agências governamentais. Os dados gerados foram apresentados usando gráficos para ilustrar as relações entre as variáveis do estudo.

O paradigma teórico usado para analisar o uso do clero na conscientização da cibersegurança pelos profissionais é o da Teoria do Comportamento Planejado. A principal premissa desta teoria é que ela procura prever a intenção comportamental, ou quão provável uma pessoa é de realizar um determinado comportamento. O pesquisador acrescentou que uma pessoa é mais provável de realizar um comportamento específico se o comportamento for considerado importante e se acreditar que outros aprovariam o comportamento (AJZEN, 2002; BLOOMFIELD, BOMMARITO, KUHL, 2015).

4 Análise e apresentação dos dados

Este capítulo contém a apresentação e a análise os dados coletados dos respondentes. Os dados analisados foram representados em números absolutos e porcentagens. Além disso, cada pergunta de seu conjunto no questionário foi analisada através de gráfico para mostrar os detalhes das respostas. Oitenta e nove questionários foram administrados ao clero, enquanto sessenta e cinco foram enviados aos profissionais da cibersegurança. Todos os questionários foram devidamente preenchidos e devolvidos.

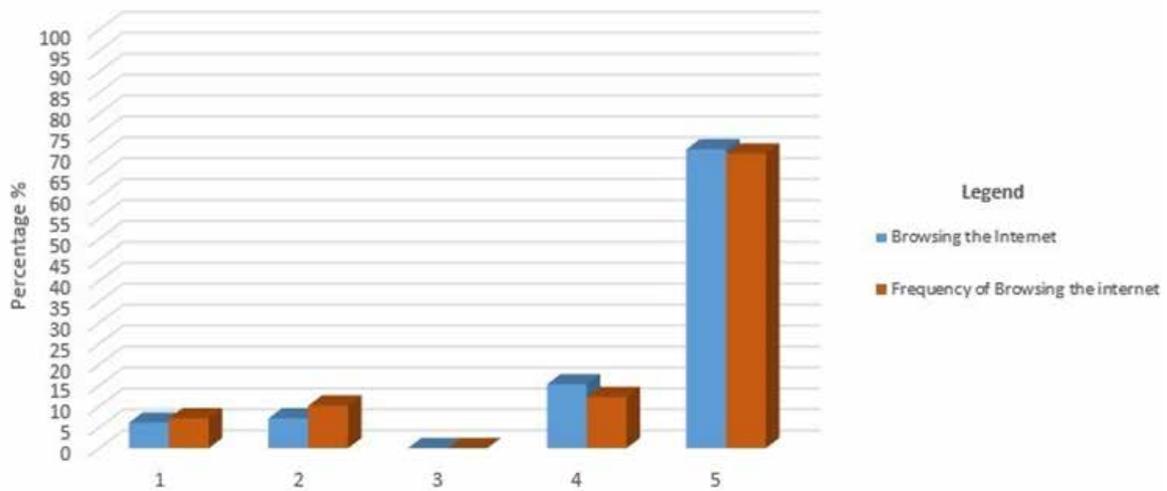
4.1 Análise dos Dados Obtidos do Clero

Os dados analisados nesta seção são os do clero. Os dados não foram analisados em termos dos que ministram na mesquita ou igreja, mas sim como representativos de seu centro religioso. O questionário possuía 16 perguntas no total e cada pergunta tinha uma classificação de 1 a 5, sendo 1 o mais fraco e 5 o mais forte.

4.1.1 Conhecimento da Internet

O pesquisador investigou se os respondentes navegam na internet e com que frequência o fazem. As respostas são como mostrado no Gráfico 1 abaixo.

Gráfico 1 – Gráfico do Conhecimento dos Respondentes sobre a Internet



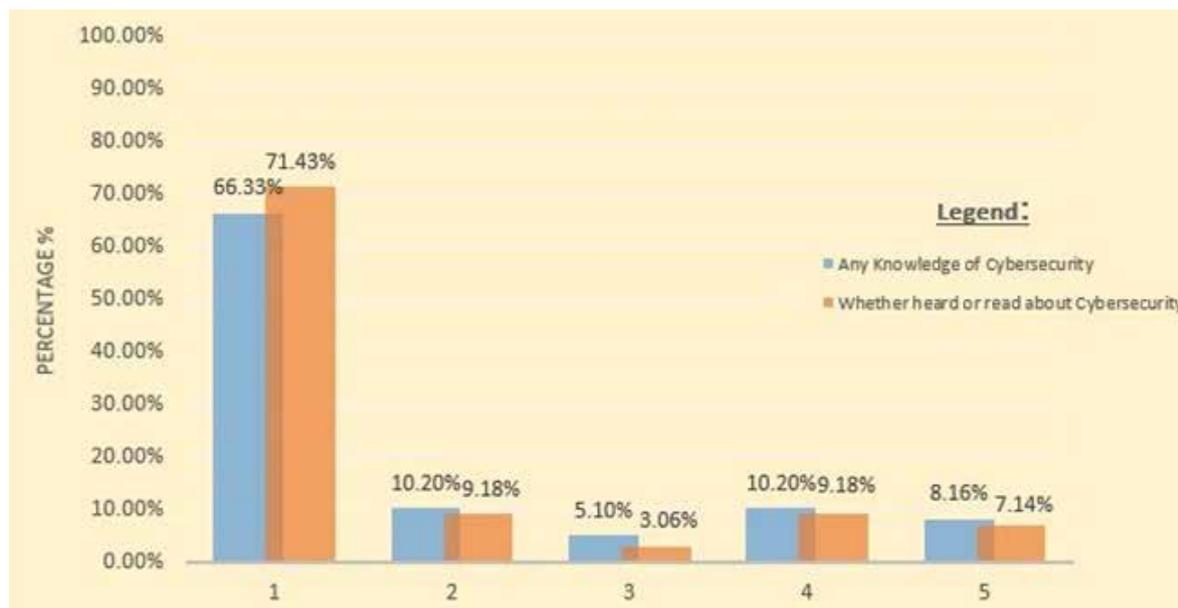
Fonte: Autor (2019).

O Gráfico 1 mostra que 71,43% dos entrevistados navegam muito bem na internet, onde 15,31% navegam bem na internet, enquanto 6,12% nunca navegam na internet. A alta porcentagem daqueles que navegam pela internet contra a baixa porcentagem daqueles que não, converge com o relatório do NCC, que afirma que existem 120 milhões de assinantes da internet em 2019 (NIGERIAN COMMUNICATIONS COMMISSION, 2019). A cifra também revelou que 70,41% dos entrevistados visitam a internet com maior frequência, contra 7,14% dos que não visitam a internet. O resultado da pesquisa sobre as duas condições confirmou a veracidade do relatório NCC.

4.1.2 Conhecimento da Cibersegurança

O pesquisador pediu para saber se os entrevistados têm algum conhecimento de segurança cibernética, já leram ou ouviram sobre ela. O resultado desse inquérito é o que se mostra no Gráfico 2.

Gráfico 2 – Gráfico sobre os Conhecimentos de Cibersegurança dos Pesquisados



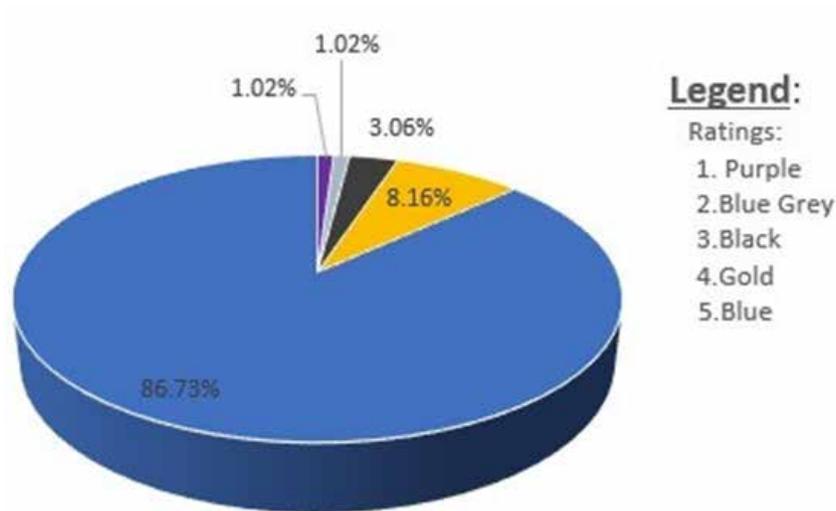
Fonte: Autor (2019).

O Gráfico 2 acima revelou que 66,33% do clero alegou não ter conhecimento sobre a cibersegurança. O relatório revelou ainda que 71,43% deles não tinham lido nem ouvido falar de cibersegurança. O número revelou ainda que 8,16% dos entrevistados afirmaram ter um conhecimento muito bom da cibersegurança, enquanto 10,20% o afirmaram ter conhecimento sobre ela. Por outro lado, 7,14% dos entrevistados indicaram ter um conhecimento muito bom da cibersegurança através da leitura ou palestras, enquanto 9,18% revelaram um bom conhecimento através dos mesmos meios. A grande diferença entre os respondentes que não têm conhecimento da cibersegurança com aqueles que tinham conhecimento dela pode indicar que aqueles que já ouviram falar sobre o tema não o fizeram necessariamente através de campanhas de conscientização cibernética organizadas no local de culto.

4.1.3 Conhecimento de Qualquer Campanha de Sensibilização para a Cibersegurança Organizada em um Local de Culto

Foi perguntado se alguma campanha de conscientização sobre segurança cibernética havia sido organizada nos locais de culto dos entrevistados e os resultados da pesquisa de campo são mostrados no Gráfico 3 abaixo:

Gráfico 3 – Gráfico do Conhecimento de Campanhas de Sensibilização para a Cibersegurança Organizada em Local de Culto



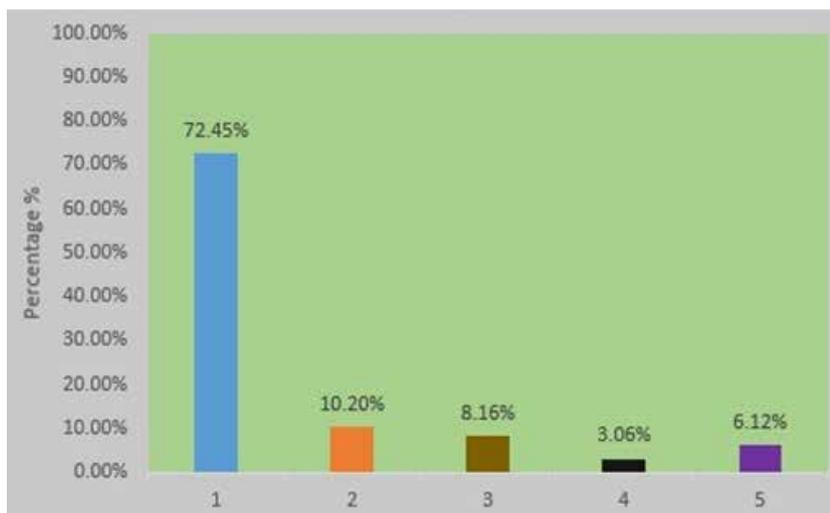
Fonte: Autor (2019).

Do Gráfico 3 acima, pode-se ver que 86,73% dos entrevistados não tinham conhecimento de nenhuma campanha de conscientização sobre segurança cibernética realizada em seu local de culto. Pode-se, portanto, deduzir que a alta porcentagem obtida aqui deu credibilidade à análise do pesquisador na Seção 4.1.2 que a pequena porcentagem dos respondentes que têm conhecimento de cibersegurança o tem por conta própria e não como resultado de uma campanha de conscientização da cibersegurança organizada.

4.1.4 Conhecimento de Cibersegurança

O pesquisador perguntou se os entrevistados estão cientes da cibercriminalidade e o resultado da pesquisa é mostrado no Gráfico 4 abaixo.

Gráfico 4 – Evolução do Conhecimento da Cibercriminalidade



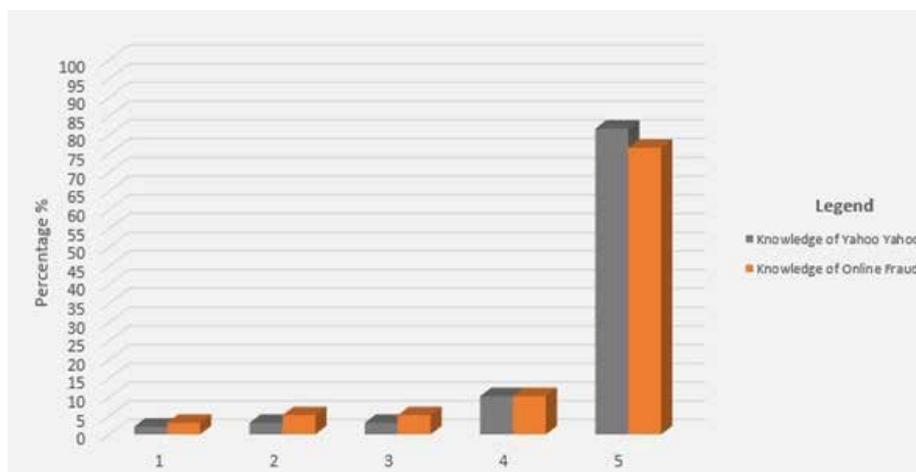
Fonte: Autor (2019).

O Gráfico 4 acima revelou que 72,45% dos inquiridos não têm conhecimento da cibercriminalidade. O resultado aqui é potencialmente preocupante se considerado no contexto do demonstrado na Seção 4.1.1 e o revelado por Business Day (AKIYODE-LAWANSON, 2019) que a Nigéria ocupa o terceiro lugar em usuários atacado por malware móvel, com 37,72%.

4.1.5 Conhecimento do Yahoo Yahoo e 419⁸

O pesquisador perguntou se os entrevistados têm conhecimento do Yahoo Yahoo e 419 na Nigéria e o resultado da pesquisa é mostrado no Gráfico 5 abaixo.

Gráfico 5 – Gráfico do Conhecimento sobre Yahoo Yahoo e 419 dos Respondentes



Fonte: Autor (2019).

⁸ O termo 7 419 é geralmente usado para descrever atividades fraudulentas. Ele se originou da Seção 419 das leis vigentes na Nigéria, que criminaliza fraudes financeiras e fraude na internet ou ciber fraude na Nigéria.

No Gráfico 5, pode-se observar que 81,63% e 76,3% dos entrevistados estão cientes do Yahoo Yahoo e 419, respectivamente. A alta porcentagem obtida aqui pode ser resultado de uma prática popular do Yahoo Yahoo de enviar mensagens fraudulentas para enganar assinantes da rede GSM. Tade e Aliyu (2011) revelaram que os criminosos, tendo conhecimento do funcionamento do sistema de promoções das telecomunicações, clonaram-no e exploraram-no para defraudar os nigerianos, enviando nos seus telefones mensagens fraudulentas relativas a uma enorme quantia de dinheiro que ganharam. Os pesquisadores mostram ainda que os criminosos, em seguida, pediam à vítima que enviassem uma certa quantidade de crédito para um determinado número antes de fazer a ligação para negociar como o prêmio seria entregue. Tais atos tornaram Yahoo Yahoo e 419 muito populares na Nigéria.

4.1.6 Conhecimento da Relação entre Cibercrime, Yahoo Yahoo e Fraude Online

O pesquisador verificou se os entrevistados estão cientes de que o cibercrime é o mesmo que Yahoo Yahoo e 419. O resultado são mostrados no Gráfico 6 abaixo.

Gráfico 6 – Gráfico do Conhecimento dos Respondentes sobre a Relação entre Cibercrime, Yahoo Yahoo e Fraude Online



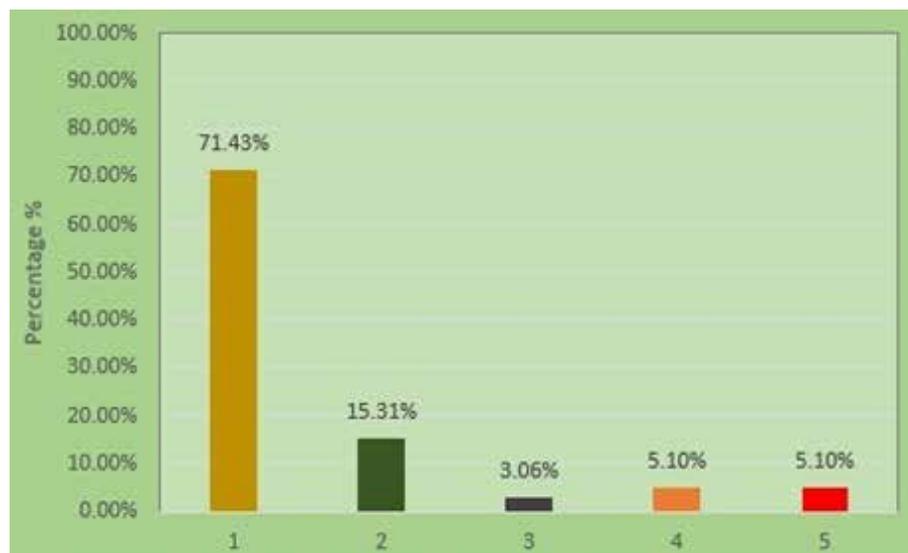
Fonte: Autor (2019).

Do Gráfico 6 acima, pode-se ver que 71,43% dos entrevistados não estão cientes de qualquer relação entre cibercrime, Yahoo Yahoo e 419. Dos resultados obtidos na Seção 4.1.4 e Seção 4.1.5, pode-se ver que os entrevistados têm amplo conhecimento do Yahoo Yahoo e do 419, mas não fazem ideia do que significa cibercrime. Portanto, o fato de que eles não estão cientes de que Yahoo Yahoo, 419 e Cibercrime significam a mesma coisa indica que eles veem Yahoo Yahoo e 419 do prisma de enganar um indivíduo e não necessariamente tendo a ver com o ciberespaço.

4.1.7 Conhecimento sobre a Ação a Ser Tomada Quando Vitimado por Crime Cibernético

O pesquisador perguntou se os entrevistados têm algum conhecimento das ações a serem tomadas quando vitimado pela cibercriminalidade. Os resultados são mostrados no Gráfico 7 abaixo.

Gráfico 7 – Gráfico do resultado sobre a ação a ser tomada quando vitimado pela cibercriminalidade



Fonte: Autor (2019).

O Gráfico 7 revelou que 69,39% dos inquiridos não têm conhecimento das medidas a tomar quando atingidos pela cibercriminalidade. O gráfico revelou ainda que apenas 12,24% estavam cientes das medidas a serem tomadas. A alta porcentagem de pessoas que não estavam cientes das ações a serem tomadas não é surpreendente devido à falta de conhecimento sobre cibersegurança por parte dos respondentes. Pode-se dizer que essa falta de conhecimento por parte dos respondentes é preocupante principalmente com a circular do CBN (CENTRAL BANK OF NIGERIA, 2019) para que todos os bancos de dinheiro de depósito informem-nos de sua política de implementação de cobrança de saques e depósitos de pessoas físicas e jurídicas em ordem para fazer cumprir a campanha do governo para uma sociedade sem dinheiro físico. A circular declarava que as taxas eram de 3% e 2% a serem cobradas de pessoas físicas por saques em dinheiro e depósitos, respectivamente, enquanto 5% e 3% se aplicavam às corporações. O fato de as cobranças entrarem em vigor em 31 de março de 2020 significa que todas as atividades financeiras no país estarão online a partir dessa data. Portanto, existe a necessidade de uma campanha agressiva de sensibilização para a cibersegurança para mitigar o risco inerente ao ciberespaço.

4.1.8 Conhecimento Sobre Ter Sido Afetado pelos Yahoo Yahoo

O pesquisador perguntou se os entrevistados já haviam sido afetados pelos Yahoo Yahoo e o resultado da pesquisa de campo é mostrado no Gráfico 8 abaixo:

Gráfico 8 – Gráfico sobre o Conhecimento de Ter Sido Afetado pelo Yahoo Yahoo



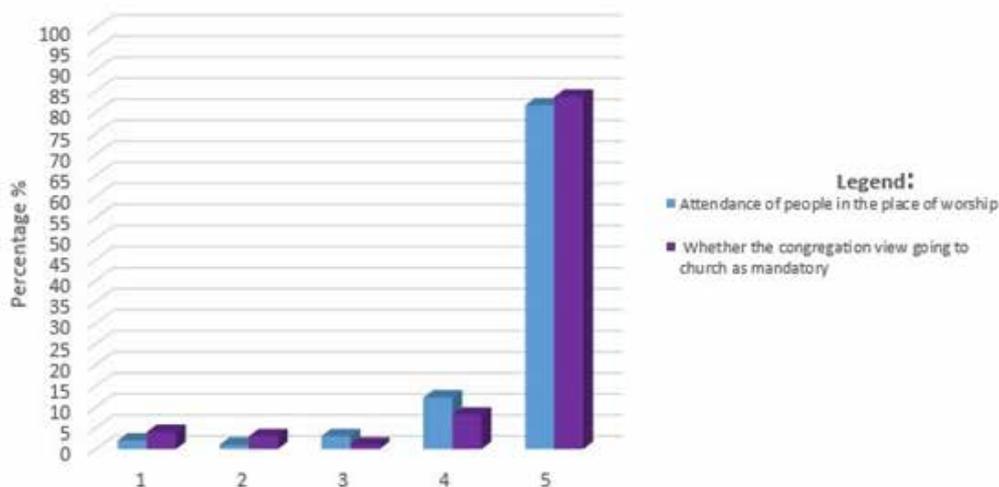
Fonte: Autor (2019).

O Gráfico 8 revelou que 61,22% dos entrevistados foram bem atingidos pelos Yahoo Yahoo, enquanto 12,24% foram moderadamente atingidos. A alta resposta observada aqui pode ser resultado do esquema GSM ou um encontro com o “viajante aflito”. O fenômeno do “viajante aflito” é um tipo de golpe na Nigéria, onde um criminoso, bem vestido e parecendo respeitável, pinta um cenário de estar preso e sem dinheiro para a tarifa de ônibus e implora por ajuda para chegar a seu destino, quando na verdade, ele é apenas um golpista que emprega táticas para enganar as pessoas por seu dinheiro.

4.1.9 Conhecimento Sobre Adoração Religiosa

O pesquisador perguntou sobre o comparecimento da congregação aos locais de culto e se eles enxergam seu comparecimento como obrigatório. As respostas são demonstradas no Gráfico 9:

Gráfico 9 – Gráficos com os Resultados sobre Adoração Religiosa



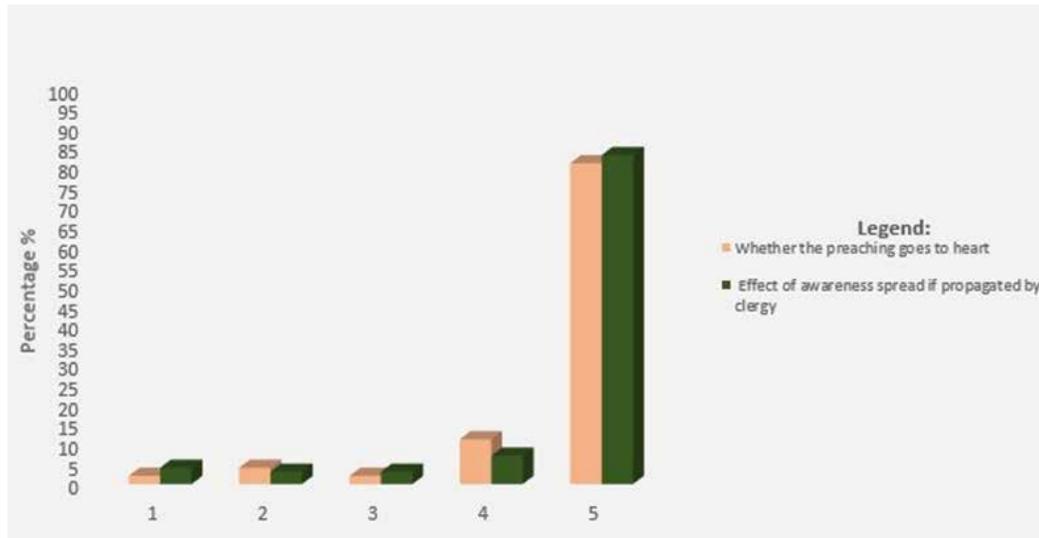
Fonte: Autor (2019).

Do Gráfico 9 acima, pode-se observar que 81,63% dos entrevistados acreditam que a população frequenta os vários cultos muito bem. Da mesma forma, 83,61% dos entrevistados acreditam que a congregação enxerga que ir ao culto é obrigatório para eles. Isto está, portanto, correlacionado com a revelação de Ajah (2019) de que a maioria das pessoas que pertencem a uma religião ou outra na Nigéria percebem espiritualidade como parte da religião. O resultado obtido também correlacionou-se com uma pesquisa da BBC 2010, que revelou que 87% dos nigerianos disseram que a religião era muito importante para suas vidas. Outro relatório da BBC de 2014, também revelou como as reuniões das mega-igrejas da Nigéria lotam os estádios de futebol.

4.1.10 Influência da Palavra do Clero na Congregação

O pesquisador questionou sobre a visão dos entrevistados sobre como suas pregações são levadas ao coração por sua congregação e o efeito daí resultante. Os resultados são mostrados no Gráfico 10 abaixo.

Gráfico 10 – Gráfico com o Resultado da Influência da Palavra do Clero na Congregação



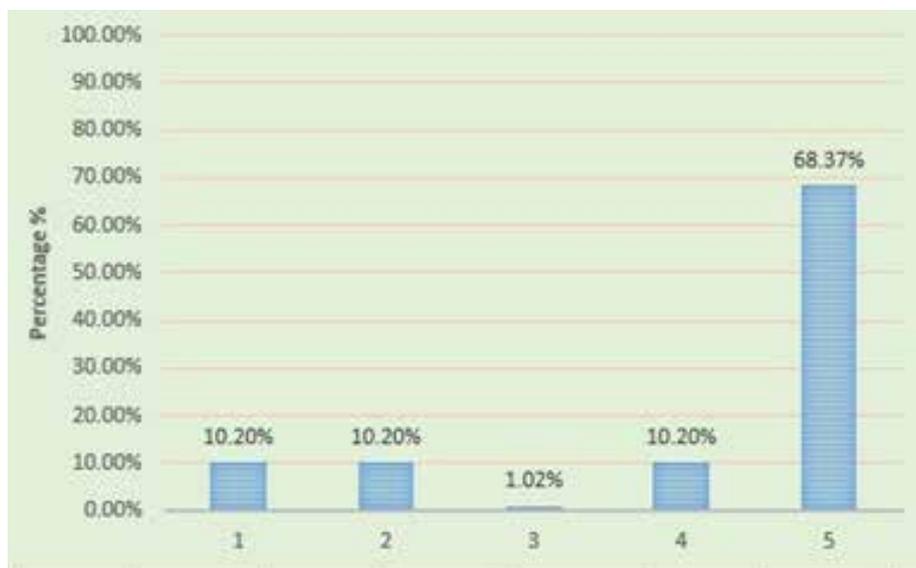
Fonte: Autor (2019).

Do Gráfico 10 acima, pode-se ver que 80,61% dos entrevistados acreditam que a congregação é totalmente submissa à sua pregação. Além disso, a pesquisa revelou que 82,65% dos entrevistados também são da opinião de que a disseminação da consciência de segurança cibernética será ampla se eles usarem seu púlpito para propagá-la. Os dois resultados obtidos nesta pesquisa vão em conjunto com a pesquisa da BBC 2010, conforme revelado por Nwaubani (LETTER..., 2014) que a maioria das pessoas na Nigéria está profundamente comprometida com as práticas e princípios de ambos Cristianismo e Islã. O resultado obtido da pesquisa pode ter enfatizado igualmente a posição de Nwaubani de que os livros publicados pelos clérigos são campeões de vendas em uma sociedade que é frequentemente acusada de ter uma pobre cultura de leitura. O relatório revelou ainda que as instruções em mensagens de texto de clérigos renomados são geralmente levadas a sério na Nigéria, e na maioria das vezes se tornam virais.

4.1.11 Efeito da Campanha de Sensibilização Para a Cibersegurança na Atenuação da Cibercriminalidade

O pesquisador inquiriu os entrevistados se eles acreditam que as atividades dos criminosos cibernéticos poderiam ser drasticamente reduzidas se houver uma grande conscientização sobre segurança cibernética e criminalidade. Os resultados são mostrados no Gráfico 11 abaixo.

Gráfico 11 – Gráfico do Efeito da Campanha de Conscientização Para a Cibersegurança na Mitigação da Cibercriminalidade



Fonte: Autor (2019).

O Gráfico 11 mostra que 68,37% dos entrevistados estão otimistas de que uma maior conscientização sobre a segurança cibernética poderia ajudar a reduzir as atividades dos criminosos cibernéticos. Esta revelação é apoiada por 10,20% que também acreditam que a campanha de conscientização poderia ter um efeito preventivo sobre as atividades dos criminosos cibernéticos. O resultado obtido aqui é semelhante à revelação de Johnson e Bowers (2003) de que a publicidade pode melhorar tremendamente a eficácia da redução do crime. O pesquisador acrescentou que uma campanha de conscientização cuidadosamente organizada pode representar uma poderosa e econômica ferramenta na prevenção do crime.

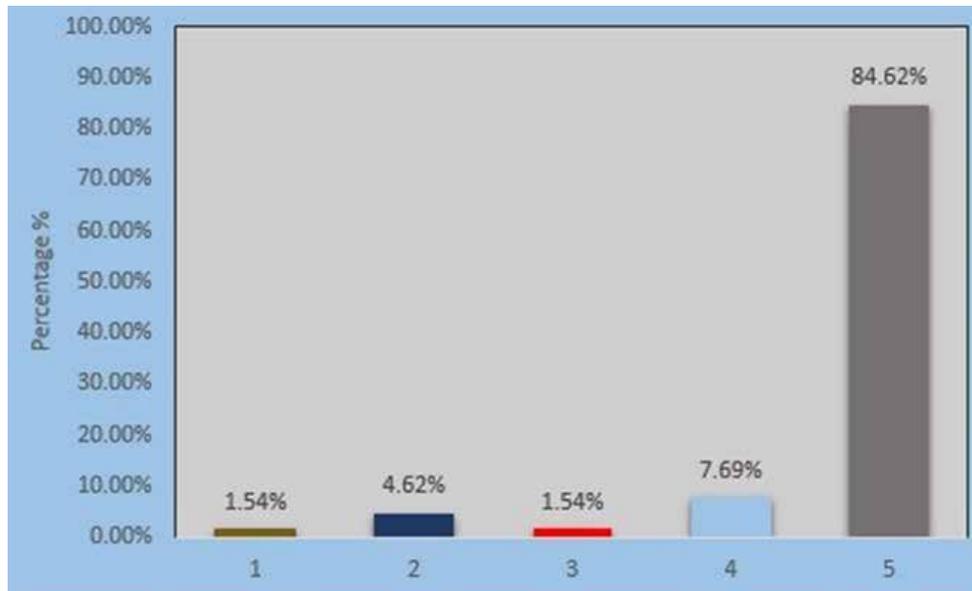
4.2 Análise dos Dados Obtidos dos Profissionais de Cibersegurança

Esta seção discutiu os dados obtidos dos respondentes que são alocados em áreas relacionadas à cibersegurança dentro das várias agências governamentais. Estas agências incluem ONSA, NITDA, EFCC, DSA e Comando Espacial do Exército. Os entrevistados de organizações privadas não foram considerados porque eles sempre organizam campanhas de conscientização sobre segurança cibernética em colaboração com as agências governamentais. Os dados não foram analisados em termos dos obtidos de cada agência individual, mas como dados das agências profissionais. O questionário possuía 4 perguntas no total e cada pergunta tinha uma classificação de 1 a 5, sendo 1 o mais fraco e 5 o mais forte.

4.2.1 Condução da Campanha de Sensibilização Para a Cibersegurança

O pesquisador perguntou aos entrevistados se já estiveram envolvidos na condução de campanhas de conscientização cibernética e o resultado da pesquisa é mostrado no gráfico 12 abaixo:

Gráfico 12 – Gráfico dos Resultados Sobre a Condução de Campanhas de Sensibilização Para a Cibersegurança



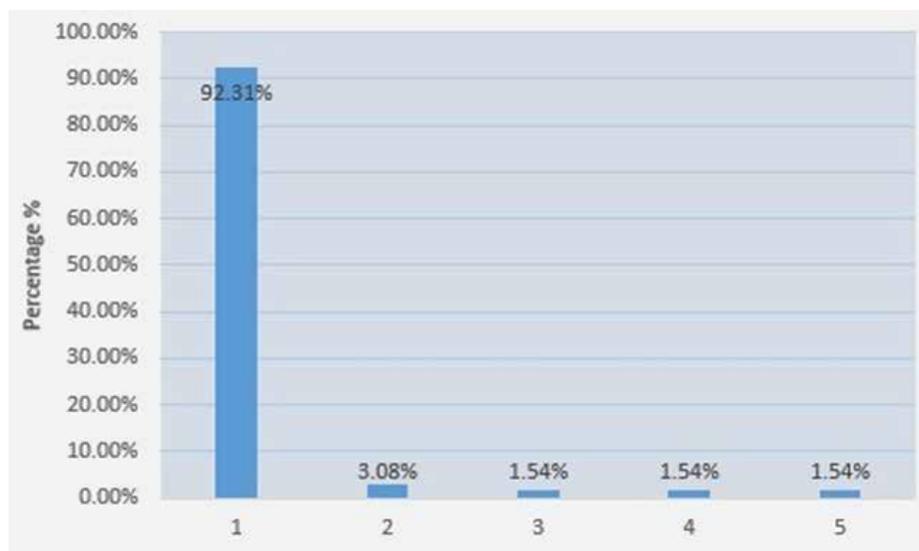
Fonte: Autor (2019).

No Gráfico 12, pode-se ver que 84,62% dos entrevistados relataram ter participado fortemente em campanhas de sensibilização para a cibersegurança. O forte contraste entre as pessoas que afirmam ter participado fortemente em campanhas de sensibilização e 7,69% dos entrevistados que alegam já ter participado revelou que quase todo o pessoal das agências estava, de uma forma ou de outra, envolvido em campanhas de sensibilização para a cibersegurança. Este achado coincidiu com a descoberta da revisão do GCSCC (2018) sobre maturidade da capacidade de cibersegurança na Nigéria, que revelou que iniciativas nacionais para a conscientização sobre segurança cibernética de fato ocorrem na Nigéria. O relatório destacou ainda que outubro de 2018 foi NCSAM representando um esforço adicional de atividades de conscientização que ocorrem na nação. A revisão também destacou a participação de organizações como CSEAN, (E-PPAN) na sensibilização do público enquanto várias universidades nigerianas oferecem cursos de segurança cibernética, juntamente com algumas pesquisas de segurança cibernética.

4.2.2 Condução de Campanhas de Conscientização Para a Cibersegurança em Locais de Adoração

O pesquisador inquiriu os entrevistados se eles já haviam organizado qualquer campanha de conscientização sobre segurança cibernética em qualquer lugar de adoração e o resultado da pesquisa é mostrado no Gráfico 13 abaixo.

Gráfico 13 – Gráfico dos Resultados Sobre Campanhas De Sensibilização Para a Cibersegurança em Qualquer Local de Adoração



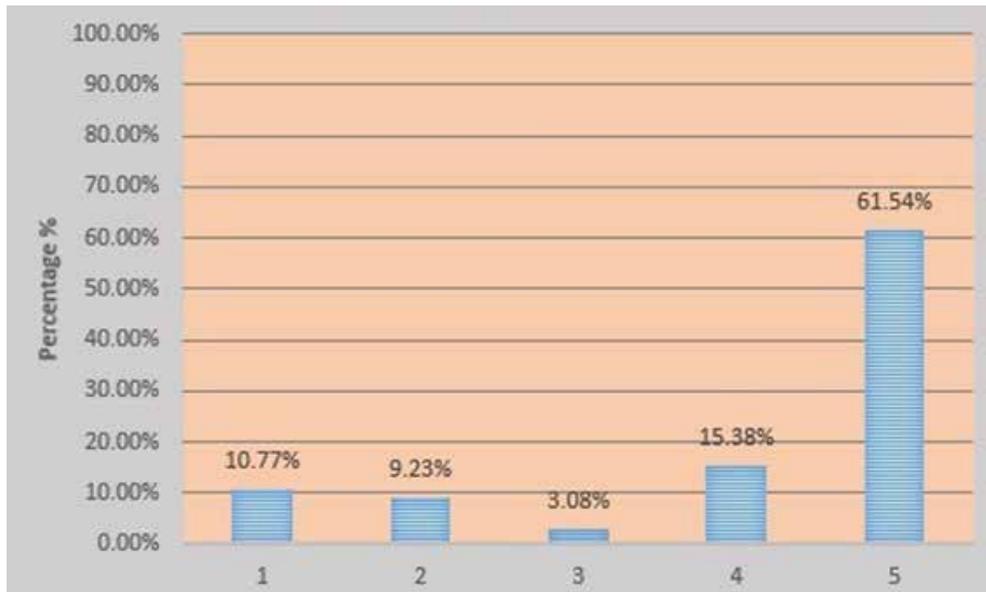
Fonte: Autor (2019).

O Gráfico 13 acima revelou que 92,31% dos entrevistados concordaram fortemente que nunca tinham organizado qualquer forma de campanha de sensibilização em qualquer centro de culto religioso. O alto percentual obtido a partir de pesquisa corroborou com o relato do Tenente-Coronel M. B. Fakandu, Assistente de Direção, Proteção da Infraestrutura Crítica de Informação (CIIP), ONSA, quando entrevistado pelo telefone afirmando que seu gabinete nunca tinha realizado qualquer campanha de cibersegurança para uma instituição religiosa, desde a sua nomeação para o cargo. Ele acrescentou que uma análise do arquivo oficial, igualmente, não revelou qualquer evidência de uma atividade anterior dessa natureza. Além disso, o Sr. Sa'adAbubakar, chefe da unidade de Cibercrime da EFCC, fez o mesmo relato quando entrevistado por telefone. A dupla também declarou não ter conhecimento de campanhas de conscientização sobre segurança cibernética organizadas por outras agências de segurança, pois nunca haviam sido mencionadas no Conselho Consultivo de Segurança Cibernética Nacional nem nas reuniões de rotina da Equipe Nigeriana de Resposta a Emergências em Computadores (ngCERT) (BASSIC-RESEARCH, 2019).

4.2.3 Influência da Religião na Sociedade

Os respondentes foram questionados sobre a influência da religião na sociedade e as suas respostas são exibidas no Gráfico 14 abaixo:

Gráfico 14 – Gráfico do Resultado Sobre Influência da Religião na Sociedade



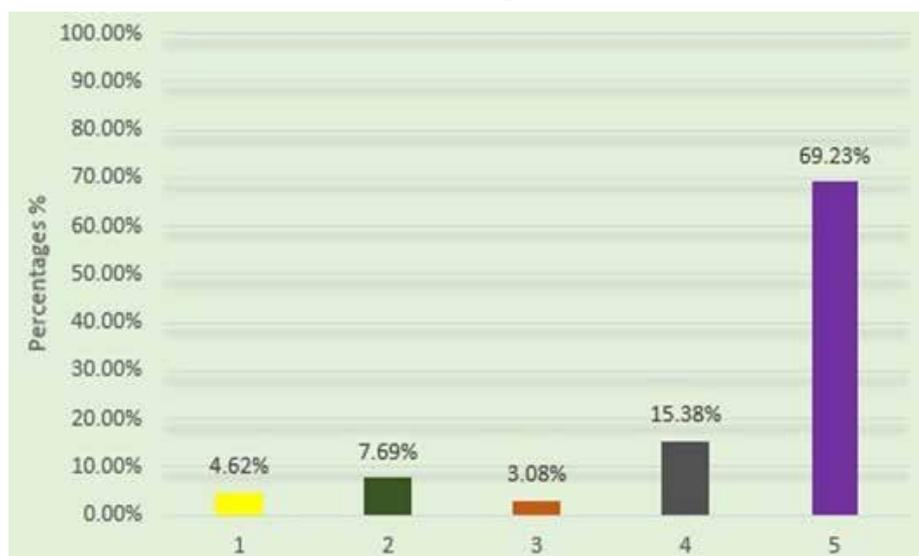
Fonte: Autor (2019).

O Gráfico 14 acima revelou que 61,54% dos entrevistados acreditam que a religião tem uma tremenda influência sobre a sociedade na Nigéria. 15,38% também acreditam que a religião tem influência sobre a população nigeriana. O resultado obtido nesta investigação pode ser considerado congruente com Ojonemi et al. (2014) que a religião na Nigéria e a fé são aspectos críticos da vida cotidiana e influenciam as leis, pensamentos e atitudes. Os pesquisadores afirmaram ainda que a religião desempenha um papel importante na formulação de políticas e grandes projetos públicos, devido à importância atribuída à ela.

4.2.4 Impacto dos Líderes Religiosos na Propagação da Consciência Sobre Cibersegurança

O pesquisador questionou sobre o impacto que os líderes religiosos podem ter na propagação da consciência da cibersegurança e o resultado obtido são como mostrado no Gráfico 15 abaixo:

Gráfico 15 – Gráfico com o Resultado Sobre o Impacto dos Líderes Religiosos na Propagação da Consciência Sobre Cibersegurança



Fonte: Autor (2019).

A partir do Gráfico 15 verifica-se que 69,23% dos respondentes acreditam que os líderes religiosos podem ter um grande impacto na propagação da consciência de segurança cibernética. A figura revelou ainda que 15,38% dos respondentes acreditam que o clero pode ter um efeito na propagação da consciência da cibersegurança. A revelação pode ser considerada verdadeira, considerando que o ponto de vista religioso sobre o planejamento familiar havia inibido o sucesso de todas as intervenções organizadas destinadas a aumentar a adoção de anticoncepcionais na Nigéria, deixando o país com uma das mais baixas Taxas de Prevalência de Anticoncepcionais Modernos (mCPRP) estimado em 9,8% (NATIONAL POPULATION COMMISSION; ICF INTERNATIONAL, 2014). No entanto, sabendo que os líderes religiosos na Nigéria podem influenciar e moldar substancialmente as ideias e opiniões das pessoas sobre a questão, a Iniciativa Nigeriana de Saúde Reprodutiva Urbana (NURHI) decidiu fazer parceria com os líderes religiosos para promover a conscientização sobre o uso de contraceptivos. Adedini et al. (2018), que documentaram a pesquisa, revelaram que a decisão de 66,4% das mulheres que concordaram com o planejamento familiar foi influenciada por declarações inspiradoras continuadas a favor do planejamento familiar em reuniões públicas e através da mídia pelo clero.

5 Resumo das conclusões

O estudo investigou o tempero que faltava na educação em segurança cibernética na Nigéria: a Perspectiva da Segurança Nacional. Para isso, dezesseis e quatro questões de pesquisa para o clero e os profissionais de cibersegurança, respectivamente, além de entrevistas, foram executadas para o estudo. Os dados obtidos foram analisados quantitativamente e apresentados usando gráficos para ilustrar as relações entre as variáveis do estudo. Consequentemente, os resumos das conclusões são:

- a. O clero tem amplo conhecimento da internet e visita a internet com frequência.
- b. O clero não tem conhecimento da cibersegurança.
- c. O clero nunca teve nenhuma campanha de conscientização sobre segurança cibernética organizada em seu lugar de culto.
- d. O clero não tem conhecimento da cibercriminalidade.
- e. O clero está ciente de Yahoo Yahoo e 419, mas não tem ideia de que é o mesmo que cibercrime.
- f. O clero, em um momento ou outro, foi afetado pela cibercriminalidade.
- g. O clero não sabe as medidas a tomar em caso de ciberataque.
- h. Um grande número de pessoas frequenta serviços em vários locais de culto.
- i. As mensagens a partir do púlpito têm grande influência nas massas nigerianas.
- j. A campanha de conscientização sobre segurança cibernética terá um grande efeito preventivo sobre o crime cibernético.
- k. Os profissionais da cibersegurança realizaram muitas campanhas de sensibilização para a cibersegurança.
- l. Os profissionais da cibersegurança nunca organizaram nenhuma campanha de sensibilização para a cibersegurança em locais de culto.
- m. A religião tem um efeito tremendo na sociedade nigeriana.
- n. A inclusão do clero na campanha de sensibilização para a segurança cibernética terá um grande efeito na educação cibernética na sociedade nigeriana.

De acordo com as conclusões do estudo, recomenda-se que a futura campanha de sensibilização para a cibersegurança seja organizada junto do clero, a fim de impulsionar o máximo benefício inerente à sua influência na sociedade nigeriana.

6 Conclusão

Ao longo da última década, a internet tem experimentado um crescimento explosivo no número de usuários conectados, aumentando diariamente a uma taxa exponencial. À medida que a internet cresce para se tornar mais acessível e mais serviços se tornam dependentes dela para o seu funcionamento diário, o mesmo acontece no horizonte da ameaça. Os Estados gradualmente se conformam com os perigos cibernéticos e estabelecem diretrizes, políticas e instituições para lidar com isso. Apesar disso, espera-se definitivamente que a fraude na internet aumente à medida que a presença do comércio eletrônico aumenta na internet e que o atual impulso do governo nigeriano para pressionar a sua política de “sociedade sem dinheiro físico”. Tendo em conta este fato, o governo concebeu vários programas para sensibilizar o público para os riscos e ameaças de cibersegurança, bem como para a forma de os enfrentar, a fim de servir de verdadeira ferramenta para mitigar os perigos da cibercriminalidade e reforçar a segurança nacional. No entanto, o esforço do governo pode não ter sido sentido devido ao fato de que todas as campanhas organizadas de conscientização sobre segurança cibernética estavam voltadas às instituições de treinamento e oficiais, enquanto a maior população do país está desempregada. Consequentemente, com a religião sendo um agente fundamental e talvez um dos fatores mais importantes que tendem a criar influência na vida da maioria dos nigerianos, a utilização do clero poderia, portanto, ser o maior ativo dos governos em sua campanha de conscientização sobre segurança cibernética.

Agradecimentos

Glória a Alá SWT, cuja misericórdia eterna me permitiu realizar este projeto. Gostaria de expressar a minha profunda gratidão ao meu ilustre supervisor, o Coronel Marcelo Gomes. Ao lado do meu supervisor, gostaria de estender a minha mais profunda gratidão ao meu país por ter dado a oportunidade de fazer parte do BASSIC 2019. Quero também agradecer à minha família pelo apoio sem fim, aos meus instrutores pela sua orientação e aos seus colegas pela sua grande ajuda.

Referências

- ADEDINI, S. A. et al. Role of religious leaders in promoting contraceptive use in Nigeria: Evidence from the Nigerian Urban reproductive health initiative. **Global Health Science and Practice**, [Baltimore], v. 6, n. 3, p. 500-514, 2018.
- AJA, V. T. The relevance of patients' spiritual care in the Nigerian cultural context: a health care chaplain's perspective. **The Journal of Pastoral Care & Counseling: JPCC**, [Thousand Oaks], v. 73, n. 2, p. 82-87, 2019.
- AJZEN, I. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. **Journal of Applied Social Psychology**, [S. l.], v. 32, n. 4, p. 665-683, Apr 2002.
- AKIYODE-LAWANSON, J. Cybercrime: Nigeria ranks 3rd most attacked country in Africa. **BusinessDay**, Lagos, Nigeria, Mar 9, 2019. Available at: <https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/>. Access on: Sep 21, 2019.
- ARANSIOLA, J. O.; ASINDEMADE, S. O. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. **Cyberpsychology, Behavior, and Social Networking**, [New Rochelle, NY], v. 14, n. 12, p. 759-763, Dec 2011.
- BAIDEN, J. **John Baiden, BSc., MBA., M.Sc., (distinction) JD, LL.M (distinction)** 1. [s. d.]. p. 1-14.
- BASSIC-RESEARCH. **BrazilWarCollege - Google Drive**. [S. l.: s. n.], 2019. Available at: <https://drive.google.com/drive/folders/1LdXeL5f7iCNwCE2xXC9AeEc1HU4PREdR>. Access on: Sep 21, 2019.
- BLOOMFIELD, C.; BOMMARITO, R. K.; KUHL, M. **Supporting military families through research and outreach public awareness campaigns**. In: SEMANTIC SCHOLAR. [S. l.]: Allen Institute for AI, July 2015. Available at: <https://pdfs.semanticscholar.org/7432/6da820ae48d452f08754e8b7d3cef0de969d.pdf>. Access on: June 6, 2020.
- CENTRAL BANK OF NIGERIA. **Cash-less Nigeria**. Abuja: Central Bank of Nigeria, 2019. Available at: [https://www.cbn.gov.ng/cashless/#targetText=The Central Bank of Nigeria,N3%2C000%2C000 for Corporate bodies](https://www.cbn.gov.ng/cashless/#targetText=The%20Central%20Bank%20of%20Nigeria,N3%2C000%2C000%20for%20Corporate%20bodies). Access on: Sep 21, 2019.
- CENTRE FOR CYBERSPACE STUDIES. **Keffi, Nigeria: CCS-NUSUK**, 2019. Available at: <https://www.ccs-nsuk.net/>. Access on: Sep 21, 2019.
- CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA. **Lagos, Nigeria: CSEAN**, 2019. Available at: <https://csean.org.ng/>. Access on: Sep 21, 2019.

DAHIR, A. L. Cybercrime is costing Africa's business billions. **QuartzAfrica**, [S. l.], June 2018. Available at: <https://qz.com/africa/1303532/cybercrime-costs-businesses-in-kenya-south-africa-nigeria-billions/>. Access on: Sep 21, 2019.

DIGITAL PEERS INTERNATIONAL. **Programs**. Abuja, Nigeria: Digital Peers International, 2019. Available at: <http://www.digitalpeers.org/programs.html>. Access on: Sep 21, 2019.

FARIVAR, M. How dozens of nigerian scammers stole millions from people, businesses. **Voice of America**, [S. l.], Aug 24, 2019. Available at: <https://www.voanews.com/usa/how-dozens-nigerian-scammers-stole-millions-people-businesses>. Access on: Sep 21, 2019.

HARE, F. The cyber threat to national security: why can't we agree?. In: CZOSSECK, C.; PODINS, K. (ed.). **Conference on cyber conflict: proceedings 2010**. Tallinn, Estonia: CCD COE Publications, 2010. Available at: https://ccdcoe.org/uploads/2018/10/1_Proceedings2010FullBook.pdf. Access on: June 10, 2020.

HILTS, S. A perspective on cyber security from the Canadian nuclear private sector. In: LEUPRECHT, C.; MACLELLAN, S. **Governing cyber security in Canada, Australia and the United States: special report**. Ontario, Canada: Centre for International Governance Innovation, 2018. p. 19-21. Available at: <https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf>. Access on: Sep 21, 2019.

INTERNATIONAL CENTRE FOR LEADERSHIP DEVELOPMENT NIGERIA. **Cyber Security Awareness Month in Nigeria**. Abuja: ICLDNG, 2018. Available at: <https://icldng.org/cyber-security-awareness-month-ng/>. Access on: Sep 21, 2019.

INTERNET WORLD STATES. **Africa Internet Users, 2019 Population and Facebook Statistics**. [MadaPradexe]: Miniwatts Marketing Group, 2019. Available at: <https://www.internetworldstats.com/stats1.htm>. Acesso em: Sep 21, 2019.

JOHNSON, S. D; BOWERS, K. J. Opportunity is in the eye of the beholder: the role of publicity in crime prevention. **Criminology Public Policy**, [S. l.], v. 2, n. 3, p. 497-524, July 2003.

KOCH, R.; GOLLING, M. **The cyber decade: cyber defence at a X-ing point**. In: MINÁRIK, T.; JAKSCHIS, R.; LINDSTRÖM, L. (ed.) **10th International Conference on Cyber Conflict: CyCon X: maximizing effects**. Tallinn, Estonia: NATO CCD COE Publications, 2018. p. 159-185, 2018. Available at: https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf. Access on: June 10, 2020.

LAWANI, L. O.; IYOKE, C. A.; EZEONU, P. O. Contraceptive practice after surgical repair of obstetric fistula in southeast Nigeria. **International Journal of Gynecology and Obstetrics**, [Malden, MA], v. 129, n. 3, p. 256-259, Feb 2015.

LETTER from Africa: the power of religion. **BBC News**, [London], Nov 7, 2014. Available at: <https://www.bbc.com/news/world-africa-29692580>. Access on: Sep 21, 2019.

LEWIS, J. **Economic impact of cybercrime – no slowing down**. Washington: Center for Strategic and International Studies (CSIS), Feb 2018. Report. Available at: https://assets.website-files.com/5bd672d1924b9893a632c807/5c171d5e85ed62697a79e351_economic-impact-cybercrime.pdf. Access on: June 10, 2020.

NATIONAL POPULATION COMMISSION; ICF INTERNATIONAL. **Nigeria demographic and health survey 2013**. Abuja: NPC; Rockville, Maryland: ICF International, 2014. Available at: <https://dhsprogram.com/pubs/pdf/FR293/FR293.pdf>. Access on: June 10, 2020.

NIGERIAN COMMUNICATIONS COMMISSION. **Industry Statistics**. Abuja: NCC, 2019. Available at: <https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables-6>. Access on: Sep 21, 2019.

NIGERIAN DEFENSE ACADEMY. **Intelligence and cyber security**: academic branch. Kaduna: NDA [201-]. Available at: <https://academics.nda.edu.ng/faculties/military-science-and-interdisciplinary-studies/intelligence-and-cyber-security/>. Access on: Sep. 21, 2019.

OJONEMI, S. et al. Deficit in religious practice in Nigeria: implications for national development. **Developing Country Studies**, [S. l.], v. 4, n. 4, p. 184-194, 2014. Available at: <https://core.ac.uk/download/pdf/234681546.pdf>. Access on: June 10, 2021.

OMODUNBI, B. et al. Cybercrimes in Nigeria: analysis, detection and prevention. **FUOYE: Journal of Engineering and Technology**, [Oye Ekiti], v. 1, n. 1, 2016. Available at: <https://engineering.fuoye.edu.ng/journal/index.php/engineer/article/view/16>. Access on: June 10, 2020.

OSHO, O.; ONOJA, A. D. National cyber security policy and strategy of Nigeria: a qualitative analysis. **International Journal of Cyber Criminology**, [Gujarat], v. 9, n. 1, p. 120-143, Aug 2015. Available at: <https://www.cybercrimejournal.com/Osho&Onoja2015vol9issue1.pdf>. Access on: June 10, 2021.

PINTER, B. et al. Religion and family planning. **European Journal of Contraception and Reproductive Health Care**, [London], v. 21, n. 6, p. 486-495, Dec 2016.

SERIANU. **Africa cybersecurity report 2016**. Kenya: Serianu, 2016. Available at: <http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>. Access on: June 10, 2021.

SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY. **Minna, Niger State:** Federal University of Tecnology, c2016. Available at: <https://sict.futminna.edu.ng/>. Access on: Sep 21, 2019.

SIOBHAN, G. Fraud ring funnels data from cards to Pakistan. **The Wall Street Journal**, New York, Oct 11, 2018. Available at: <https://www.wsj.com/articles/SB12236699999723871>. Access on: Sep, 20, 2019.

TADE, O.; ALIYU, I. Social Organization of Internet Fraud among University Undergraduates in Nigeria. **International Journal of Cyber Criminology**, [Gujarat], v. 5, n. 2, p. 860, 2011. Available at: <https://www.cybercrimejournal.com/tadealiyui2011julyijcc.pdf>. Access on: June 10, 2020

TECH-U. Faculty of natural and applied sciences. Ibadan, Oyo State: **First Technical University**, [201-]. Available at: <https://tech-u.edu.ng/faculty-of-natural-and-applied-sciences/#>. Access on: Sep 21, 2019.

TIEMO, P. A.; NELLY, D. B. Efforts in combating cyber crime and criminality in Nigeria. **Information and Knowledge Management**, [S. l.], v. 6, n. 3, p. 23-28, 2016. Available at: <https://www.iiste.org/Journals/index.php/IKM/article/view/29271/30060>. Access on: June 10, 2020.

TIIRMAA-KLAAR, H. Building national cyber resilience and protecting critical information infrastructure. **Journal of Cyber Policy**, [London], v. 1, n. 1, p. 94-106, 2016.

UNIVESITY OF CALIFORNIA. Institute for Digital Research & Education Statistical Consulting. SPSS. Frequently asked questions. **What does Cronbach's alpha mean?**. Los Angeles: UCLA, [201-]. Available at: <https://stats.idre.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/>. Access on: Sep. 21, 2019.

VERMUELEN, J. Anonymous hacks SA government database. **MyBroadband**, Olifantsfontein, South Africa, Feb 12, 2016. Available at: <https://mybroadband.co.za/news/security/155030-anonymous-hacks-sa-government-database.html>. Access on: Sep 21, 2019.

WHAT is Yamane sample calculation?. In: QUORA. [S. l.: s. n., 2017?]. Available at: <https://www.quora.com/What-is-Yamane-sample-calculation>. Access on: Sep. 21, 2019.