https://doi.org/10.52326/jes.utm.2022.29(4).15
UDC 004.056.5

REMOTE SURVEILLANCE: A MEANS OF INTELLIGENCE GATHERING FOR MINIMIZING SECURITY CHALLENGES IN NIGERIA

Anas Shehu [1*], ORCID: 0000-0002-5307-1457,
Hadiza Aliyu Kangiwa [1], ORCID: 0000-0002-7363-9353,
Abubakar Sani [2], ORCID: 0000-0001-9616-0647

[1] *Department of Computer Science, Kebbi State Polytechnic Dakin-gari, Dakin-gari, 862106, Nigeria.*
[2] *Department of Computer Science, Yusuf Maitama Sule University, Kano, 700214, Nigeria.*
*Corresponding author: Anas Shehu, *anasshehu8@gmail.com*

Received: 10. 28. 2022
Accepted: 12. 02. 2022

Abstract. Nowadays, national security issues are increasing day by day in most countries. A multitude of measures to reduce the challenges have been presented and even implemented by many authors, but without exhaustive results. The use of computers and sophisticated IT tools by the terrorist group, increasing number of citizens, lack of social amenities and other factors have made some of them inadequate enough to control the problems in Nigeria. The purpose of this paper is to highlight national security challenges in Nigeria and how security oversight is operated. To achieve this, the authors analyze available secondary data, investigating national security modus operandi and presenting the general concept of surveillance. Related works were also investigated for discussion. Remote surveillance, wiretapping, geospatial intelligence and a consolidated national database are proposed to achieve digital intelligence collection for insecurity management.

Keywords: *geospatial intelligence, national database, national security, lawful interception, soft wiretapping, SIM card.*

Rezumat. În zilele noastre, problemele de securitate națională cresc zi de zi în majoritatea țărilor. O multitudine de măsuri pentru a reduce provocările au fost prezentate și chiar implementate de mulți autori, dar fără rezultate excaustive. Utilizarea de computere și instrumente sofisticate IT de către grupul terorist, creșterea numărului de cetățeni, lipsa de facilități sociale și alți factori au făcut ca unele dintre ele să fie suficient de inadecvate pentru a controla problemele din Nigeria. Scopul acestei lucrări este de a evidenția provocările de securitate națională din Nigeria și modul în care este operată supravegherea securității. Pentru a atinge acest scop, autorii efectuează analiza datelor secundare la dispoziție, investigând modus operandi de securitate națională și prezentarea conceptului general de supraveghere. Au fost investigate și lucrări conexe pentru discuții. Pentru a realiza colectarea de informații digitale în vederea gestionării insecurității, se propune supravegherea de la distanță, interceptările telefonice, informațiile geospațiale și o bază de date națională consolidată.

Cuvinte cheie: *informații geospațiale, baza de date națională, securitate națională, interceptare legală, interceptare soft, cartelă SIM.*

1. Introduction

Security is a feeling of safety, protection, and relative freedom [1]. This security is always the number one priority according to Maslow's order of needs besides psychology and as such, each nation's responsibility is to provide its citizen security. And has become a basic necessity of human beings and society [2].

Any security threats are known as security challenges [3]. The rate at which security challenges are progressing in countries of the world is ubiquitous, Nigeria as a sovereign nation will not be exempted. Many Nigerians will agree to the fact that many disparate security mechanisms vis-à-vis human and technological were suggested and even implemented to minimize the menace, but to no avail; due to its pervasive nature and the huge threats it poses to human lives and material belongings. The aforesaid proposal and strategies suggested by previous writers are insufficient enough, and therefore; it has to call need for other means and strategies to curb it.

The notion of insecurity may be seen as subjective depending on an individual defining it based on a situation and particular place. But, two things might lead to its definition and meaning. 1. *Public upheaval* 2. *Threat to peace* [4]. Violation of state criminal law can destroy human and other resources leading to human abduction, murder, suicide bombing, armed robbery, armed banditry and so forth [5]. These criminal activities that cause insecurity are engaged with the aid of tools of information and communication technology such as mobile phones, the internet, software, and the like [6].

Additionally, these security challenges are facing Nigeria for more than two decades. Recent among them are kidnapping, banditry, and herdsmen/farmers clashes [7]. Though their root causes are not far from politics, sectional agitations, ethnic & religious crises, militias, boundary disputes, cultism, criminality, and organized crimes" [8].

Technology has revolutionized how humans interact and communicate day by day. This revolution has evolved the world and made it a global village where humans pass messages - text, audio, and video comfortably from any angle wirelessly. Because of the pervasive nature of technology, criminals, and terror groups leverage this technology for national insecurity.

Therefore, a plethora of modern technological means was suggested by researchers to minimize the vices, that include human policing, *close circuit television* (CCTV) cameras, Data mining, and biometric-based system. They remain insufficient, taking cognizance of Nigeria's increased number of citizens and other factors.

Therefore, there is a need for cutting-edge technological ways of digital intelligence gathering and analysis that will match the challenges. Consequently, a strategy of *digital surveillance* is proposed to detect communication contents, location, time, and other communication metadata of communicants—citizens communicating over telecommunication or social media networks.

2. Contributions

Contributions of this work include a brief overview of Nigeria's national security challenges and how it's currently being operated conventionally. Modern IT-based surveillance for tackling insecurity in Nigeria will be seen as second contribution. The third contribution will cover surveillance concept.

And lastly, the discussion and way forward to Nigeria security community to handling these challenges will be covered.

3. Methodology

In this section, we will present the methodology used in the conduct of this work including analysis of secondary data at our disposal, investigating Nigeria national security modus operandi, presentation of general concept of surveillance, related work and finally, discussions on the way forward towards tackling insecurity in Nigeria.

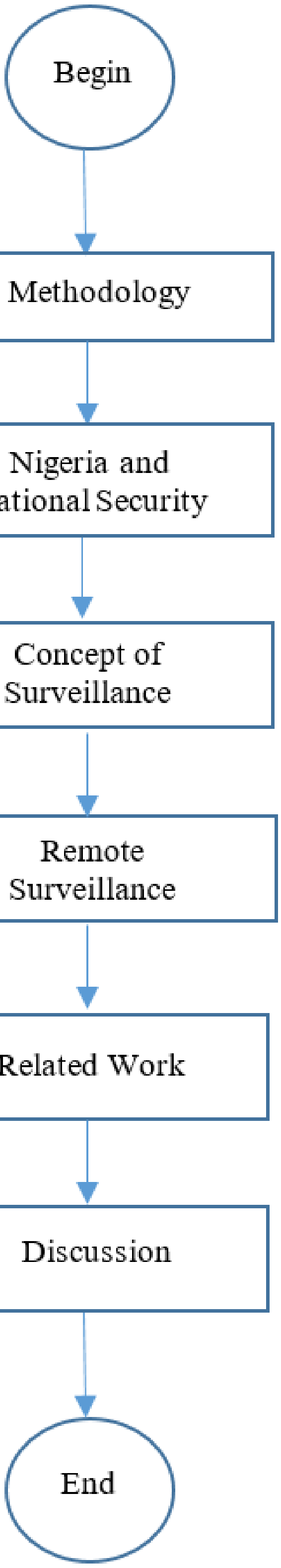

Figure 1. Activity diagram.

4. Nigeria and National Security

Nigeria as a nation is struggling with security challenges—*Southeast*, Indigenous People of Biafra (IPOB), *Northeast*, Boko Haram, *Northwest*, banditry, cattle rustling, kidnapping for ransom, *Southwest*, herdsmen/farmers clash, and *Southsouth* with militancy and oil bunkering. All these could not be possible without the aid of communication technologies such as cell phones and social networks [9]. For instance, the bombing of Super screen TV stations in Lagos in 2009 was coordinated by mobile communications. Another example noted in [10] where Boko Haram sects use computer and other information communication technology (ICT) tools in achieving their objectives on social media platforms and also communicate among themselves. Another famous example was Khalid Almidhar and Nawaf Alhazmi who used mobile networks (though arguable) to coordinate the 9/11 attack in the USA[11]. In Nigeria, cyberspace insecurity activities and actions are taking place with no fear. Nigeria, as of July 2022, has recorded a total number of active SIM cards for cell phone users to be (208, 61,000) making calls and other network-related engagements [12]. With the orthodox security architecture in Nigeria [13], it is impossible to track down and acquire sufficient intelligence in large numbers. To this end, the country's security agencies have at their disposal abundant sources of intelligence gathering—digital devices owned by individuals and internet facility. But, only if Nigerian security abolishes traditional and paper-based security operations and information sharing [14] and embraces modern IT equipment blended with our proposal for systematic and efficient adoption. That could only be the alpha and omega solutions to modern security issues that are going digital day by day.

5. Concept of Surveillance

Surveillance is legal if the government has lawful facts to do it without using it as a vehicle of political intimidation or oppression or reducing citizens' autonomy [15]. Surveillance as mentioned in [16] is "monitoring of behaviors, activities or other changing information to influence, manage, directing or protecting people. State surveillance is lawful when undertaken for legitimate means [15] as technology permeates our daily lifestyle such as in education, transactions, manufacturing, and production, defense, etc., coupled with the digitization of many activities, items, and events indicating individuals produce a significant amount of communication data. These communication data produce an output report of one's movement over time which, in turn, becomes an integral part of the nation's surveillance. Additionally, electronic surveillance gives an idea of what communicants are saying or planning. The majority of foreign governments at the national level embrace digital surveillance because the vast volume of communications moving over the internet is beyond human understanding. The nations are the United State of America [16], the United Kingdom [17], Australia, China [18], and Bangladesh which avert insecurity challenges that going digital and moving over communication networks within society. Government surveillance programs include *landlines, cell phones, mobile devices—tablets, laptop computers, online communications, search engine queries, social media,* and the like [16]. Through this surveillance, intelligence would be deduced and analyzed for further actions. As noted in [19] "*intelligence*" are series of actions and policies observed by any nation to forestall internal/ external threats to its territories, economy, and stability. The authors in [2] Argue that intelligence is a cluster of people and organizations that carry-out missions of collections and analysis, counterintelligence, and covert action. With modern information and communication technology, executing digital intelligence is simpler and, allows joining together communication data that gives a big and comprehensive picture of an individual's communication pattern and behaviors that point to threats to national security [16]. Consequently, UK intelligence & security services were reported to have used the bulk communication data for citizen protection of human rights—security. Finally, this special information gained is what provides a state of the nation, organization, or individual basis to progress its action plan toward securing the country and other individuals.

6. Remote Surveillance

6.1. Wiretapping

National security agency (NSA) via their ex-contractor was reported to have said that NSA has been collecting US citizen's calls logged in greater number. And this called for the interpretation of some sections of the patriot Act [20]. The act was implemented in full capacity in the United State of America and also inspired intelligence gathering in various means [21]. The act provides legal and constitutional backing for forestalling terrorist acts and maintaining the security of the nation. Wiretapping was one of the techniques employed by the US intelligence community for call logs and other things. Wiretapping is a way of interception and listening to communication over a network without the consent of communicants [22].

The act of interrupting and taking total control of oral and electronic communication media is also called wiretapping [23]. Lawful wiretapping is practical in every democratic state [24] the patriot act bill might be activated or implemented in Nigeria towards achieving maximum security via eavesdropping. Couple with other plethora of laws/acts by Nigerian government which provide lawful interception and surveillance such as: *Lawful Interception of Communication Regulations* (preventing, investigating and protecting crime), *Cybercrime Act 2015* (warrant to search data deposited in computer or network and to apply any technology to decode, decrypt messages), *Part V of Mutual Assistance in Criminal Matters Act 2019* (for surveillance, interceptions of communications and postal items), *Terrorism Prevention Amendment Act 2013* (power to intercept communications to forestall act of terrorisms and offences), *Nigerian Section 147 of Communication Commission Act 2003* (provides capability to intercept digital communication [25] Nigeria security agencies are obligated to launch the desired eavesdropping gadgets and software to intrude all cell phone network communications of all callers or suspected callers for state security (if at all the SIM cards registration database is active and running).

Intercepting mobile phone calls is much easier because its signals are on the air. It needs only unwired devices of interception [26]. As noted in [27] when insecurity issues arise, there is a significant rise in domestic and international surveillance which call the use of wiretapping. But as cited by the aforementioned authors, the reverse is the case in Nigeria. Thus, activating laws/bills is essential for interrupting or hijacking cell phone communication for state security. This proves to be more probable and less difficult than on landline conversation. The most suitable wiretapping is *soft wiretapping,* where information over communication lines on the ply on phone devices is being studied. Its implementation is on network provider's equipment [28] and is more covert, user-friendly and inexpensive [29]. It is a common culture of intelligence agencies, larger organizations, and the black box in a developed country [30]. A research conducted by [31] proved that 96% of intercepted communications display and present location data to intelligence communities. For instance, in 2010, the USA army succeeded in tracking down Abu Ahmad al-Kuwaiti who was a courier service provider working for Osama bin Laden. And this led to the death of Bin Laden in a city called Abbottabad, Pakistan [32]. Intelligence communities are always on alert for suspicious conversations, that is when they will access relevant wiretapping systems for location information to further their actions. As pointed out by Nigerian Communication Commission Act 2003, the Nigeria government could be made it necessary for all mobile network providers working in the country to install and activate wiretap capability network (if not installed) as stated in Nigerian Communication Commission Regulations 2011, Nigerian Communication Commission Regulations 2019 and the USA Communications Assistance for Law Enforcement Act (CALEA) 1994 [32].

As reported in [15,25], the Nigerian government procured surveillance technologies from Israel in 2013, and also collaborated the same year with Firm Circle - a telecom Spy Company; to spy on political opposition in Nigeria. These revelations of surveillance acquisitions and domestic laws/acts in place, plus witnessing a high increase in security challenges; indicated little or no application of wiretapping by security agencies for state security. Even if wiretapping exist in Nigeria then, is for tracking the opposition as noted in [25]. Nigerian security community can choose to adopt one of these or some combinations of *soft wiretapping, hard wiretapping, and* use of *active* and *passive devices* for its covert intelligence operations. Both active and passive technologies were used sometime in 1995 to fish out notorious hackers.

Wiretap terms

Hard Wiretapping: Physical wire is attached for signal interception.

Soft Wiretapping: Network information is analyzed as it moves on. Is achieved through mobile phone software.

Passive Device: a technology use for intercepting close-range mobile phones signal and that of service provider's networks. It takes advantage of soft encryption or absence of any during signal transmission. This technology is more invisible during its operation.

Active Device: a technology used for interception of communication contents between mobile phones. Takes advantage of the absence of authentication of base station by mobile phone. Is less invisible as they produce telltale light.

6.2. Geospatial Intelligence (GEOINT)

The contemporary world now is seeing a lot of technological changes with rapid phase day in and day out by making us understand what is going on at a particular time in the exact venue. This is only achievable with ICT and, geospatial intelligence is component of it [33]. Geospatial intelligence is the defined as the “exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the earth” [34]. Geospatial intelligence comprises imagery, imagery intelligence, and geospatial information. Imagery, also known as “photograph intelligence” [35], gives thorough analysis of the images in question (whether still picture or full-motion video that was reproduced electronically or by optical means) [34] data to locate, group, and recognize objects or any establishment [36]. GEOINT data is gathered through space-borne, airborne sensors stationed on the ground. GEOINT covers large geographical distance and helps in providing scientific geolocation of the target. Through the air, imagery could be acquired via satellite unmanned aerial vehicles and reconnaissance aircraft. Videos and pictures acquired or posted by terrorist groups will be analyzed for scientific location when blended with geospatial information techniques.

Geospatial intelligence was used to locate the Iraqi terror group training camp which even revealed the timing of the coverage and the camera location. Furthermore, with this geospatial intelligence, the exact place where a United States journalist was executed was spotted after a photo examination was carried out via video posted on social media by the sect [37]. Again, the geolocation of social media users was used by the US intelligence service to map out refugees fleeing Syria [34]. These were and would be achieved when optimum utilization of *Geospatial Technologies* by Nigerian security agencies such as the State Security Service (SSS), Defense Intelligence Agency (DIA), and other security communities is in full force [38] to know the whereabouts of victims kidnapped by bandits for ransom, bandits themselves or Boko haram sect.

For law enforcement agencies to start the war against insecurity without using GEOINT, is as simple as fighting nobody[33]. For the security community to apply imagery intelligence, Geospatial intelligence toolkits should be employed.

6.3. National Database

As in other developed countries such as the US, UK, Germany, Canada, China, and so on, the Nigerian security architecture should have a consolidated database that contains comprehensive information on citizens and foreigners living in the country. It is the same database that will be used to link individuals using wiretap contents or metadata as the case may be and/ or image analysis was done to identify the suspects. The database holds many advantages to the security community by using it to play back on how crime has happened and who was involved. Also to use this data store is like hastening investigation because of available information that can be reached quickly. It is essential to note that developing this data store is simple and easy. Since Nigeria had claimed to have updated the Independent National Electoral Commission (INEC) database, National Identity Management Commission (NIMC) database, National Population Commission (NPC) database, bank database, driver's license and plate number database, SIM card registration database, and so on. Further, an electronic transport system (as a mobile app) should be implemented, plus automatic vehicle plate number systems for vehicle movement in real-time should exist. These disparate data could be integrated and consolidated into the single and robust data warehouse for intelligence analysis and the like.

7. Related Work

This section will present works related to digital surveillance or the application of any ICT tools/systems in observing nation-state security.

Presentations were made by [9] that explain how information and communication technology is used to create unrest and security issues in the country. Also, the same technology could be used to stabilize national security. Though no clearer direction was provided on how to achieve that. The strategy proposed by [39] pointed out the value to be achieved when geospatial intelligence is used to track down the insurgency. Photographs and videos taken from the satellite give much idea on the location of the terrorist camp, the objects spotted in the photograph will also be different from one another base on the type (person for person, sea for sea, and tree for tree, etc.). Global Positioning System (GPS) is one of the emerging technology used in recent times for counter-terrorism [6] which uses triangulation to measure and determine the position, time, and speed of an object at a point attached to the system.

Data mining technology was proposed as a means of discovering notorious personalities, financial movements, unusual patterns, and behavior through intelligence to fight crime-related acts associated with them [39]. The data mining schemes like *Classification* and *Link Analysis* would help to ascertain genuine patterns of information and behaviors which, in the end, meet intelligence objectives. Additionally, activities like phone calls visited places and email contacts could be linked to one another statistically for additional intelligence analysis. In [12] biometrics means were proposed to curb the insecurity in the country. And it is an automated way of fishing out a personality using physical, physiological, or behavioral characteristics through identification and verification. The features to consider in this process are facial features, retina, fingerprint, and iris. [40] Proposed a system that is viable to point out a suspected terrorist under the security watch list during screening in the airport and whose facial features were pre-processed in biometric systems. This system is so profound that it did not label innocent as culprits or the other way round. The contribution in [40], a biometric system based on fingerprint was designed to authenticate personality gaining access to the building with an IP-video surveillance camera connected to it serving as an intelligence vehicle with the capability to report to the terminal any suspicious movement and unwanted gatherings. In the work of [13], digital devices and software were mentioned in the presentation and deployed for usage to Nigerian security agencies but had little or no impact on minimizing the security challenges facing Nigeria. Amongst the technology is: *close circuit television* (CCTV) supposed to be installed in Lagos and Abuja in large numbers but, only a few were installed. *Global Positioning Systems* (GPS) are supposed to be installed in cars, *Pre-Arrival Assessment Reports (PAAR)* for customs operations, *biometric technology, and SIM card registration* for all Nigerians, *Integrated (IPPIS)* and *Bank Verification Number (BVN)*. Though listed some elements militating the successful implementation of these technologies that included 1. Digital divide 2. Insufficient training for security personnel and 3. The dearth of political will.

Presentation of essential use, nature, and analysis of intelligence sources by the US intelligence community were made [34]. In the contribution, sources of intelligence were stated such as Human Intelligence (HUMINT), Geospatial Intelligence (GEOINT), Signal Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), and Open Source Intelligence (OSINT). Detail role of each source and the problems associated—i.e. financial, were elaborated. The composition and designation of some US intelligence communities were also mentioned. In another research conducted by [41], the history of imagery intelligence (IMINT), its origin, and previous applications in world wars I and II were highlighted. Modern-era UAVs and the future of IMINT for the usage of the intelligence community (more specifically military) were discussed. In another work presented by [42] application of information technology via Geographic Information Systems was proposed to tackle crime and insecurity. In the document, the author provides a model where crime can be mapped and located. Finally, hotspot mapping techniques were elaborated on in the report. The work of [43], provide insecurity issues in Nigeria emanating from Niger Delta militancy, kidnapping from South East, Boko haram insurgency rooted in North East, the herdsmen crisis in Benue, and banditry centered in the Northwestern states. However, the author proper technological solution to this menace by employing aerial drones for state surveillance. He however further itemized the functions of some drones for deployment. Another proposal by [44], pointed to security challenges posed by Boko Haram and their application of information and communication technology (ICT) for intelligence gathering and launching mayhems to citizens. The authors noted that ICT gadgets and systems should be used for surveillance and intelligence gathering. Also, a central intelligence unit and development of any single identification means were proposed.

In another work done by [45], techniques were proposed where personnel can intercept wireless communications by sending a signal through the jamming antenna to hear out the transmitting messages. In a similar research by [46] techniques of using a receiver that can divide the message communicated into two—interception and spoofing is used. The technique employed optimizes the eavesdropping rate more than traditional eavesdropping does. New means of checkmating insecurity in public safety networks, national security centers and national databases were among them [47]. The authors also listed some ICT gadgets/means to improve national security architecture. Intelligence gathering, interception of messages, use of geographic information systems, launching fingerprint systems in almost all endeavors, deployment of the crime management systems and so on were also itemized in the report. Furthermore, the research outlined a list of basic technological devices and means to help control insurgency in Nigeria.

The use of big data analytics to analyze social media contents for intelligence gathering by citing free analytics for security agencies to use in the country, Nigeria. Specifically, there are some tips that will aid intelligence community for effective social media analysis[48]. Integration of data modeling with the Geographic Information System (GIS) database for profiling terror group location and predicting the sect pattern of activities for better close observations was proposed in[49]. Research work conducted by [50] proposed the use of a Global Positioning System (GPS) chip by an individual on their body for easy tracking and locating when kidnapped or in danger. Also, issues facing the application of technology in Nigeria's security domain such as insufficient training, dearth of the fund, consolidated national database, and absence of security satellites were expatriated. In another research conducted by[51], weighted linear combination was used on top of geospatial intelligence for identification and fishing out terror groups' location and territory in Sulawesi Province, Indonesia. Among the beauty of their work is using water source, slopes, settlements and land cover as research parameters. On the other hand, [52]made presentation on how geospatial technology could be of help in surveillance and security research within the academia. They stressed how importance it is to acquire such knowledge for proper tracking, mapping and digitizing terrorist actions on crime map. Consequently, GEOINT research group was formed to cover six geological zones in Nigeria with one university in each zone covering the activities, plus the authors base university.

Authors in [53] made presentations as surveyed papers on the applicability of GEOINT by counter-terrorism squads to subduing insecurity. It was reported by many of the respondents that GEOINT has a role to play in conquering terrorism in the country. The work specifically focused on the Boko Haram insurgency between 2015 to 2018. In another work prepared and presented by[54], the history of the US laws mandating legal wiretap was expatriated. Also, wiretapping concepts and a few of its devices were mentioned. The researchers argued the use of wiretapping techniques citing harm caused to US citizens in the process, but; suggested the use of vulnerabilities technological devices to listen to conversations and other digital messages which the US security community are using secretly and in small quantity. Analyzing social network content gathered by its users over time for solving issues of terrorism was proposed by[55]. Examples of how SNA helped mapped out terrorist groups and their networks were stated in detail. The author highlighted two sub-division of SNA - data collectors and modelers. Nigerian government should take hold of information communication technology (ICT) in checkmating insecurity in its bushes, forests, and other terrorist hiding places. There exist national space laws in the country that can be relied on in using drones, helicopters, close circuit television (CCTV), and satellite to guard them which in turn keep an eye on and terrorize criminals [56]. Based on the survey results compiled, they conclusively made recommendations that the Federal Government of Nigeria should fund technology in the security cycle. Train them on modern technology and data analysis. The national database was among the recommendation also. An interesting proposal was made in [57] where, smart objects and surveillance technologies could be fused into one single system for proper monitoring, controlling, and overseeing of citizens' affairs for security and other purposes. It was assumed in the framework that all other security agencies have dedicated system for their affairs, including office of the national security adviser. These systems are then connected to national secured and centralized systems via secured internet connection and pass on data to and fro. However, on one hand, smart objects, GPS, surveillance camera and the like are connected and transmit needed data through a common gateway to national database.

From the literature above, it is evident that none of the author(s) made wider coverage/ proposal of using wiretapping for all incoming and outgoing calls by Nigerian citizens for the sake of intelligence gathering. Also applying geospatial intelligence couple with wiretapping for detecting images and locations of criminals/terrorist and warehouse them in a single data store for analyses and interrogations were not fully addressed. Based on these, we can say that Nigeria security community is operating in a conventional way—human intelligence for tackling insecurity, hence the need for our proposal to Nigeria's security personnel.

8. Discussion

From the above literatures and other submissions, we can observe that some authors suggest application of GPS only for tackling insecurity in Nigeria. Other writers only proposed the use of data mining to fish out the criminals when a correlation was found. For some authors, we can see that their proposal was only for the use of biometric to identify criminal at the gate of domestic or national airport in the country. Other group of papers were based on deploying ICT hardware and software (national database and CCTV) alone for neutralizing insecurity in Nigeria. And finally, some authors suggest the Nigeria security to deploy Ariel drones for surveillance. This proposal was not feasible because all the five satellites belonging to Nigerian government, none is allocated for gaining intelligence [39], so Ariel drones might be difficult. It is important to note that, data mining, CCTV, GPS, GIS, biometric, Ariel drone and national database as independent system alone may not solve Nigeria security issues without having digital intelligence gathering in place, couple with consolidated national database for linking the information and then employ analysis and trigger actions. It is worthy to note that many wars against insecurity were fought with success because of IT-based intelligence facilities [58]. It is equally important to know that counter-terrorism flourishes with the help of digital intelligence in this information age. Nigeria as a nation is and has witnessed security crises which inspired federal government to have pointed it as a reason for surveillance [25]. Hence the need of our proposal.

9. Conclusions

Security is the number one priority of every country to give to its citizen. The need for a suitable and trusted strategy to relax the insecurity issues is timely. Our Remote surveillance proposal only needs Nigeria's espionage/intelligence community to collaborate with mobile phone service providers to access their call record database/ duplicate the contents or mount intelligence devices on their respective towers or apply the two. Nigeria security agencies can also learn from or corroborate with Egypt, Libya, Bahrain, Saudi Arabia, United Arab Emirates, and India to acquire the intelligence technology as them as noted by another author above. To our knowledge, succeeding in this domain of security, a citizen must sacrifice their privacy in exchange for security. Of importance, to keep crimes and insecurity in check in this information age, technology-based techniques should be embraced, deployed, and relax the orthodox methods in use since Nigeria's independence. Since Nigerian government procured surveillance technologies from Israel and also formed a collaboration with a spy company. Then, using physical power by law enforcement agencies might not win the war against insecurity without the acquisition/deploying greater intelligence. In future work, the authors will cover the nitty-gritty of how modern IT-based intelligence-gathering/ surveillance devices function plus their classifications and architecture.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Abdullahi, A.S.; Mukhtar, J.I. Armed Bnaditry as a Security Challenges in Northwestern Nigeria. *African Journal of Sociological and Psychological Studies* 2022, 2, pp. 45-62.
2. Abiodun, T.F.; Oludotun, A.; Chukunyere, N.; Oladejo, A.A. Security Intelligence Cooperation and the Coordinated War on Terror Among Nigeria's Security Agencies: Panacea to Stable National Security. *Global Scientific Journals* 2019, 7, pp. 542-566.
3. Eke, C.C. Terrorism And The Dilemmas Of Combating The Menace In Nigeria,. *International Journal Of Humanities And Social Science* 2013, 3, pp. 1-7.
4. Okeke, G.N. A Legal Approach To Combating Terrorism: Modern Dimension. *Journal Of International Law & Jurisprudence* 2011, 2, pp. 293-303.
5. Gony, A. Red Teaming The Red Team: Utilizing Cyber Espionage To Combat Terrorism. *Journal Of Strategic Security* 2013, 6, pp. 1-9.
6. Akinode, J.L.; Alawode, A.J.; Ojuwo, O.O. Improving National Security Using GPS Tracking System Technology. *African Society for Scientific Research* 2011, pp. 634-645.
7. Emmanuel, A.O.; Eyinnaya, O.L. Critical Thinking in Information Technology and Management for National Security in Nigeria. *Asian Journal of Applied Science and Technology* 2019, 3, pp. 41-52.
8. Okechukuwu, A.T.; Onyekaneze, O.O. Forensics TechnologyDeoxyribonucleic Acid (DNA) Profiling in Security Management and Fight Against Insecurity/Terrorism in Nigeria. *Journal of Humanities and Social Science* 2019, 24, pp. 36-45.
9. Maryam, U.B. Available online: http//:punchng.com (accessed on 12 October 2022).
10. Chinda, F.E.; Shuaibu, A.N.; Dyikuk, J. Information Technology as an Indispensable Security Tool: Nigeria's Boko Haram Sect in Focus. *International Journal of Applied Research and Technology* 2018, 7, pp. 39-51.
11. Hewitt, M. *Wiretapping: A Neccessity for Effectively Combating Terrorism in the 21st Century*. Liberty University, 2008; pp. 1-49.
12. Chima, P.; Joseph, I.S. Adoption of Digital Solutions in Managing Security Challenges of the 21st Century in Nigeria Option for Effective Responses. *Journal of Management Sciences Research* 2022, 2, pp. 334-341.
13. Tanriverdi, H.; Chen, H. Government Digital Surveillance and Citizan's Self-censorship of Technology Use. In *Proceedings of the Thirty ninth International Conference of Information Systems*, San Fransisco, USA, 2018.
14. The Role of Information Technology in Enhancing National Security in Nigeria (2001-2020). *Pinisi Journal of Art, Humanity and Social Studies* 2021, pp. 44-53.
15. Oloyede, R.; Roberts, T.; Mohamed, A.A.; Farahat, M.; mutung'u, g. *Surveillance Law in Africa: A Review of Six Countries*; Brighton, 2021; pp. 2-203.
16. Milanovic, M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Havard International Law Journal* 2015, 56, pp. 81-146.
17. Milward, J.; Peterson, D. China's System of Oppression in Xinjiang: How it Developed and How to Curb it. *Global China: Assessing China's Growing* 2022, pp. 1-25.
18. Eke, G.E.; Okechi, H.A.; Uche-Nwachi, E.O.; Ekeh, L.K. Science-Systems as a Catalyst to Sustainable National Security in Nigeria. *Science World Journal* 2021, 16, 3 pp. 97-401.

19. Richard, H.J.; Don, G. Intelligence And Its Role In Protecting Against Terrorism. *Journal of Strategic Security* 2010, 3, pp. 31-38.
20. Soghoin, C.; Pell, S.K. A Lot More Than A Pen Register, And Less Than A Wiretap: What The StingRay Teaches us About How Congress Should Approach The Reform of Law Enforcement Surveillance Authorities. *Yale Journal of Law & Technology* 2013, 134, pp. 134-171.
21. American Heritage Dictionary. Available online: www.legal-dictionary.thefreedictionary.com/wiretapping (accessed on 12 August 2015).
22. Steven, B. Law.illinois. Available online: http://www.law.illinois.edu/bljournal/post. (accessed on 2 September 2012).
23. Steven, B.M.; Matt, B.; Sandy, C.; Susan, L. Lawful Hacking: Using Existing Vulnerabilities For Wiretapping On The Internet. *Northwestern Journal Of Technology And Intellectual Property* 2014, 12, pp. 1-64.
24. Accountable Wiretapping-or- I Know They Can Hear You Now. *Journal of Computer Security* 2015, 23, pp. 167-195.
25. *Surveillance Law in Africa: A Review of Six Countries*. Institute of Development Studies: Brighton, 2021, pp. 103-131.
26. Pell, K.S.; Soghoian, C. Your Secret Stingrays No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy. *Havrd Journal of Law & Technology* 2014, 28, pp. 1-76.
27. The Correlation Between Wiretapping and Terrorism: A Comparative Analysis of American and European Societal Views on Government Surveillance. *ILSA Journal of International & Comparative Law* 2016, 23, pp. 55-74.
28. Yee, M.J.; Philips, S.; Condon, G.R.; Jones, P.B.; Kao, E.K.; Smith, S.T.; Anderson, C.C.; Waugh, F.R. Network Discovery with Multi-Intelligent Source. *Lincoln Laboratory Journal* 2013, 20, pp. 31-46.
29. Your Secret Stingrays No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy. *Havrd Journal of Law & Technology* 2014, 28, pp. 1-76.
30. Blake, N.C. The Constitution And The NSA Warrantless Wiretapping Program: A Fourth Amendment Violation?? *Yale Journal Of Law And Technology* 2009, pp. 228-259.
31. Surveillance, T. seussbeta.tripod.com. Available online: http:///seussbeta.tripod.com (accessed on 2 September 2015).
32. Ryan, D.; Glenn, G.; Laura, P. firstlook. Available online: "www.firstlook.org (accessed on 13 October 2022).
33. Understanding Geospatial Intelligence and the Challenge of Effective Counter-Terrorism Strategy: A Case Study of Nigeria's Boko Haram Challenge. *Unnes Law Journal* 2020, 6, pp. 163-185.
34. Intelligence Sources in the Process of Collection of Information by the US Intelligence Community, "Security Dimensions", 2019, pp. 82-105.
35. Staff, I.O.S. *Operations Security Intelligence Threat Handbook*. 1996, pp. 1-80.
36. Margaret, Hu. Available online: http://www.washingtonpost.com (accessed on 5 September 2022).
37. Sani, A.; Paki, Z.S.; Hadiza, A.U. Location Information: Another Perspective of Intelligence Gathering for Minimizing Terrorism in Nigeria. *International Journal of Scientific & Engineering Research* 2015, 6.
38. Emenari, S.U. The Application Of Geospatial Intelligence In National Security For Sustainable Development To Combat Terrorism Insurgence In Nigeria. *Journal Of Environmental Science, Toxicology And Food Technology* 2014, 8, pp. 2319-2402.
39. Okonkwo, R.O.; Enem, F.O. Combating Crime And Terrorism Using Data Mining Techniques. In *Proceedings of the Nigeria computer society (NSC): 10 th International conferenc*e, 2011.
40. Akinmosin, A.S.; Yusuf, S.E.; Dada, A.M. Combating Terrorism With Biometric Authentication Using Face Recognition. In *Proceedings of the Nigeria computer society (NSC): 10 th International conference*, 2011.
41. Guide to Imagery Intelligence. *Journal of U.S. Intelligence Studies* 2011, 18, pp. 61-64.
42. Crime Mapping in GIS by Using Hotspot. *SJCMS* 2018, 2, pp. 13-19.
43. Usage of Drones or Unmanned Aerial Vehicles (UAVs) for Effective Aerial Surveillance, Mapping System and Intelligence Gathering in Combating Insecurity in Nigeria. *African Journal of Social Sciences and Humanities Research* 2020, 3, pp. 29-44.
44. Information Technology as an Indispensable Security Tool: Nigeria's Boko Haram Sect in Focus. *International Journal of Applied Research and Technology* 2018, 7, pp. 39-51.
45. Xu, J.; Duan, L.; Zhang, R. Proactive Eavesdropping Via Copgnitive Jamming in Fading Channels. *arXiv* 2017, pp. 1-16.

46. Zeng, Y.; Zhang, R. Wireless Information Surveillance Via Proactive Eavesdropping With Spoofing Relay. In *Proceedings of the 4th IEEE International Conference on Acoustics, Speech and Signal Processing*, Shanghai, China, 2016.
47. Oludare, A.I.; Omolara, O.E.; Umar, A.M.; Kenni, D.V.; Ezenwosu, A.C. Harnessing Information Communication Technology (ICT) in Handling Crime and Terrorism in Nigeria. *Journal of Social Science and Public Politics* 2015, 5, pp. 1-25.
48. Jibril, M.L.; Mohammed, I.A.; Yakubu, A. Social Media Analytics Driven Counterterrorism Tool to Improve Intelligence Gathering Towards Combating Terrorism in Nigeria. *International Journal of Advance Science and Technology* 2017, 107, pp. 33-42.
49. Idhoko, K.E.; Ojaiko, J.C. Integration of Geographic Information Systems (GIS) and Spatial Data Mining Techniques in Fight Against Boko Haram Terrorist in Nigeria. *International Journal of Science and Research* 2015, 4, pp. 1932-1934.
50. Udochukwu, E.; Christian, S.I.; Adebayo, A. The Application of Geospatial Intelligence in National Security for Sustainable Development to Combat Terrorism Insurgence in Nigeria. *Journal of Environmental Science, Toxicology and Food Technology* 2014, 8, pp. 11-16.
51. Utomo, A.M.; Wijayanto, G.N.; Yusfan, M.A.; Wardani, M.; Poniman, A.; Supriyadi, A.A.; Gultom, R.; Martha, S. Geospatial Intelligence Analysis to Support National Defense Interest. In *Proceedings of the 2021 International Conference on Advanced Computer Science and Information Systems*, 2021.
52. Nwachukwu, M.A.; Nwachukwu, J.; Anyanwu, J.; Babatunde, A.; Ekweogu, C.; Nwachukwu, A.N. Geospatial Intelligence Training Concept for Terrorism Surveillance, Nigeria to Infusive Sub-Saharan African Countries. *American Journal of Geosptial Technology* 2022, 1, pp. 44-51.
53. Nte, N.D.; Abdulaziz, A.B.; Uzorka, M. Understanding Geospatial Intelligence and the Challenge of Effective Counter-Terrorism Strategy: A Case Study of Nigeria's Boko Haram Challenge. *Unnes Law Journal* 2020, 6, pp. 163-185.
54. Bellovin, S.M.; Clark, S.; Landan, S. Lawful Hacking: Using Existing Vulenarabilities For Wiretapping on The Interner. *Northwestern Journal of Technology and Intellectual Property* 2014, 12, pp. 1-64.
55. Ressler, S. Social Network Analysis as an Approach to Combat Terrorism: Past, Present and Future Research. *Homeland Security Affairs* 2006, 2, pp. 1-10.
56. Chima, U.H.; Muritala, O.; Elisha, N.C. Harnessing Information and Communication Technology (ICT) For The Management of Ungoverned Spaces in Nigeria: Policy and Strategic Way Out. *International Journal of Development and Management Review* 2020, 15, pp. 17-31.
57. Obodoeze, F.C.; Ozioko, F.E.; Okoye, F.A.; Mba, C.N.; Ozue, T.I.; Ofeogbu, E.O. The Escalating Nigeria National Security Challenge:Smart Objects and Internet-of-Things to The Rescue. *International Journal of Computer Networking and Communication* 2013, 1, pp. 81-94.
58. Michael, H. *Wiretapping: A Necessity For Effectively Combating Terrorism in 21st Century*; liberty university: 2008, pp. 1-49.

Citation: Shehu, A.; Kangiwa, H.A.; Sani, A. Remote surveillance: a means of intelligence gathering for minimizing security challenges in Nigeria. *Journal of Engineering Science* 2022, 29(4), pp. 59-71. https://doi.org/10.52326/jes.utm.2022.29(4).15.

Submission of manuscripts: jes@meridian.utm.md