The Internet and National Security in Nigeria: A Threat-Import Discourse

Okoli A. I. Chukwuma (Ph.D) & Idom Augustine Mogom

Federal University Lafia, Nigeria.
okochu007@yahoo.com
austineidom@gmail.com

Abstract: The internet has been an important feature of modernization. Paradoxically, it has also been a veritable threat to security of nations. The implication of the internet as a security threat has been amply demonstrated in the rising incidence of cyber criminality across the world. The apparent virtual un-governability of the cyber space in Nigeria has provided a platform for the perpetration of cyber crimes, such as advanced fee fraud, terrorist recruiting and financing, hate speech, and ideo-religious radicalization, etc. Adopting a threat-import approach, predicated on secondary sources, this paper posits that poor governance of Nigeria’s cyber space has presented an opportunity for high incidence and prevalence of cyber malaise in the country. The paper submits that the prospect of mitigating the challenge rests with the entrenchment of a multi-stakeholder vigilant and resilient cyber security regimen capable of countering the activities of cyber criminals in a pro-active and co-ordinated manner.

Keywords: Cyber-security, cyber-space, Internet, national security, cyber vigilantism.

1. Introduction
Technology has been the prime-mover of human civilization, nay its most potent threat (Abraham, 2014). It is a prime-mover for it has been the force behind major societal transformations from the traditional to modern era. It is a threat because it has accounted for the world’s worst calamities. The historic Industrial Revolution that brought about the modernization of the world would not have been possible without technology. Yet, the horrendous humanitarian outcomes of the First and Second World Wars could have been averted but for technology. The Internet is a crucial aspect of modern technology. Domiciled in the global
cyber space, the Internet wields the world into an articulated digital superstructure characterized by virtual connectivity and visibility (cf. Nye, 2014). This domain has presented the world with a platform of limitless opportunities for progressive and nefarious activities. The irony of the Internet is that is both indispensable and dangerous. Concerning this irony, Dasuki (2014, p. i) avers:

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming our economy and security posture more than ever before, creating opportunities for innovations and means to improve general welfare of citizens. It is transforming many countries’ growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas. However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security.

The Nigerian cyberspace has been a critical hotbed of criminality. It has been increasingly exploited by criminals to plan and prosecute various forms of criminality. As observed by Omale and Idom (2016) although the advent of internet was not intended for crime perpetration, nonetheless its use by criminals to plan and prosecute crimes has come to stay. The activities of cybercriminals on the internet are casting a dark shadow on the integrity of the cyberspace with far-reaching implications for Nigeria’s national security. Hence as the internet continues to expand, the inevitable outcome is that our nation will be increasingly exposed to a fragile and insecure highway that offers both the good and the evil (Idom & Ugal, 2016). According to Nnamani (2016, p.8), “cyber-terrorists, spies, hackers, and fraudsters are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it and the perceived lower risk of detection and capture in conducting cybercrime….” In effect, the Internet, aided by technology-induced anonymity, has influenced cybercrime. With endless routes to a spectrum of websites, cyber criminals now have a pool of victims. Idom (2012) borrowing from Durkheim (1893), attributes these spate of criminal activities to the anonymity created by the ICT world, the distance and lack of geographical boundaries of the internet, the large pool of potential victims, the fastness of a computer mouse or telephone button in wrecking havoc and above all, the difficulty involved in tracing a cyber criminal. The misappropriation of the Internet as an instrument of crime commission in Nigeria has been vividly demonstrated by the incidence and prevalence of Advanced Fee Fraud (AFF), otherwise popularly known as ‘419’ (Osho & Onoma, 2015). Emerging trends indicate that terrorists and organized criminal syndicates have utilized the Internet as a means of perpetrating cybercrimes, such as espionage, sabotage, terrorism financing and recruiting, and human trafficking. This is in addition to the issue of hate-speech, which has been largely propagated via the social media at the detriment of the wellness of the nation.

The vulnerability of Nigeria’s cyberspace to different dimensions of cybercrime has added a new twist to the country’s national security conundrum.
More importantly the continued instrumentalization of the Internet as a channel for commission of crime in Nigeria warrants a systematic interrogation in order to situate its import vis-à-vis national security calculus. It is this concern that has informed this study. The remainder of this paper is broadly organized under the following themes: conceptual clarification; theoretical framework; contextualizing Nigeria’s cyber threat and vulnerability; implications of Nigeria’s cyber menace for national security; and conclusion.

2. Conceptual Clarifications
Two basic concepts constitute the conceptual thrust of this paper, namely the Internet and national security. The Internet is a computer based global information system composed of many interconnected computer networks (Comer, 2009). It “is a diffuse collection of standards, technologies and actors and dramatically different across layers, geographies and services” (Abraham, 2014, p.44). The Internet resides in global cyberspace, which consists of inter-connected computers networked into a digital order as well the operational culture associated with system.

National security refers to the protection of a polity and its people from all forms of existential threats, be they economic, political, social, ecological, military, technological, or psychological (Okoli & Opaleke, 2014). It is the assurance of the basic conditions that guarantee state and human security of a country. National security is a function of a blend of certain socio-structural conditions. According to Aladenusi:

National security is an appropriate and aggressive bland of political resilience and maturity, human resources, economic structure and capacity, technological competence, industrial base and availability of natural resources and finally the military might (2014, slide 3).

Evidently, the conception of national security in this discourse comprehends both its military/defence-centric and development-centric paradigms. This puts into due consideration the concerns of state and human security

The state is a territorial order that enforces its will within a jurisdictional domain. This domain comprises the land, the waters, the air-space and the cyber-space (Okoli & Ochim, 2016). Territoriality presupposes the ability of the state to hold sway within the confines of its jurisdiction. This implies the capacity to regulate persons and activities within its sphere of authority without limitations (Goldsmith, 1998).

The emergence of the cyber-space has questioned the conventional notion of territoriality. The “difficult-to-detect multi-jurisdictional transactions” that characterized the Internet have reduced the idea of territoriality to an exception rather than a rule. Hence, it is easier for public and private actors to circumvent territorial rules, often without detection (Clopton, 2016, p.46). The multi- and trans-jurisdictional transcendence of the Internet has created the challenge of governability for nations. According to Goldsmith:

A distinguishing feature of the Internet is that protocol addresses do not necessarily correlate with physical location. This means that persons transacting in cyberspace
sometimes cannot know each other’s physical location and cannot control geographical flow of content. In addition, information mediated by many internet services can appear simultaneously in all jurisdictions around the world. Finally, information transmitted on the Internet can easily flow across national borders without detection (1998, p. 477).

So, the arrival of the Internet has not only questioned the orthodox understanding of territoriality; it has, in fact, eroded it by bringing about spheres of ‘ungoverned spaces’ in its stead. It is within the ‘ungoverned spaces’ that cyber-crime breeds and culminates into a threat to national security.

In order to further enrich the theoretical anchorage of the foregoing discourse, there is need for theoretical triangulation so as to have a robust appreciation of how the internet has become attractive for criminals, posing thereby a serious threat to the Nigerian cyber security. In the light of this, the theory of routine activity has been elected. The routine activity theory of crime was propounded by Cohen and Felson (1979). The theory points to the interaction between three salient variables that explain the routine occurrence of crime in society: the availability of suitable targets, the absence of capable guidance, and presence of motivated or potential offenders. Using this theory in analogy to internet’s threat to Nigerian cyber security, it could be observed thus: the availability of suitable target depicts the potential pool of victims on the internet and the porous nature of the internet; the absence of capable guidance in this case represents lack of cyber vigilantism and security, e-policing, national central control, and functional national database; while the presence of motivated or potential offenders connotes teeming unemployed youths with high quest for material aggrandizement.

When these variables or components are present in any given society, there is a greater likelihood that crime (cybercrime in the case of the foregoing) will occur. Thus, according to Idom and Tormusa (2016), the motivation to commit crime and the supply of offenders tend to be constant in contemporary society. That is, in most societies, there are always some people who are willing to break the law for gain, revenge, greed or some other motives. Greed and gain from both perpetrators and victims have made cybercrimes to thrive on the internet.

The utility of this theory in the context of this study is that it provides a simple and powerful insight into factors that engender cybercrimes in Nigeria. The crux of this theory is the idea that, in the absence of effective control, such as cyber security or cyber vigilantism, offenders will prey upon attractive targets such as the porous internet infrastructure.

4. Contextualizing Nigeria’s Cyber Threat and Vulnerability

Nigeria’s cyberspace is characterized by high risk exposure. This is evident in the extent of threat and vulnerability to which the domain is exposed. Prominent sources of cyber threat in Nigeria include terrorist or extremist groups, organized criminal syndicates, and international spies’ networks, corporate insiders, and free-lance hackers (Nigeria, 2014).

The cause and drivers of cyber malaise in Nigeria are systemic and various. According to Nnamani (2016:8), they
“can be attributed to the rising poverty levels, greed (of both perpetrators and sometimes even the victims), easy access to gullible targets by criminals, and lack of adequate legal and regulatory policies to prevent and prosecute the perpetrators....” Economic hardship, accentuated by lack of employment and safety nets, has provided material incentive for criminal indulgence and franchise among the youths (Adesina, 2017). This has given rise to the phenomenon of yahoo-yahoo boys’ who specialize in computer-aided Advanced Fee Fraud [AFF] (Osho & Onoja, 2015, p.121).

Besides the survivalist motivation of cyber criminality, the penchant for ‘easy money’ among the Nigerian youths has also been a veritable culpable factor. The scenario is complicated by the near absence of entrenched cyber governance regime capable of enforcing minimum regulation in the cyber sector. The consequence of this is the prevalence of criminal impunity, which has found expression in the multiplication of cyber scams in the country. Common examples of cyber based scams in Nigeria include Advanced Fee Fraud (otherwise known as ‘419’), Internal Fraud Compromise, Third Party Application Compromise, Identity Theft, Phising Sites, Skimming Rogue Mobile Application, Rogue Merchant, Ransomeware, etc. (CBN, 2015, p.8).

Available data indicate that Nigeria’s cyber vulnerability status has been disturbing. For instance, in 2015, Nigeria suffered an estimated number of 2,175 cyber-attacks, among which 585 were targeted on government websites. Table 1 below is instructive in this regard.

Table 1: Nigeria’s Cyber Vulnerability Status, 2015: Some Facts

<table>
<thead>
<tr>
<th>Fact</th>
<th>Figure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated number of attacks</td>
<td>2,175</td>
</tr>
<tr>
<td>Estimated percentage of people that suffered attacks</td>
<td>14% of 97 million internet users</td>
</tr>
<tr>
<td>Number of government websites that suffered attacks</td>
<td>585</td>
</tr>
<tr>
<td>Nigeria’s global cyber-attack rating</td>
<td>17th most attacked nation of the world</td>
</tr>
</tbody>
</table>


In 2016, Nigeria lost the sum of 550 million to cyber-crime. This record made Nigeria, by far, the worst hit country in terms of cost of cyber-crime. Table 2 below situates this fact in comparative times.
Table 2: Nigeria’s* Cyber-crime Cost (2016) in Comparative Terms

<table>
<thead>
<tr>
<th>Country</th>
<th>Population</th>
<th>GDP</th>
<th>Internet users and subscribers</th>
<th>Estimated cost of cyber-crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>1,185,529,578</td>
<td>USD 2,89T</td>
<td>340,783,342</td>
<td>USD 2 Billion</td>
</tr>
<tr>
<td>Nigeria*</td>
<td>186,879,760*</td>
<td>USD 48,1066B*</td>
<td>97,210,000*</td>
<td>USD 550m*</td>
</tr>
<tr>
<td>Kenya</td>
<td>46,790,758</td>
<td>USD 63,398B</td>
<td>37,716,579</td>
<td>USD 175M</td>
</tr>
<tr>
<td>Tanzania</td>
<td>52,482,726</td>
<td>USD 44,95B</td>
<td>17,263,523</td>
<td>USD 85M</td>
</tr>
<tr>
<td>Ghana</td>
<td>26,908,262</td>
<td>USD 3,786B</td>
<td>19,125,469</td>
<td>USD 50M</td>
</tr>
<tr>
<td>Uganda</td>
<td>38,319,241</td>
<td>26,369B</td>
<td>14,564,660</td>
<td>USD 35M</td>
</tr>
</tbody>
</table>


More recent records indicate that Nigeria’s cyber infamy has persisted. In 2017, for instance, Nigeria’s ranked the third worst country in terms of cyber-crime incidence. By this ignominious record, the country followed the lead of the United Kingdom (1st position) and United States (2nd position) on the global scale. What are the implications of Nigeria’s cyber dis-reputation for national security? It is to this pertinent concern that we now turn.

5. Some Implications of Nigeria’s Cyber Menace for National Security

The first victim of Nigeria’s cyber malaise is the country’s national image and reputation. Nigeria’s notoriety with cyber-crime has, over the years, given the country a negative brand as a fraudulent country (Okoli, 2013). As observed by Osho and Onoja (2015, p.121), “Long term commission of these crimes has left Nigerians and foreigners alike overly cautious to the extent where legitimate interactions of all forms originating in, or concerned with Nigeria and across cyberspace are now characterized with increasing disbelief”.

As observed by Omale and Idom (2016), Nigeria’s global cyber notoriety has made it possible that vital country’s financial documents such as bank cheques and drafts are now being viewed with suspicion in other countries of the world. This means that our financial documents are no longer viable and reliable pieces for international transactions. Also, Nigeria e-mails are nowadays often being viewed with extreme caution by the international community. Even internet communication waves from Nigeria are sometimes blocked by other countries internet gateways. Nigerians are now being generally discriminated upon in the world because of the "yahoo boys" syndrome. According to Idom and Ugal (2016), International Banks now do proper findings and protracted researches on Nigeria financial transactions before clearance often causing delay. For this reason, foreign investors are scared of investing their capital into Nigerian economy. The implication of this is that Nigeria commands only a little credibility by the reckoning of the comity of nations. This jeopardizes the prospects of the country as a business and an investment destination. Little wonder then that Nigeria has fared rather woefully in the recent World Bank’s Ease of Doing Business Rankings. The 2017 report places Nigeria at the bottom of the chart. This is reflected in table 3 below.
Besides negating the prospects of international business and investment, cybercrime has been implicated in communal and sectarian violence in Nigeria. The abuse of the social media in propagating divisive sentiments has often given rise to needless tension and animosity among various social groupings in the country. A case in point is the prevailing farmer-herder conflict in the country where the social media has complicated issues by framing the conflict in terms of ethno-religious agenda (Ibrahim & Dabugat, 2016).

Perhaps, the most critical dimension to the Nigeria’s cyber security challenge is the utilization of the Internet as an avenue for terrorism recruiting and financing. This is done through the solicitation of funding, donations, as well as membership by terrorist organizations. The use of the Internet as a means of ideological indoctrination and radicalization by terrorist syndicates has been one of the dire of counter-terrorism in the contemporary world (Jacobson, 2009). In the case of Nigeria’s experience with Boko Haram insurgency, the Internet has provided the insurgents with a platform for transnational networking with other extremist groups elsewhere in the world.

From the foregoing, it is evident that the Internet has been a major threat to national security in Nigeria. The financial cost of cyber-crimes constitutes a huge economic waste. Beyond the economic waste are critical opportunity costs, such as unfavorable investment and business climate. Added to this are the complications of hate-speech, terrorism financing cum recruiting and human trafficking, whose collateral implications have been inimical to the survival, corporate existence, and sustainability of the nation. To redress this ugly trend, Nigeria has been struggling rather precariously to make good its commitment to improving its cyber security profile as table 4 tends to buttress.

### Table 3: Nigeria’s* Ease of Doing Business Profile (2017) in Comparative Terms

<table>
<thead>
<tr>
<th>Country</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>25</td>
</tr>
<tr>
<td>Rwanda</td>
<td>41</td>
</tr>
<tr>
<td>Kenya</td>
<td>80</td>
</tr>
<tr>
<td>Botswana</td>
<td>81</td>
</tr>
<tr>
<td>South Africa</td>
<td>82</td>
</tr>
<tr>
<td>Nigeria*</td>
<td>145*</td>
</tr>
</tbody>
</table>

In spite of the manifest commitment as indicated in table 4, Nigeria’s cyber security profile has remained the worst in Africa. The country has continued to play a frontline role as a veritable cyber crime origination, transit, and destination. The persistence of cyber crime has been one of the most critical dimensions of the contemporary national security crisis in Nigeria.

6. Conclusion and Recommendation
The contemporary world is fast transforming under the digital order instantiated by the Internet revolution. The phraseology of ‘global village’ is no longer an abstraction. It has been concretized with the spread of the Internet across the world. The global internet renaissance has brought about radical transformation in all spheres of society, breaking the barriers of time and space. On the downside, it has been associated with nefarious activities that negate the security of nations. The virtual un-governability of the global cyberspace has made it a veritable avenue for the perpetration of crimes by the state and non-state actors.

As this paper has observed in the case of Nigeria, the arrival and spread of internet in the country has amounted to a mixed blessing. While this development has been associated with unprecedented innovations that have benefitted the economy, it has equally conduced for the commission of criminal and subversive acts that jeopardize national security. The vulnerability of the Internet to criminality in Nigeria buttresses the vacuum of effective governance of the country’s cyber-space. This highlights the imperative for a pragmatic cyber governance regime capable of regulating the activities of internet operators and users in the interest of national security.

Consequently, the paper recommends a multi-stakeholder governance system whereby the various private, public, national and international authorities in the Cyber sector are synergized into a regime, complex superintended from NITDA by a team of expert technocrats vast in aspects of cyber-criminality such as cybercrime, cyber-terrorism and cyber-espionage. The team will be charged with leveraging and mainstreaming capacity for cyber-vigilantism through research, innovation and technical resourcing. Expert resources generated by the team will deployed in informing and guiding the activities of private, corporate, and governmental stakeholders in their efforts to combat all forms all forms of

Table 4: Nigeria’s* Global Cyber Security Commitment (2017) in Comparative Terms

<table>
<thead>
<tr>
<th>Country</th>
<th>Score</th>
<th>Global Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>0.830</td>
<td>6</td>
</tr>
<tr>
<td>Rwanda</td>
<td>0.602</td>
<td>36</td>
</tr>
<tr>
<td>Kenya</td>
<td>0.574</td>
<td>45</td>
</tr>
<tr>
<td>Nigeria*</td>
<td>0.569*</td>
<td>46*</td>
</tr>
<tr>
<td>Uganda</td>
<td>0.536</td>
<td>50</td>
</tr>
<tr>
<td>South Africa</td>
<td>0.502</td>
<td>58</td>
</tr>
<tr>
<td>Botswana</td>
<td>0.430</td>
<td>69</td>
</tr>
<tr>
<td>Cote d’Ivoire</td>
<td>0.416</td>
<td>74</td>
</tr>
<tr>
<td>Cameroon</td>
<td>0.413</td>
<td>75</td>
</tr>
<tr>
<td>Ghana</td>
<td>0.326</td>
<td>87</td>
</tr>
</tbody>
</table>

Source: Global Cyber Security Index (GCI) 2017, p. 51.
cyber abuse and misappropriation. Meaningful attempt to fight internet-based criminality must recognize the fact that it is an intelligence-driven phenomenon. The anti-graft operatives must possess requisite intellectual and technical capacities to out-smart the “smart guys” who perpetrate such act.

References


Information Technology Development Agency.


