

In view of crimes in Nigeria: Another perspective to functional illiteracy

Adaobi ifeoma ik-Iloanusi & Mbagwu, D. Ugochukwu

Department of Linguistics

Nnamdi Azikiwe University, Awka

Anambra State, Nigeria

Email: ai.ik-iloanusi@unizik.edu.ng/du.mbagwu@unizik.edu.ng

Abstract

Generally speaking, functional illiteracy is a state in which an individual is unable to apply knowledge acquired to solving problems in their immediate environment. This paper deconstructs this definition in view of the rate and dimensions of crimes in Nigeria. It advances the position that functional illiteracy is the choice or failure of an individual to apply skills acquired formally in educational institutions or other training centres to solving problems to the benefits of society but channels or harnesses the capacity accruing from such skills to perpetration of crimes in the society. Currently, Nigeria is experiencing a surge in crimes like drug peddling and trafficking, kidnapping, banditry, terrorism, bunkering, cybercrime, etc. Observations and facts from arrests made in connection with some of the crimes in the country reveal that most of the suspects are considerably educated or well educated. In fact, there are records of crime suspects who are university and other tertiary institution graduates. More so, cybercrime, hacking, phishing, data breach, scam calls, and bugging are technically demanding for an illiterate to deal in. In other words, perpetrators of these crimes are skilled but do not direct such skills to the benefit of their society but to hurt it. Here, they are described as 'literately illiterate', being the redefinition of functional illiteracy as advanced here. Again, subject to this, a redefinition of functional literacy is posited as the ability to translate acquired skills, reading, writing, and computing for the benefit of oneself and one's immediate or larger community. That is, literacy with the absence of an ability to translate acquired skills for the benefit of oneself and others qualifies 'literately illiterate' with a token of meaning that could facilitate a behavioral change in the response of skilled persons to crimes and thereby curbing them.

Keywords: literacy, illiteracy, functional illiteracy, insecurity, Nigeria situation.

Introduction

Literacy simply put is the ability to read, write and understand simple texts. Nickel (2007) corroborates this, 'literacy is the ability to understand, evaluate, use and engage with written texts to participate in society, achieve one's goals, and develop one's knowledge and potential'. He adds that it involves the application of basic knowledge that develops during the whole lifetime, not only during school years. This ability is evidently the controlling mechanism in the development situation of any human society. Absence of it or its inadequacy spells different problems in the society.

Statistics shows that in Africa, percentage of the literate population is very low. And, this is undoubtedly the bane of underdevelopment in the continent. It is true that in recent times some progress has been made. For instance, in 2018, World Bank reports that in Nigeria, the literacy rate of the youths (ages 15-24yrs) has risen to 75.03%. While this is a welcome development in the rate of formal literacy over the past 20 years in the country, the worry is about the older age brackets, which influence economic, social, political, religious, etc events in the country. This situation is the host of the myriad of problems the country is battling with.

The picture above describes that illiteracy is rather a more prevailing and pervasive case in Africa. The implications of this are not far-fetched, poor or absence of employment opportunities, low self-esteem and welfare dependency. These clearly point to negative manifestations such as crimes, which are precursors of insecurity. The explanation of the situation in Africa currently is therefore obvious. However, in this paper, attention is given to functional illiteracy, which has been redefined here for the purpose of accounting for how it is a factor of crimes (especially, those that require technical skill) in

Africa with Nigeria in focus. In the sections that follow, literacy and illiteracy are focused with a view to justifying the redefinition of functional illiteracy in relation to illiteracy.

Overview of literacy and illiteracy

Vágvölgyi et al (2016) comment that functional illiteracy needs better diagnosis, as there is partial evidence that points to the fact that there are no differences between functional illiterates, illiterates and dyslexics. Their findings show that there is need for thorough assessment from the theoretical, empirical and diagnostic perspective. This difficulty in distinguishing functional illiteracy from illiteracy is clearly absent in the relation between literacy and functional literacy. Ayodele and Adedokun (2012) explain that functional literacy does not end with the acquisition of skills, but being able to use those skills to solve problems in daily life. They emphasize that when people are functionally literate, they think on being self-reliant and thus make a living that will lift them above poverty level. In other words, acquisition of basic education without a translation of learnt material into performance for the benefit of one and one's immediate environment captures literacy while corresponding performance or application of the learnt material describes functional literacy. This buttresses the need to factor into the education provided, to equip individuals to respond to learnt material as it demands.

Akpan (2015) believes that illiteracy amongst other social vices like corruption, poor management of resources, and faulty institutional structure are some of the factors responsible for national insecurity. Implicitly, the position here is that illiteracy is a social security threat with a high cause probability for social vices. Omoroge, et al (2021) corroborate this in commenting that the relationship between national security and education is very significant by reference to the persons involved in banditry and acts of terrorism in the Northern Nigeria. The view here is widely held. However, a different perspective is now advanced towards distinguishing between functional illiteracy and illiteracy. Moral consideration characterizes this perspective and the following questions provide insight into the perspective: What is the limit of the inability to read, write and compute? Of course, the inability predicts lack of formal education. What should be the case if the skills are acquired but there is no or a poor or misdirected expression of the skills? The next section attempts at clarifying the scenario projected.

Illiteracy versus functional illiteracy

Illiteracy is the inability to read or write, or the actual perceived state of being uneducated or insufficiently educated. This is evident in Akpan (2015:4), who states that illiteracy is “the inability of an individual to read or write and change behavior to conform to modern norms of the society or the inability of an individual to reason or act civilly and meet with the societal values of his age”. On the other hand, functional illiteracy according to Vagvolgyi et al (2016) is a state in which a person cannot use reading, writing, and calculation skills for his/her own and the community's development. This supports UNESCO (1978) position that a person is functionally illiterate, if they cannot read, write, and understand simple basic statement for effective functioning of his personal and community development. A manifesting projection is that literacy, more appropriately as argued earlier functional literacy, applies to personal and community development but the last question in the preceding section comes now into focus.

There are individuals who have acquired certain skills but for one reason or the other do not deploy the skills to solve their own or immediate community problems. Such skills over time become redundant and the individuals could lose the ability the skills bestowed on them: a kind of illiteracy has emerged. Worse still, there are individuals who after the acquisition of certain skills deploy the skills to undermining their immediate community instead of contributing to its development. What is evident here is that the canonical definitions of literacy or functional literacy do not account for these scenarios. Hence, aligning with the position that illiteracy is the bane of social vices becomes very difficult and if it is anything to go by, then misdirection or vile application of skills is not just illiteracy but functional illiteracy.

From the foregoing, we present ‘functional illiteracy’ as a situation in which an individual chooses or fails to apply skills acquired formally in educational institutions or other training centres to solving problems for the benefits of society but channels or harnesses the capacity accruing from such skills to perpetration of crimes, thereby undermining the development and peace of the society. This scenario is much the case if cybercrimes are in perspective. Beyond this, the coordination that kidnapping, banditry, terrorism, drug peddling, and trafficking require is subject to skills that could hardly demonstrate or exemplify illiteracy or functional illiteracy as originally defined.

Crimes evident of functional illiteracy

Crimes that strongly indicate vile or misdirected application of skills are cybercrimes even though they could go beyond that. As we have argued that the coordination of kidnapping, banditry, terrorism, drug peddling and trafficking could hardly be driven by illiterates. Yes, illiterates could perpetrate such crimes but supervised and controlled by functional literates who have chosen to misdirect their skills, hurt social order and not to build it (functional illiterates). In other words, illiterates are vulnerable to the manipulation of functional illiterates even though this does not rule out cases in which illiterates are involved in crimes all by themselves.

Cybercrimes used here are listed by Baker (2023). They are malware, denial-of-service (DoS), phishing, spoofing, identity-based attacks, code injection attacks, insider threats, DNS tunneling, and IoT-based attacks.

- **Malware:** this is a programme or code created for the purpose of harming a computer, network or server. This term covers such terms as ransomware, Trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking, etc. The reports of network failure and server breakdowns could be better understood and it is for nothing; usually, it is to access systems to collect information or valuable data.
- **Denial-of-service attack:** this an attack in which a surge of requests is created in order to disrupt business operations such as accessing emails, websites, online accounts or other resources connected to a computer or network.
- **Phishing:** this is the use of email, SMS, phone, social media and social engineering techniques with the intent to entice a victim to share private information like passwords, account details or compel the person to download a malicious file to corrupt a computer or phone. Phishing could be broken specifically into phishing, which targets specific individuals or organization with malicious emails for the purpose of stealing sensitive information such as login credentials or attack their system with malware; whaling, a social engineering attack directed at senior or executive employees to steal money, information or gain access to their computers for more control and manipulation; smishing, sending fraudulent text messages designed to make a person share their passwords, usernames and credit or debit card details; and vishing, use of phone calls and voice messages in the name of the representative of a reputable organization to convince a victim to reveal sensitive information like bank details and passwords.
- **Spoofing:** this is a technique of establishing trust with a victim with the intent to engage them and gain access to their systems and devices for extorting them or stealing valuable information from them or installing malware or other harmful software in their systems. Three types of spoofing have been identified, they include domain spoofing, in which someone impersonates a known business or uses a fake website or email domain to win the trust of victims and by that means swindle them; e-mail spoofing, which involves the use of emails with malicious link or attachment to hack into victims’ systems or crash them; and ARP spoofing, a technique deployed to make a victim send a message to a hacker by means of which the hacker gains access to the victim’s devices communications and sensitive data.
- **Identity-based attacks:** fraudulent acquisition of a valid user’s credentials and deployment with which to defraud the person or persons connected with them. There are different shades of kerberoasting, man-in-the-middle (MITM) attack, pass-the-hash attack, silver ticket attack, credential stuffing, password spraying, and brute force attacks.
- **Code injection attacks:** this involves the injection of malicious codes a vulnerable computer or network for the purpose of changing its course of action. Three types are common, SQL

injection, which targets at altering, stealing or erasing an application's database; cross-site scripting (XSS), this involves injecting a code into a website, which infects script in a user's web browser, enabling the attacker to steal sensitive information or impersonate the victim; and malvertising, which involves the breaching of a third party server to make a way for a malicious code to be injected within a display ad or some other element such as banner ad copy, creative image imagery or video content by which a malware or adware is installed in a user's computer once it is clicked.

- Supply chain attack: this could be software supply chain attack, which involves injecting a malicious code into an application in order to infect all users of an app or hardware supply chain attack, which compromises the physical components of a system for the same purpose.
- Insider threats: this points to cybercrimes occasioned or perpetrated by internal actors such current or former employees, who deploy passwords and credentials of organization they are connected with to access the network of the organization to steal sensitive data and other valuable resources including fund.
- DNS tunneling: this involves compromising a domain name system to bypass traditional security measures to transmit data and code within a network. In other words, the DNS is targeted and once infected, a hacker gains access to command and control activities of the owner of the DNS.
- IoT-based attack: this works at compromising connected devices, Internet of Things (IoT) to assume control of the devices with the intent to steal data or defraud victims. It could also be applied to take over control of a network to launch DoS (Denial of Service) or DDoS (Distributed Denial of Service) attacks.

A critical analysis or consideration of the crimes mentioned here proves one thing; they are expressions of skills formally acquired and such skills require foundational literacy. In other words, no illiterate could possibly engage in or execute any of the crimes. Again, it is more obvious that no one signs up to train to perpetrate such crimes. That is, there are no training institutions or setups dedicated to training the criminals. If there are, they must be secret institutions that might be difficult to access. Even with this scenario, the state of being unable to read, write and compute could not leverage anyone to acquire the skills. Evidently therefore, it is more likely to conclude to what exists as a misdirection or vile application of skills acquired to solve problems to undermine a social system. While much argument might not be advanced against this conclusion, reference to crimes that lack the technicalities involved in cybercrimes could surface strongly, for instance, banditry, kidnapping, terrorism, etc. Reports of arrests in different parts of the country have pictured many with School certificate and other qualifications including tertiary qualifications rule out illiteracy as the bane of the crimes. Akpan (2015) and many others who finger illiteracy as a crime factor could therefore be wrong.

There is a claim of high illiteracy in Northern Nigeria, which is factored into accounting for rate of banditry in the area. This is not agreeable if literacy is applied beyond reading, writing and computing in English. People could be literate in their local languages or others such as Arabic, Kiswahili, etc: many who are categorized as illiterate because they could not read, write and compute in English could be literate after all. The bane of crime in Nigeria is hardly illiteracy being that there are many illiterate Nigerians who are making honest living in the informal sector contributing to the economic stability of the country. And, there is evidence of many literate persons who are engaged in crime. Would by the evidence a conclusion of literacy being a factor of crime be drawn? No. This calls for a redefinition of literacy and illiteracy, and functional illiteracy and functional literacy.

Conclusion

A distinction has been made between illiteracy and functional illiteracy: while illiteracy is the absence of the ability to read, write and compute, functional illiteracy is the inability to apply such skills to personal or community development. With escalation of criminal activities in Nigeria, many have argued and accepted it to be that this state is the bane of the activities. This conclusion motivates the position as advanced here. By considering the basic views about literacy/illiteracy and illiteracy/functional illiteracy and following a moral perspective, a redefinition of functional illiteracy

is proposed, as a situation in which an individual chooses or fails to apply skills acquired formally in educational institutions or other training centres to solving problems for the benefits of society but channels or harnesses the capacity accruing from such skills to perpetration of crimes, thereby undermining the development and peace of the society.

To prove the redefinition, cybercrimes have been used. Evidently, no cybercrime could be perpetrated with the absence of the ability to read, write and compute or the inability to deploy such skills to personal or community development. More so, reports on arrests of criminals of other categories do not specify more illiterates as perpetrators. There is a record of many graduates of tertiary institutions who have been convicted for one crime or the other. The conclusion of illiteracy or functional illiteracy being the bane of crimes is therefore irregular with the existing facts about crime and criminals. Besides, some persons described as illiterate could be literate in their local languages or any other languages. For instance, the claim that there is high illiteracy in Northern Nigeria is based on the evident illiteracy in English but the truth is that there is considerable literacy in Hausa and Arabic in the area. The coordination of banditry and insurgency accounts for this.

Considering other crimes like money laundering, diversion of public fund by ‘public office holders’ and bunkering (notice the emphasis on public office holders), one could hardly think of illiteracy or functional illiteracy. The point here is that the factor of crime is not anything connected with illiteracy or literacy. As has been mentioned, there are many illiterates in the informal sector of the economy contributing to the economic development of the country as well as literates who are making honest living while contributing to the growth and development of the country; and, literates and illiterates who have been found to commit crimes. For a redirection, a redefinition of literacy/functional literacy is also required to initiate a consciousness drive in individuals about the qualification of a literate person, which must include translation of acquired skills into self and community development, more particularly, functional literacy is the ability to translate acquired skills, reading, writing and computing to the benefit of oneself and one’s immediate or larger community. The clear implication of this is that many described literate could be functionally illiterate and establishing this order would definitely promote consciousness that could forestall any kind of misdirection or vile application of any literacy-driven acquired skills.

References

- Akpan, D.A (2015). Youth’s Unemployment and Illiteracy: Impact on National Security, the Nigerian Experience. *International Journal of Arts and Humanities (IJAH)* (vol.4 (2), s/no14.)
- Ayodele, J.B and Adedokun, M.O (2012). Towards Achieving Functional Adult Literacy in Nigeria. *European Scientific Journal*, ESJ, 8(5).
- Baker, K. 2023. 10 most common types of cyber-attacks. Retrieved 14-06-2023 from www.crowdstrike.com.
- Nickel, S. (2007). Family-orientated basic education in the social space as a key-strategy for extended participation in literacy. In A. Grotlu“schen & A. Linde (Eds.), *Literality, Grundbildung oder Lesekompetenz? Beitr“ge zu einer TheoriePraxis-Diskussion* (pp. 182–192). Mu“nster: Waxmann.
- Omoroje, S.D.O, Egbule, P.O and Emuebie, J.E (2021). Achieving National Security in Nigeria through Education. <http://dx.doi.org/10.4314/ujah.v21i4.8>
- UNESCO (1978). Records of the General Conference. 20th Session Vol. 1 Paris: UNESCO.
- V“g“v“lgyi R, Coldea A, Dresler T, Schrader J, Nuerk HC. A Review about Functional Illiteracy: Definition, Cognitive, Linguistic, and Numerical Aspects. *Front Psychol*. 2016 Nov 10;7:1617. doi: 10.3389/fpsyg.2016.01617. PMID: 27891100; PMCID: PMC5102880.