RESEARCH ARTICLE OPEN ACCESS

Cybersecurity Atlas, Nigeria

Egere, A.N

Department of Computer Science The Polytechnic - Bali

ABSTRACT

As cyber-attacks continue to evolve, posing real threats to businesses, individuals and national security, there is an urgent need to respond with concerted effort to counter the threats. Nigeria is the 8th country in the world with most internet users and the threat of cyber-attacks can only get worse. An effective response would require a collective approach revolving around public and private sectors working together to deliver real-world outcomes and ground-breaking innovation to tackle the challenge. This will involve developing and harnessing relevant cyber skills and capabilities. We propose that the first vital step in this direction is to identify and locate existing cyber related-skills. This research seeks to map existing centres of expertise in the field of cybersecurity in Nigeria into a "Cybersecurity Atlas". This paper focuses on academic institutions of higher learning as a prelude to a wider scope focusing on other public and private cybersecurity centres as well as businesses. A preliminary result shows that only 36 Innovation Enterprise Institutions and 5 Universities offer cybersecurity related programmes in Nigeria.

Keywords:-cybersecurity; atlas; Nigeria; tertiary institutions

I. INTRODUCTION

Nigeria ranks 8th in a 2017 report [1] of top 20 countries with the highest number of internet users. This implies that there are more internet-connected devices in Nigeria than most countries in the world. With increased connectivity comes increased attack vectors and exposure, leading to increased possibility of attacks. This poses huge risks to national security, critical national infrastructures and businesses in Nigeria.

Cybersecurity risks are increasing exponentially. According to studies, the global economic impact of cybercrime, from 2013 to 2017, rose by fivefold, and could further quadruple by 2019 [2]. There has been a continuous global increase in the sophistication and number of cybersecurity attacks [3]. Most of these attacks are untargeted – they are not aimed at any specific targets. These are mostly malware distributed via the internet seeking to exploit any vulnerable system they come in contact with. A typical example is the 2017 WannaCry Ransomware attack [4] that affected over 400,000 computers in over 150 countries. The Moore's Law order of increasing innovation in technology has proliferated capabilities and what is now possible to be accomplished with the computer. As a result, the *Cyber World* (the Internet and its possibilities) has almost completely mirrored the real world – and more worryingly in the areas of crime, war, terrorism, election influence, business battle, misinformation, fake news etc. Governments across the world have realised the enormity of the challenge and are responding appropriately.

In 2015 the Nigerian 7th NASS passed the Nigerian Cyber Crime Act [5, 6] and it was signed into law by President Goodluck Jonathan. This was, according to the Nigerian Army, in response to the cyber space's increasing "implication and challenges to Nigeria's national security". The Nigerian Army is also prepared, and improving its capability, to also defend Nigeria in the cyberwar arena [7, 8]. In the UK, the government recently established the National Cyber Security Centre to help "make the UK the safest place to live and do business online" [9]. The government, through its HEFCE (Higher Education Funding Council for England), is currently funding conversion MSc Cybersecurity programmes across universities to enable those without relevant computing background to acquire important cybersecurity skills. This is with the understanding that the more cyber skills and awareness the people have, the more cyber secure the country will be. In Europe, the European Union (EU) is sponsoring a project for the creation of "a network of cybersecurity competence centres to stimulate the development and deployment of technology in cybersecurity" [10]. This is aimed at pooling resources together and encouraging partnership amongst the cybersecurity community, both public and private.

This research is similar to the EU's network of cybersecurity competence centres project. The aim is to map existing centres of cybersecurity expertise and competence in Nigeria. These centres, public and private include academic institutions, research centres, training institutes, organisations and businesses providing cybersecurity-related services etc. The results of this mapping will be translated into a "Nigeria Cybersecurity Atlas", indexing existing cybersecurity centres in Nigeria. This will share information about the organisations such as their cybersecurity work, expertise as well as relevant contact details. The atlas will be made publicly available via a dedicated website and other publications. This will form a one-stop shop for anyone seeking information about cybersecurity competence in the country. It will help in boosting capabilities in terms of technology and skills, as it aims at becoming a valuable tool and a reference for the cybersecurity community to look for potential partners and pool resources.

Opportunity for partnership, resource pooling and skills identification are core aspects of this study. There is no doubt that this study will increase awareness, encourage development in the sector and thereby contribute to the cyber security of the nation. This study will be in phases, leading to a complete mapping of cybersecurity skills centres in the country including academic institutions, research centres, training institutes, organisations and businesses providing cybersecurity-related services etc. The initial phase, as in this paper, focuses on public and private academic institutions of higher learning. These form the natural place for acquiring the required skills. This study will reveal where the skills are.

II. DATA COLLECTION

There are several methods of data collection [11, 12] available to research however, a chosen method for a particular research should be relevant and well suited to the needs of that particular research [12]. This means that it should help in the collection of data in a way that makes it easy to answer the research questions. Another important consideration is the source of data. This is particularly important as some sources may not present accurate data – e.g., unreliable source, outdated data, incomplete data etc. So the quality of a research outcome does not only depend on how data was collected but also on the integrity of the data as well as other factors.

For the wider scope of this study, a structured and comprehensive survey would be necessary for the collection of relevant data. However, in this preliminary study, considering accredited academic institutions of higher learning, data was collected directly from relevant agencies. These are government agencies responsible for supervising and overseeing the running of the tertiary academic institutions. The academic institutions in this category, within the scope of this study, include universities, polytechnics and colleges of education. The relevant government agencies include the National Universities Commission (NUC) [13], Joint Admissions and Matriculation Board (JAMB) [14], National Board for Technical Education (NBTE) [15], and National Commission for Colleges of Education (NCCE) [16]. Data was collected in person by visiting the agencies as well as accessing their sites for verified formal documents.

The academic institutions comprise of federal, state and private owned. Only accredited programmes from the relevant sources [13, 14, 15, 16, and 21] are considered. Table 1 shows the classification of generated data.

TABLE 1: Classification of research data

Type of institution	**Ownership**	**Location**	**Cybersecurity related course/Level***
College of Edu	Federal	North/South	BSc/BEng/HND/ND/NID
Polytechnic & Others	Private	NC/NE/NW	MSc/MEng/MRes
University	State	SE/SS/SW	PhD
Contact	Other		Research

* No college of education in Nigeria currently offers any cybersecurity related course. That is why a relevant degree classification has not been included.

Of importance here are the location of the institutions and information regarding any cybersecurity related programmes (degree and/or research). Data is classified as in Table 1 to give a general picture of the spread of academic programmes in cybersecurity across the country. Institutions are identified by name, contact (e.g., the department and/or contact person/office for the programme), type, ownership and location. Programmes are identified by courses (e.g., Cybersecurity, Risk Management, Information Assurance, Information Security etc.) and relevant degree/level classification (e.g., HND, BSc, MSc, PhD etc.). It is important to note that *course* and *programme* are used interchangeably in this paper to refer to a programme of study, e.g., *BSc Cybersecurity* and not a module, e.g., *SEC101: Foundations of Cybersecurity* that is part of a *BSc Cybersecurity* programme.

The location of these studies does not represent a concentration of the corresponding cybersecurity skills. A correlation of cybersecurity academic centres and localised expertise will need to be studied in order to make an informed conclusion. Whereas in other places, like the UK, stats [17] suggest that most graduates end up living in the region where they studied, this is not the case in Nigeria. Nigerian graduates are required to complete the national youth service programme after graduation and this influences where many of them work and live.

III. DATA ANALYSIS

The generated data are analysed to give a clear picture of the spread of academic institutions and cybersecurity academic centres across Nigeria. It is important to note that the aim of this is for easy identification of relevant cybersecurity skills to aid collaboration, awareness and national cyber security preparedness. After analysing the categories and spread of institutions, an atlas is built for geolocalised information display.

A. *Colleges of Education*

There are 86 colleges of education in Nigeria [16] and these comprise of federal, state and private colleges of education. Table 2 is the summary of colleges of education in the six geopolitical zones.

TABLE 2: Summary of colleges of education across Nigeria

Zone\Ownership	**Federal**	**State**	**Private**	**Total**
North Central	3	7	2	**12**
North East	4	7	1	**12**
North West	4	8	0	**12**
South East	3	4	7	**14**
South South	3	9	0	**12**
South West	5	11	8	**24**
Total	**22**	**46**	**18**	**86**

There is at least one college of education in every state, including the Federal Capital Territory (FCT). The South West zone has the highest number of colleges, in every category, with Lagos topping the list. All three Northern zones have equal number of colleges.

These colleges offer a very wide range of programmes, including specialised courses. The analysis indicates that no college of education (both private and government) in Nigeria is offering courses in cybersecurity or related. Colleges of education are primarily there to provide teacher education and according to NCCE, the seminal philosophy in the National Policy on Education (NAPE) is that "no education can rise above the quality of its teachers". NAPE [18] requires that Information Technology (IT) training be incorporated into all teacher-training programmes. Cybersecurity is now at the core of IT and yet no college of education is currently training teachers in relevant skills. This is particularly important as efforts are in place elsewhere [19, 20] to include cybersecurity training at pre-tertiary education in order to raise future experts that would defend country from cyber-attacks. Skills shortage will surely undermine confidence in the country's cyber defences.

B. *Polytechnics and Similar Tertiary Institutions*

This category includes Polytechnics (Poly), Colleges of Agriculture (CoA), Colleges of Health Science (CoHS), Technical Colleges (TC), Innovation Enterprise Institutions (IEIs), Vocational Enterprise Institutions (VEIs) and Other Monotechnics (OM) in Nigeria. There are 499 accredited institutions in this category [21], summarised according to the zones in Tables 3 and 4.

TABLE 3: Summary of polytechnics and similar institutions in the North [21]

Type / Zone	**North Central**			**North East**			**North West**			**Total**
	Fed	Sta	Pri	Fed	Sta	Pri	Fed	Sta	Pri	
Poly	5	6	5	4	4	0	5	7	0	**36**
CoA	6	4	0	2	4	0	4	4	0	**24**
CoHS	2	2	1	2	0	0	3	1	0	**11**
OM	2	0	0	1	3	0	6	1	0	**13**
IEIs	0	0	20	0	0	0	0	0	13	**33**
VEIs	0	0	9	0	0	0	0	0	12	**21**
TC	2	14	0	1	15	0	2	24	0	**58**
Total	**17**	**26**	**35**	**10**	**26**	**0**	**20**	**37**	**25**	**196**
	78			**36**			**82**			

KEY: Fed - Federal   Sta - State   Pri - Private

In the North, the North East has the lowest number, less than half of the second placed North Central, of institutions as shown in Table 3.

TABLE 4: Summary of polytechnics and similar institutions in the South [21]

Type / Zone	South East			South South			South West			**Total**
	Fed	Sta	Pri	Fed	Sta	Pri	Fed	Sta	Pri	
Poly	3	3	4	4	11	7	4	12	15	**63**
CoA	2	2	0	0	1	0	5	1	0	**11**
CoHS	3	3	0	5	3	0	4	2	1	**21**
OM	4	0	0	3	0	0	5	0	2	**14**
IEIs	0	0	13	0	0	28	0	0	53	**94**
VEIs	0	0	10	0	0	19	0	0	22	**51**
TC	1	9	0	2	15	0	3	18	1	**49**
Total	**13**	**17**	**27**	**14**	**30**	**54**	**21**	**33**	**94**	**303**
	57			**98**			**148**			

KEY: As in Table 3 above

There are a total of 179 unique accredited programmes available in the different institutions identified in Tables 3 and 4. Only one of these programmes, NID (National Innovation Diploma) in Networking and System Security, is cybersecurity related. The NID in Networking and System Security is only available in IEIs. Table 5 shows the distribution of accredited IEIs that offer the programme as at January 2018 [22].

TABLE 5: Summary of IEIs that offer NID Networking and System Security

Zone\Ownership	**Federal**	**State**	**Private**	**Total**
North Central	0	1 (Kogi)	9	**10**
North East	0	0	0	**0**
North West	1 (Kano)	1 (Katsina)	3	**5**
South East	0	0	5	**5**
South South	0	0	10	**10**
South West	1 (Lagos)	0	20	**21**
Total	**2**	**2**	**47**	**51**

There are 51 NBTE accredited IEI centres across the country with cybersecurity related skills. 'Centres' is used instead of 'Institutions' as the aim of this study is to map skills locations. Most of these centres are private institutions. Note that some of these centres are branches of the same institution – e.g., there are 12 NIIT Training Centres across many states. Detailed information about these centres are captured in the atlas (Figure 2) and available interactively at [24].

The number of accredited programmes for an institution may differ from the actual number of programmes available in that institution. For example, the number of NBTE accredited programmes for IEIs is different from the number of IEI programmes in JAMB brochure [14]. Some of these institutions obviously have many centres (branches) like the NIIT Training Centres. The study in this paper is based on accredited programmes and institutions. It relies on data from the appropriate accreditation agencies and not from JAMB.

It is important to note that while the Joint Admissions and Matriculations Board (JAMB) oversees and conducts entrance examinations for prospective students into Nigerian tertiary academic institutions, it does not concern itself with the accreditation of the programmes offered in those institutions. The programmes listed in JAMB brochures are sourced directly from the institutions and not from the accreditation bodies. So, the brochures may contain both accredited and non-accredited programmes. This is understandable as institutions may be going through the accreditation process while a brochure is in print. According to the 2018 JAMB brochure [14], all programmes advertised in the brochure "*have been officially received from the institutions and are deemed to have met all appropriate standards and have been approved by competent authorities*".

The analysis in this section indicates that, apart from IEIs, no accredited polytechnic or any other related institution (both private and government) in Nigeria is offering courses in cybersecurity or related.

C. *Universities*

Unlike private IEIs, universities do not have duplicate branches. A university may have different campuses but each campus runs unique programmes. So, university campuses are not counted as separate centres. Also, affiliate institutions are not counted as additional centres as they would have been captured in their relevant categories.

TABLE 6: Summary of universities across Nigeria

Zone\Ownership	**Federal**	**State**	**Private**	**TOTAL**
North Central	6	5	7	**18**
North East	6	7	2	**15**
North West	9	7	1	**17**
South East	5	6	13	**24**
South South	6	9	13	**28**
South West	8	12	38	**58**
TOTAL	**40**	**46**	**74**	**160**

According to the National Universities Commission [13], there are 40 federal, 46 state and 74 private universities in Nigeria, shown in Table 6. These 160 universities run a wide range of programmes accredited by the NUC. Accreditation is an ongoing exercise which gives universities approval to run certain programmes. There are cases of institutions running unapproved programmes. For example, the NUC acknowledge this challenge and have issued a list of universities with approval to offer postgraduate programmes at the Masters and PhD levels [23]. This study only considers NUC approved programmes and institutions. Table 7 shows the list of Nigeria universities that run cybersecurity programmes.

TABLE 7: Universities offering Cybersecurity related programmes

Inst.	**Owner**	**Locatn**	**Programme**	**Degree**
AUN, Yola	Private	NE	Information System with Information Security & Assurance	BSc
BUK	Federal	NW	Cyber Security science	BSc & MSc
FUTA	Federal	SW	Cyber Security science	BSc
FUT Minna	Federal	NC	Cyber Security science	PGDM, BTech, MTech & PhD
Tech-Ibadan	State	SW	Cyber Security	BSc

Only 5 out of the 160 universities in Nigeria offer cybersecurity related programmes. These include American University of Nigeria, Bayero University Kano, Federal University of Technology Akure, Federal University of Technology Minna, and Oyo State Technical University Ibadan. Information about these institutions are mapped in the atlas. The Nigerian Defence Academy, Kaduna also offers degree programmes in Intelligence and Cyber Security.

D. *Nigeria Cybersecurity Academic Atlas*

The identified cybersecurity academic centres of expertise are designed into an atlas for a geolocalised view of the centres. This is achieved using the '*Your Places*' tool on Google map. An exported view of the atlas is shown in Figures 1 and 2. A comprehensive interactive atlas, at the end of the research, mapping all cybersecurity centres in Nigeria will be publicly available via a dedicated site. However, the interactive atlas for this initial study is publicly available via [24].

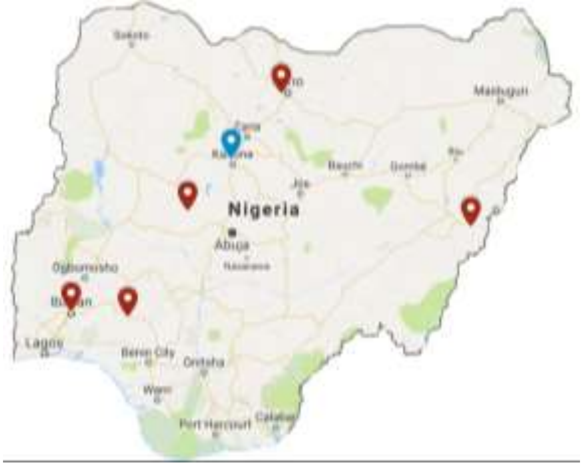


Figure 1: Cybersecurity atlas for Nigerian universities and NDA

The red beacons in Figure 1 represent the 5 universities (Table 7) that run cybersecurity related programmes. Clicking on the beacons in the interactive atlas [24] reveals detailed information about the universities, including contacts and programmes (see Figure 3). The blue beacon represents the Nigerian Defence Academy (NDA), Kaduna. NDA offers undergraduate programmes to military officers in training and postgraduate programmes for both military and civilian students.

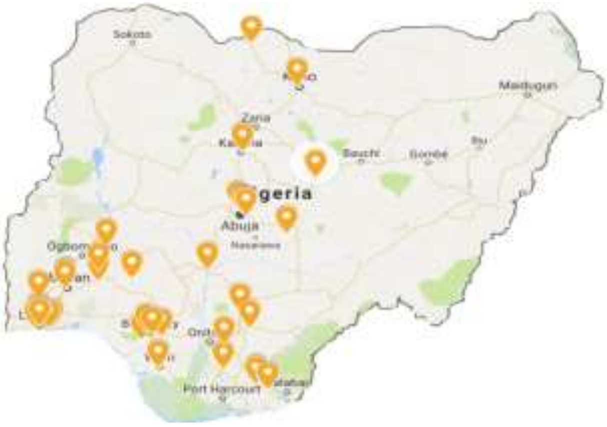
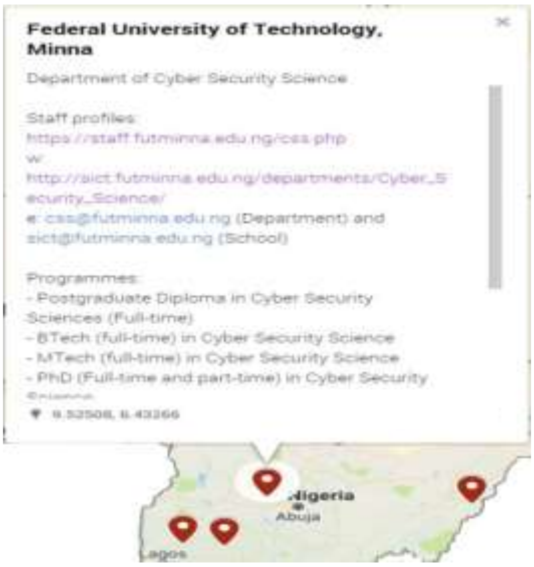


Figure 1: Cybersecurity atlas for Innovation Enterprise Institutions (IEIs)

Figure 2 shows the 51 IEIs (Table 5) that offer NID Networking and System Security. As this is a compressed static view of the atlas, it does not clearly show all the centres. For example, there are clusters in Lagos, Edo (mainly Benin City), Abuja, and Kaduna areas. These are clearly visible in the interactive atlas.



Federal University of Technology, Minna

Department of Cyber Security Science

Staff profiles:
https://staff.futminna.edu.ng/css.php
w:
http://sict.futminna.edu.ng/departments/Cyber_Security_Science/
e: css@futminna.edu.ng (Department) and sict@futminna.edu.ng (School)

Programmes:
- Postgraduate Diploma in Cyber Security Sciences (Full-time)
- BTech (full-time) in Cyber Security Science
- MTech (full-time) in Cyber Security Science
- PhD (Full-time and part-time) in Cyber Security Science

9.53508, 6.43266

Figure 3: Detailed atlas information about FUT Minna

The importance of the atlas is that it is a single-point collation of useful information about cybersecurity expertise and centres. It puts people and institutions' cybersecurity expertise on the map and makes it very easy for people to locate them. Figure 3 shows the level of information revealed by interacting with the atlas.

IV. CONCLUSION

This sponsored research seeks to map existing centres of expertise in the field of cybersecurity in Nigeria into a "Cybersecurity Atlas", publicly available through a dedicated site. This initial study has focused on tertiary academic institutions and other accredited training institutes, both government and private. The next phase of the research will include other centres of cybersecurity expertise, e.g., SMEs, consultants, private and public research centres etc. into the atlas.

This paper has analysed all accredited tertiary academic and training institutions in Nigeria and has mapped relevant cybersecurity programmes into a *Cybersecurity Atlas*. A link has been provided for interacting with the atlas. The academic institutions, both government and private, are classified into 3 groups – Colleges of Education, Polytechnics & related institutions, and Universities. None of the 86 colleges of education in Nigeria is offering programmes in cybersecurity or related. Analysis also shows that while no polytechnic offers any cybersecurity related programmes, 36 Innovation Enterprise Institutions (comprising 51 centres) offer NID in Networking and System Security. Only 5 out of the 160 universities offer cybersecurity related programmes at different levels.

This research has put cybersecurity expertise in Nigeria on the map, making it easily accessible to everyone. The importance is that, amongst many other benefits, it is a handy tool to foster collaboration in the sector. Collaboration in this sector, for example, in the area of research, is significantly important and will boost national capacity in the fight to defend Nigeria's cyber security.

REFERENCES

[1] Miniwatts Marketing Group, (2018), *Top 20 Countries With Highest Number of Internet Users - December 31, 2017*. Retrieved 24/02/2018 from http://www.internetworldstats.com/top20.htm

[2] McAfee, (2014), *Net Losses: Estimating The Global Cost of Cybercrime*, Center for Strategic and International Studies. Retrieved 24/02/2018 from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf

[3] National Cybersecurity Centre, (2018), *The Cyber Threat to UK Business - 2016/2017 Report*. Retrieved 24/2/18 from http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file

[4] The Guardian, (2017), The global ransomware attack. Retrieved 24/2/18 from https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

[5] Nigerian Government, (2015), *Cybercrimes (Prohibition, Prevention, Etc) Act, 2015*. Retrieved 24/2/18 from https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf.

[6] Fredrick, I. (2015), *Nigerian Cyber Crime Bill An Imperative to the Nigerian Armed Forcesr*. Retrieved 24/2/18 from http://www.army.mil.ng/nigerian-cyber-crime/.

[7] Fredrick, I. (2016), *Cyberwarfare and National Security: An Imperative of Nigerian Army preparedness*. https://www.docdroid.net/hPuNFKv/1-cyber-warfare-and-national-security-an-imperative-of-the-nigerian-army-preparedness-by-ikerionwu-fredrick.pdf.

[8] Nigerian Army, (2016), *Cyberwarfare and National Security*. Retrieved 24/2/18 from http://www.army.mil.ng/cyber-warfare-and-national-security/.

[9] Uk National Cyber Security Centre https://www.ncsc.gov.uk/

[10] European Commission, (2017), *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. Retrieved 24/2/18 from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

[11] Save the Children, *6 Methods of data collection and analysis*, via www.open.edu/openlearncreate/mod/resource/view.php?id=52658, viewed 20th February 2018

[12] Peersman, G. (2014), *Overview: Data Collection and Analysis Methods in Impact Evaluation*, Methodological Briefs: Impact Evaluation 10, UNICEF Office of Research, Florence.

[13] National Universities Commission, http://nuc.edu.ng/, viewed 20th February 2018

[14] JAMB eBrochure (2018), http://ibass.jamb.gov.ng/ebrochure.html, viewed 20th February 2018

[15] National Board for Technical Education, https://www.web.nbte.gov.ng/, viewed 20th February 2018

[16] National Commission for Colleges of Education, *List of Colleges of Education in Nigeria*, http://www.ncceonline.edu.ng/colleges.php, viewed 20th February 2018

[17] Ball, C. (2013), *How does the region you study in affect your graduate employment prospects?*, Which? Retrieved from https://university.which.co.uk/advice/career-prospects/how-does-the-region-you-study-in-affect-your-graduate-employment-prospects, viewed 20th February 2018

[18] Federal Republic of Nigeria (2013), *National Policy on Education*, 6th Edition, NERDC Press, Lagos

[19] Symonds, T. (2017), *Cyber security lessons offered to schools in England*, BBC. Retrieved from http://www.bbc.co.uk/news/education-38938519, viewed 20th February 2018

[20] Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017), *National Initiative for Cybersecurity Education (NICE)*, NIST, US Department of Commerce. Available at https://doi.org/10.6028/NIST.SP.800-181, viewed 20th February 2018

[21] National Board for Technical Education, (2016), *Directory of Accredited Programmes Offered in Polytechnics, Technical and Vocational Institutions in Nigeria*, 18th Edition

[22] NBTE, (2017), *Approved Innovation Enterprise Institutions as at January 2018*, Retrieved from https://www.web.nbte.gov.ng/IEIs, viewed 20th February 2018

[23] NUC, (2012), Universities approved to run Post Graduate Programmes, Retrieved from http://nuc.edu.ng/approved-universities-to-run-postgraduate-programmes/, viewed 20th February 2018

[24] Nigeria Cybersecurity Atlas, https://drive.google.com/open?id=1Dcd7aLmjcJYGceyLFAh0oIYINYvz3npW&usp=sharing