Artificial Intelligence: The Missing Critical Component in Nigeria's Security Architecture

Falode,[1] Adewunmi, Faseke,[2] Babajimi O. & Ikeanyichukwu,[3] Chukwuma

Abstract

Nigeria, a country of over 200 million people, has been battling with various national security threats since independence in 1960. Some of these core threats include religious extremism, ethnic conflicts, poor public health facilities, porous and poorly-manned borders; and, added to these in the 21st century are terrorism, insurgency, banditry and cybercrimes. This study discovers that the country has deployed various multi-levered measures that are a mix of both traditional defence mechanisms and socio-economic and political measures designed to ensure the survival of the Nigerian state. However, the study discovers that artificial intelligence has zero presence in the country's strategic policy document and doctrine. It argues that Nigeria should follow in the footsteps of countries like the United States, Russia, China, Israel and Estonia that have effectively integrated artificial intelligence into their overall national security architecture. This integration, it discovers, has helped in the creation of a more secured environments in such states. The study concludes by arguing strongly for the integration of artificial intelligence into the Nigerian national security architecture in the areas of cybersecurity, intelligence, defence and internal security.

[1] Adewunmi James Falode, PhD, is Associate Professor of international relations and strategic studies in the Department of History and International Studies, Lagos State University, Lagos, Nigeria.

[2] Babajimi Oladipo Faseke is a lecturer in the Department of History and International Studies, Ajayi Crowther University, Oyo, Oyo State, Nigeria..

[3] Chukwuma Ikeanyichukwu is a graduate of Mass Communication from Lagos State University, Ojo, Lagos.

Keywords: artificial intelligence, cybersecurity, security, Nigeria, architecture

Introduction

Artificial Intelligence (AI), is a relatively recent phenomenon that started in the middle of the 20th century. However, the idea that mechanical statues were capable of wisdom and emotion is as old as antiquity and finds expression in Greek and Egyptian mythologies (McCorduck, 1979). AI has many definitions, but the idea behind it is that machines can develop the capability for intelligence similar to that of humans or even better. Indeed, Babuta et al. (2020) have rightly observed that AI systems can rapidly derive insights from large, disparate datasets and identify connections that would otherwise go unnoticed by human operators. This makes AI a significant tool for the improvement of humans' everyday life. In fact, it is not outlandish to liken AI to electricity, which Thomas Edison had rightly predicted as, "a field of fields (that) holds the secrets which will reorganize the life of the world" (NSCAI, 2021). The Russian President, Vladimir Putin was therefore not exaggerating when he claimed that "whoever becomes the leader in the field (of AI) will rule the world" (Hoadley & Lucas, 2018, p. 1). AI has many uses and can readily be adapted and adopted into different sectors within the society. Countries like the United States of America, Israel and Russia have comprehensively integrated AI systems into every area of their respective states. Infact, AI systems play prominent role in ensuring the overall security architecture of such states. This is apart from the fact that such states now rely extensively to regulate their social, political, and economic lives. For example, Isreal deployed offensive and defensive weapon systems largely controlled by AI systems to counter the various attacks launched against it by Hamas during the latest phase of their confrontation in 2021 (Lappin, 2021).

The United States relies on AI systems to ensure the effective and optimal functioning of its healthcare, financial and energy sectors (Sayler, 2020). The adoption of such AI systems has contributed significantly to the overall security of such states. To be able to use AI systems effectively, there is need to continuously provide adequate and accurate data. Data, in the form of raw information, is the primary material that any AI systems require to function optimally and effectively. The paucity of such data has been a major barrier to the adoption of AI systems technologies in developing countries. Nigeria, being a developing country and with its low internet penetration, has found it difficult to effectively utilize AI systems to address its pressing security challenges. It is the considered opinion of these authors that the effective utilization of AI systems will go a long way to help Nigeria to efficiently and effectively resolve such security challenges like terrorism, banditry, insurgency and economic insufficiency.

Conceptual Clarification: Artificial Intelligence

What exactly does AI mean? Owing to the diverse approaches to research in the field, AI has no universally acceptable definition. One of the earliest definitions came in 1956, the year AI was discovered as a field of science, when John McCarthy defined the term as "the development and use of machines to execute tasks which usually require human intelligence" (Hoadley & Lucas, 2018, p. 5). With the explosion of interest in AI technology during the new millennium, more definitions sprang up. Russell & Norvig (2016), for example, defined the concept as "the use of technology to carry out a task that would typically require human intelligence." Similarly, Bundy (2017) defined AI as the branch of computer science dealing with the reproduction or mimicking of human-level intelligence, self-awareness, knowledge, and thought in computer programmes." Despite the varied definitions and descriptions of AI, one thing is constant, AI aims to replicate human intelligence in machines. AI has been defined by the European Commission (2018, p. 1) as systems that display intentional behaviour through the analysis of their environment and take specific actions, with some degree of autonomy to achieve specified goals. AI-based systems can be purely software-driven, acting in the virtual world (search engines like Google or speech and face recognition software) or embedded in hardware devices (advanced robots or autonomous drones). AI system works on rationality and it achieves this through immersion (perception of the environment via sensors), after which it reasons and tries to modify its environment through actuators (European Commission, 2018, p. 2)

Going by this description, AI has three broad categories. There is the Artificial Narrow Intelligence (or Narrow AI), which refers to algorithms that address specific problems, but can either have limited memory or be reactive (Ajayi, 2020, p. 5). It responds to different stimuli without previous experience, just like the human mind. A second category is known as Artificial General Intelligence (or Deep AI/Strong AI). This category of AI is a machine that can solve any task with its human-level intelligence. Its likeness to humans means Deep AI can discern emotions, needs, thought processes, and beliefs (Ajayi, 2020, p. 5). The third and final category is the Artificial Super Intelligence, which is a hypothetical AI system that does not just understand or mimic human intelligence, but surpasses it (Ajayi, 2020, p. 5). Many experts have predicted that it will take many decades before the field of AI advances to the state of Artificial Super Intelligence. In fact, all current AI fall into the Narrow AI category, which includes social media monitoring tools, drone robots, self-driving cars and so on (Hoadley & Lucas, 2018, p. 2). This is the kind of AI system that this research addresses.

AI in History

The birth of AI research is often traced to 1956 at a workshop held in Dartmouth College (Haenlein and Kaplan, 2020, p. 3). It was at this gathering that Marvin Minsky and John McCarthy coined the term Artificial Intelligence to distinguish the field from related disciplines like cybernetics (Haenlein and Kaplan, 2020, p. 3). By this time, AI had also advanced to the level of solving algebra and even speaking English. Such was the optimism of the age that, by the mid-1960s, the U.S. Department of Defense started funding research into AI very heavily (Russell & Norvig, 2021, pp. 63-79). Unfortunately, the enthusiasm that greeted this new science was not sustained and AI technology began to wane in the

1970s. The 1980s provided a brief period of boom in AI technology. This revival was, however, short-lived as a couple of new additions to the technology were commercially and functionally unsuccessful in the late 1980s. This marked a period of a second hiatus in AI science (Russell & Norvig, 2021, pp. 63-79). The late 1990s and the early 2000s represented yet another period of resurgence in AI technology. The period coincided with breakthroughs in the science, and AI started being used for logistics, data mining, and medical diagnosis, among others (Russell & Norvig, 2003, p. 28). This period witnessed advanced technology in computer games to the extent that computers began defeating human champions in games such as chess.

Anderson (2015) has detailed how changing methods of communication, vis-à-vis information technology, have posed new challenges for intelligence agencies who have to grapple with terrorism and cybercrimes. As such, these challenges call for the development of more sophisticated analytical tools, and AI is likely to inform an important element of this new toolkit. This fact is not lost on developed countries. In the U.S., for example, the 2018 Department of Defense Artificial Intelligence Strategy posits that "the United States, together with its allies and partners, must adopt AI to maintain its strategic position in the world" (BPC, 2020). In fact, the U.S. Department of State AI efforts are being coordinated by an agency established for that purpose, the Join Artificial Intelligence Centre (JAIC) (BPC, 2020, p. 3). Hoadley & Lucas (2018) have indeed documented how AI is an integral part of U.S combats in both Syria and Iraq, with algorithms designed to speed up the target identification process (Hoadley & Lucas, 2018, p. 2). Indeed, U.S is not the on/ly developed country that has tapped into AI for the purpose of national security, China, Russia and the U.K. are nations that infuse AI into their security apparatus. Of a truth AI belongs to the immediate future and countries—whether developed or developing—need incorporate it into their national security fabric, particularly in countries such as Nigeria where insecurity is rife.

Artificial Intelligence and Nigeria

The year 2015 was a landmark in the development of AI worldwide as the number of projects that use AI within Google (now Alphabet) increased to 3,000 projects (Clark, 2015). This development owed much to affordability, which itself is a consequence of a rise in cloud computing infrastructure as well as research tools and datasets (Clark, 2015). This development led AI software developers to expand their presence from the West into developing countries such as Nigeria. *Andela* was the first prominent company AI software developer company to have an operational branch in Nigeria (Odeyemi, 2019). Founded by Ian Carnevale, Iyinoluwa Aboyeji, Jeremy Johnson, and Christina Sass, the company launched operations in Nigeria in 2014, few months before the explosion in AI technology, to help global companies overcome the severe shortage of skilled software developers (Odeyemi, 2019, pp. 2045-2046). It is, in fact, a training company set up to match developers in emerging markets now known as technology hubs with North American companies. With the presence of a company such as Andela, software using algorithms to generate instantaneous credit scores to users in Nigeria started emerging (Strusani & Houngbonon, 2019, p. 5). This represented one of the greatest advancements in Nigeria's financial technology (fintech). An example of such software application is *Branch*, a Nigerian fintech company that was launched in 2015 and started disbursing loans to Nigerians in 2017 (Deloitte, 2019). The company offers microloans to first-time borrowers and customers without bank accounts. Many other examples of such technologies including *Carbon*, *Palmcredit* and *Fairmoney* (Deloitte, 2019). In truth, most AI innovations in Nigeria to date have come in the area of fintech. There is also the adoption of "chatbots," which was an innovation by Nigeria's United Bank for Africa (UBA) when *Ada and Leo* were introduced as customer service touchpoint in 2018 (Ebarafeye, 2019).

It was not until the second decade of the 21st century that Nigeria started tapping into AI technology. By this time, algorithmic improvements and access to large amount of data had further aided the development of AI and guaranteed better accuracy of the technology in the country. "Intelligent personal assistants," which were software agents that could perform tasks for humans based on commands, were incorporated into phones to make them "smartphones" in 2012. Consequently, Nigerians hands-on experience with AI came mainly in the form of the use of smartphones which became popular in the 2010s. By 2018 there had been a proliferation of AI software development companies in Nigeria, with an overwhelming majority of them located in Lagos, Nigeria's commercial capital. Many of these companies have contributed to the development of AI technology, particularly in the financial sector and such contributions have not escaped government notice. The Lagos State Government, for example, is using AI to enforce traffic regulations with the use of Automatic Number Plate Recognition (ANPR) cameras to scan license plates and fine motorists who violate traffic laws (Google, 2019, p. 4). In fact, the vehicle inspection service has revealed that about 13, 750 motorists have been identified through this system in the first quarter of 2019 alone (Google, 2019, p. 4). It must however be noted that Nigeria has failed to integrate the AI systems into its overall security architecture. This is an important considering the fact that the use of AI in its security architecture would have gone a long way in helping the country to effectively tackle overarching existential issues like banditry, terrorism and insurgency.

Nigerian National Security Policy *sans* AI

Nigeria has three important policy documents, National Security Strategy (NSS) (2019), National Counter Terrorism Strategy (NACTEST) (2016) and the National Cybersecurity Policy and Strategy (NCPS) (2021) that were specifically created to guarantee the country's human and state security. There are various security challenge that threaten the existence of the state. Some of the major ones are banditry, kidnapping, armed robbery, insurgency, terrorism, food insecurity, decrepit health sector, flailing economy, cybercrimes and cattle rustling. For instance, Nigeria's cybercrime statistics is high and climbing (Osho & Onoja, 2015, p. 121). Kidnapping, armed banditry and militia activities have become very serious threats to Nigeria's national security, to the extent that they collectively constitute about 40 per cent of incidences of national insecurity in Nigeria. Boko Haram and the Islamic State in West Africa Province (ISWAP) still engage in intermittent attacks on various locations in the Northeast. The effects of these terror campaigns include loss of lives, mass displacements and destruction of properties. In fact, the defeat of ISIS in Syria has been deemed a potential threat to Nigeria as former fighters form the terror group have now moved into the Sahel. To make matters worse, the potential use of disruptive and emerging technologies, AI inclusive, by non-state actors remain a key concern considering growing advances in the field. The U.S. NSCIA (2021, p.2) has warned that state criminals, and terrorists will conduct AI-powered cyber-attacks in the foreseeable future. Countering these security threats will, therefore, require effective intelligence gathering among other things.

Internal security is the statutory duty of a number of security and intelligence agencies in Nigeria. The Joint Intelligence Board (JIB) and Intelligence Community Committee (ICC) work together with the National Crisis Management Centre (NCMC). All of these coordinate intelligence and information analysis required for strategic decision making by the National Security Council. It is also worth mentioning that law enforcement and the criminal justice system are paramount in internal security. These roles are carried out by all security agencies in Nigeria, but principally by three critical institutions: the Nigerian police Force (NPF), the Judiciary and the Nigeria Prison Service (NPS). While not discountenancing the function of the JIB and the ICC, the State Security Services (SSS) is the foremost intelligence agency in international security matters. The Nigerian Police Force (NPF), on the under hand is responsible for crime detection, prevention and general constabulary functions. In response to the prevailing security threats in the country in the past decade, successive Nigerian governments have put in place some policies to stem the tide. For example, in response to the threat posed by terrorism, the Nigerian government under Goodluck Jonathan enacted the Terrorism Prevention Act 2013; and in 2016, during Muhammadu Buhari's tenure, Nigeria developed the National Counter Terrorism Strategy (NACTEST) and established the Counter Terrorism Centre to coordinate the country's national counter-terrorism efforts. In 2017, Nigeria also adopted a policy Framework and National Action Plan for Preventing and Countering Violent Extremism (Falode, 2019).

In fact, in recent years, a number of notable initiatives have been employed in the fight against terrorism. This includes the initiation of programmes to encourage defection from terrorist groups as well as promotion of rehabilitation and reintegration of repentant terrorists. In response to increasing cyber security threats, Nigeria developed the National Cybersecurity Policy and Strategy (NCPS) in 2015 (Falode, 2021b). This gained traction with the subsequent promulgation of the Cybercrimes Act (CPPA) that same year (NCPS, 2021). The Act provides the comprehensive legal framework for cyber security as well as the prohibition and punishment for cybercrimes in Nigeria. Both the NCPS and CPPA, in particular, try to build comprehensive capabilities to protect Critical National Information Infrastructure (CNII) and to mitigate cyber risks. Banditry and kidnapping are still crimes Nigeria's security infrastructure struggle with, and the best done in this regard is the attempt to better equip the NPF in training.

Despite all these efforts, Nigeria has not been able to effectively tackle the various threats. A major factor is the country's over reliance on conventional strategies to resolve security-related challenges in the state. Indeed, the country's three policy documents on how to effectively shield the country from attacks in both physical and cyber realms did not give any critical consideration to the role an AI system could make in ensuring a more secured Nigeria. That the three aforementioned documents fail to mention AI systems show the level that Nigeria accorded emerging technologies in its security architecture. This is unlike what is obtained in the security documents of some other comparable nations like the United States and China that gave prominent role to AI systems in their security architecture (NDS, 2018; DoD, 2020; NIDS, 2020). One should remark at this point that various factor are militating against the adoption and absorption of AI systems into the overall security architecture of Nigeria. It is these factors that are analyzed in the next section.

Challenges of AI Adoption in Nigeria

AI is still in its nascent stages in Nigeria and as such, there are certain challenges affecting full implementation. AI and machine learning are quite complex and intricate. The technicalities involved in harnessing AI demands particular skill set and expertise which is currently lacking in Nigeria. The following are factors militating against the integration of AI systems into Nigeria security architecture: inadequate data and statistical information, dearth of military hardware for possible AI systems integration and lack of ready workforce

Inadequate Data:

Artificial Narrow Intelligence (ANI), the most commonly used AI in existence, uses algorithmic techniques that enable machines to discover patterns and insights from data, and then use the generated information to make informed decisions (Delipetrev, Tsinaraki & Kostic, 2020, pp. 4-5). This is how Apple's Siri and Amazon's Alexa are able to interact with their environment and humans they come into contact with (Gadzala, 2018, p. 2). However, to perform such functions optimally, AI requires large volume of data, usually referred to as "big data" (Gadzala, 2018, p. 2) Machines (AI) analyze this data to learn, make connections and arrive at decisions. Thus, the availability of plenteous and uninterrupted supply of data is key to the successful utilization and integration of AI systems into the security architecture of any state. Herein lies the first challenge to successful AI systems integration into the Nigerian security architecture – dearth of large volume of data. The presence of big data explains why it has been relatively easier for both China and the United States to integrate AI systems into their overall security architecture. For example, successful and targeted drone strikes that the United States Army recorded in Iraq and Syria were only possible because of the inexhaustible supply of real-time data fed into its weapon systems during the war against the

Islamic States (Fisk, Merolla & Ramos, 2019). Although, in 2019, due to the burgeoning menace of the activities of non-state actors like terrorists, bandits and kidnappers, Nigeria mandated a federal agency, National Identity Management Commission (NIMC), to "forcefully" collect the biometric data of its citizen. The aim is to use the collected data to establish a national database of all Nigerian citizens and use the warehoused information to check largescale incidences of kidnapping and banditry in the country (NIMC, 2020).

A related problem is the poor quality of data available. There is no accurate statistical data available on most metrics in Nigeria. For example, Nigeria has not been able to conduct accurate census since independence in 1960. This has affected both short and long-term planning in the country. The country still relies on both the census figure of 2006 and extrapolation to provide an estimate of the total number of people in the country (Ezeah, Iyanda & Nwangwa, 2013, p. 52).

Lack of Military Hardware for Possible AI Integration

Nigeria relies heavily on conventional human-directed weapons in its engagements with non-state actors with the country. Such conventional weapons include tanks and small arms and light weapons like bombs, rifles and machine guns. All these does not involve the use of AI systems. Advanced weapon systems like drones, cruise missiles and robots would have required the use of AI systems. However, despite their suitability to the warfare terrain, especially in the vast Sambisa Forest, the stronghold of Boko Haram in Bornu state, they are non-existent in the military arsenal of the Nigerian army. This is partly due to the cost of purchasing such advanced weapon systems and the lack of qualified engineers to maintain the weapon systems.

Nonexistent Knowledge Base

Successful integration of AI systems into the Nigerian security architecture requires that there should be a ready and continuous pool of both the skillsets needed to generate data and create software. These can be gotten from both the country's educational system and private and public sector partnership in the area of AI research and innovation. However, the educational system that should have been the powerhouse for innovation and research into AI systems and that should have supplied the local manpower need in the areas of software and hardware development had fallen short. The president of Nigeria, Muhammadu Buhari, presented the 2021 budget proposal to the National Assembly on October 2020. Out of N13.08 trillion budgeted for the coming year, N742.5 billion was allotted to education. At just 5.6 percent, this is the lowest allocation since 2011 (Olufemi, 2020). The effect of these were made even more apparent at the height of the lockdown in Nigeria due to the Coronavirus. With schools shut down, some secondary and tertiary institutions transitioned into e-learning. This wasn't without its difficulties though as most tutors are not ICT compliant and also the high cost of ICT infrastructures, as well as the constant erratic power supply that constantly affects all sectors in Nigeria. Strusani & Houngbonon (2019) have explained this in terms of the lack of access to expertise and data, which often discourage private investors from pursuing AI projects in emerging markets. Therefore, scarce AI expertise in developing countries increases the cost of implementing any AI projects in emerging markets.

AI and Nigerian National Security Architecture

Nigeria has four domains—land, air, water and cybersphere-to protect in order to ensure its security. The country's preeminent defence and strategic policy documents spell out specific measures that Nigeria can use to ensure effective protection of the state from malign state and non-state actors. What is missing in these strategic documents are the specific areas that AI systems can be used or integrated into the country's overall security architecture to provide adequate and holistic protection. By using specific and poignant examples from other climes, this section will show that Nigeria can effectively integrate AI systems into its overall security architecture. This study has identified four key areas for AI integration in the Nigerian security sector: cybersecurity, defence, intelligence and internal security.

i. *Defence*—Nigeria has an expansive territorial space that is very difficult to police effectively. Over the years, this has made it easier for non-sate actors like Boko Haram and bandits to embed themselves in pockets of ungoverned spaces within the country. The issue of non-state actors embedding themselves in ungoverned spaces is a problem that is felt in all regions of the federation. To overcome this challenge, in the first instance, the country can use AI systems with hardware such as drones and ground robots to provide active and continuous coverage over large swath of the country. It will also be possible to effectively use such systems for surveillance and reconnaissance. The information provided by these AI-enabled systems will make it possible for the state to carry-out targeted and surgical response to every emerging threats. This will not only save time and money but will further lead to optimal deployment of warfighters to where they will be most effective. Secondly, and crucially, the use of AI ground robots in contested zones in the northeast of Nigeria like Borno state will save lives of warfighters and it will further keep down the cost of deployment. This is because non-state actors in the region, especially Boko Haram and Islamic State West Africa Province (ISWAP), rely heavily on the use of IEDs to cripple and blunt the response and effectiveness of warfighters in the zone (Falode, 2016, pp. 42-47). AI-enabled ground robots could be sent ahead of the main force to act as scout and decoys, and be the first to come into contact with surreptitiously planted IEDs. For example, Israeli army used AI-enabled ground robots in Gaza during the latest phase of its war with Palestinian militants (Sprengel, 2021).

ii. *Intelligence*—AI systems will be particularly suited to intelligence collection and real-time analysis. Copious data now exists Nigeria because of the ubiquitous use of smart phones and the Internet. The rate at which data is churned-out by such activities would have been very difficult for human to process effectively and efficiently. Bu, AI systems can help to quickly show threads that connects data, flag suspicious activity, spot trends, fuse disparate elements of data and anticipate future behaviour. Since all the malign non-state actors in Nigeria make use of either smart devices like phones (bandits and kidnappers) or Internet-enabled technologies like Youtube, Facebook and Twitter (Boko Haram and ISWAP), there exist treasure troves of data that can be mined to better counter the nefarious activities of such groups. Using AI to sieve through these data can help Nigeria to predict the actions of malign non-state actors, responds proactively before attacks are launched, and effectively curtail the spread of violent extremist ideology. China has effectively used such AI systems like Integrated Joint Operations Platform (IJOP) to keep radical extremist at bay within the country (Ding, 2019, pp. 43-46; Feldstein, 2019, pp. 20-21). Importantly, intelligence is the livewire of any successful counterinsurgency and counterterrorism operations (Falode, 2021a). The integration and deployment of AI systems into Nigerian security architecture, especially in the areas of collection and analysis of data, will complement or even eclipse human intelligence (HUMINT) in the contested zones of the northeast.

iii. *Cybersecurity*—Although, Nigeria has devoted considerable efforts to protect the state in cybersphere, the country has failed to deploy and utilize AI as a key plank of its security protocols. The cyber domain plays critical role in every sector of the Nigerian state. Key sectors like financial institutions and oil and gas rely heavily on cyberspace. Realizing the significance of the domain to the overall of the state, Nigeria developed a robust cybersecurity policy and strategic documents to shield the state from the activities of malign state and non-state actors in cybersphere (Falode, 2021b, pp. 553-554). However, the absence of AI tools in the nation's cybersecurity architecture has left the country wide open to deadly and opportunistic attacks in cyberspace. Using AI systems as one of the tools in the country's cybersecurity arsenal will allow the country to respond to breaches faster and make the system to be more resilient in the face of attacks. Importantly, AI tools could be deployed to monitor and flag insidious financial transactions in cyberspace. This point is crucial. Money is the livewire of successful malign activities such as terrorism and transnational crimes. AI tools can be used to monitor financial transactions in real-time, flag suspicious exchanges and cut-off funding to malign non-state actors.

iv. *Internal Security*—AI tools will be particularly suited to border policing in Nigeria. Nigeria has multiple official and unofficial border points. It has been extremely difficult and expensive for the state to effectively man most of the borders. Indeed, illicit goods, especially small arms and light weapons (SALWs) have found their way into the country via some of these poorly manned borders (Falode, 2021c, pp. 411-415). In addition to this, malign non-state actors like bandits, cattle-rustlers, kidnappers and terrorists have successfully infiltrated Nigeria through these borders. To overcome this challenge, Nigeria can use AI tools to complement the efforts of its human security agents. Unmanned aerial vehicles and AI-enabled ground robots can be used to monitor borders through advances in automated surveillance and anomaly detection. AI systems that monitor human emotional expression and behaviour, like those used in China, could aid in recognizing humans that appear nervous or are acting erratically (McKendrick, 2019, p. 13).

Conclusion

Nigeria has four important domains - land, air, sea and cyberspace - to protect in order to ensure the existential survival of the state. In the 21st century, the country has had to confront simultaneous threats from three out these four domains. The major threats are terrorism, insurgency, trans-border crimes, kidnapping, banditry and piracy. These threats have severely challenged the ability of security agencies to respond proactively and effectively to the defence of the state. To protect Nigeria in these critical domains, and to check the activities of malign non-state actors that threatens its existence, Nigeria has relied on conventional counter measures. These measures include the use of ground forces, police, SALWs and HUMINT. However, all these have failed to provide holistic and effective security shield that the country sorely needed. In order to make the nation's security more effective and strategic, this work has suggested the integration of AI tools into the country's security architecture. The work identifies key areas like cybersecurity, intelligence and defence for AI integration and deployment. With the present multi-modal threats that confronts the country in different arenas, AI systems integration and deployment into Nigeria's security architecture will save money, time and countless lives.

REFERENCES

Adegbami, A. (2013). Insecurity: A threat to human existence and economic development in Nigeria. *Public Policy and Administration Research,* 3(6), 8-13. https://www.iiste.org/Journals/index.php/PPAR/article/view/6348

Ajayi, J. (2020, April 12). Artificial Intelligence in the Nigerian legal industry: A threat or an opportunity? https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3574324

Anderson, D. (2015). A question of trust: Report of the investigatory powers review. Independent Reviewer of Terrorism Legislations, United Kingdom. https://terrorismlegislationreviewer.independent.gov.uk/wpcontent/uploads/2015/06/I PR-Report-Web-Accessible1.pdf

Babuta, A., Oswald, M., & Janjeva, A. (2020, April). Artificial intelligence and UK national security. RUSI Occasional Paper. Royal United Services Institute for Defence and Security Studies. https://rusi.org/exploreourresearch/publications/occasionalpapers/artificial-intelligence-and-uk-national-security-policy-considerations

Bipartisan Policy Centre (BPC). (2020). Artificial Intelligence and National Security. Washington D.C: Centre for Security and Emerging Technology. https://bipartisanpoli cy.org/report/ai-national-security/

Bundy, A. (2017). Preparing for the future of artificial intelligence. *AI and Society*, 38, 285-287. https://link.springer.com/article/10.1007/s00146-016-0685-0

Clark, J. (2015, December 8). Why 2015 Was a Breakthrough Year in Artificial Intelligence. Bloomberg. https://www.bloomberg.com/news/articles/2015-12-08/why-2015-was-a- breakthrough-year-in-artificial-intelligence

Counter Terrorism Centre. (2020, March 8). Nigerian Government Presents Policy Framework and National Action Plan for Preventing and Countering Violent Extremism to Members of the Public. https://ctc.gov.ng/nigerian-government- presents-policy-framework-and-national-action-plan-for-preventing-and- countering-violent-extremism-to-members-of-thepublic/

Defense Budget Overview (DBO). (2020, May 13). Defense budget overview: Irreversible implementation of the national defense strategy. Office of the Under Secretary of Defense Comptroller/Chief Financial Officer. https://comptroller.defense.gov/Portals/ 45/Documents/defbudget/fy2021/fy2021_Bud get_Request_Overview_Book.pdf

Delipetrev, B., Tsinaraki, C, & Kostic, U. (2020). AI watch. Historical evolution of artificial intelligence. European Commission Joint Research Centre. doi:10.2760/801580, JRC120469

Deloitte. (2019). Fintech in Nigeria and the women who lead. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/financial-services/ng-fintech-in-Nigeria-and-the-women-who-lead-29032019.pdf

Ding, J. (2019). The interests behind China's artificial intelligence dream. In N. D. Wright (Ed.), *Artificial intelligence, China, Russia and the global order* (43-46). Air University Press. https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161 _wright_artificial_intelligence_china_russia_and_the_glob al_order.pdf

Ebarafeye, J. (2019, August 31). ADA meets Leo: 2 Nigerian banks introduces social media chatbots. The Xplorion. https://thexplorion.com/nigerian-banks-social-media- chatbots/

Egbefo, D. (2014). Internal Security Crisis in Nigeria: Causes, Types, Effects and Solutions. *International Journal of Arts and Humanities,* 177-195.

European Commission. (2018). A definition of AI: Main capabilities and scientific disciplines. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai _18_december_1.pdf

Ezeah, P., Iyanda, C., & Nwangwu, C. (2013, November - December). Challenges of national population census and sustainable development in Nigeria: A theoretical exposition. *IOSR Journal of Humanities and Social Science*, 1, pp. 5056. http://eprints.gouni.edu .ng/2604/1/my%20article%20with%20 ezeah%20and%20chuks.pdf

Falode, J. A. (2016). The nature of Nigeria's Boko Haram war, 2010-2015: A strategic analysis. *Perspective on Terrorism*, 10(1). https://www.universiteitleiden.nl/binaries/c ontent/assets/customsites/perspectives-on-terrorism/2016/005-the-nature-of-nigeria-s-boko-haram-war-2010-2015-a-strategic-analysis.pdf.

Falode, J. A. (2019). Hybrid doctrine: The grand strategy for counterinsurgency and counterterrorism operations in Nigeria. *Defence Against Terrorism Review (DATR*), 11, 18-21. https://www.tmmm.tsk.tr/publication/datr/volumes/Datr_Vol.11.pdf

Falode, J. A. (2021a). Cybersecurity policy in Nigeria: A tool for national security and economic prosperity. In S. N. Romaniuk & M. Manjikian (Eds.), *Routledge companion to global cyber security strategy* (553-563). Routledge.

Falode, J. A. (2021b). Guns, arms trade and transnational crime in Africa. In U. A. Tar & C. P. Onwurah (Eds.), *The Palgrave handbook of small arms and conflicts in Africa* (411- 425). Sringer Nature. https://doi.org/10.1007/978-3-030-62183-4_20

Fedstein, S. (2019, September). The global expansion of AI surveillance. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP- Feldstein-AISurveillance_final1.pdf

Fisk, K., Merolla, J. L., & Ramos, J. M. (2019). Emotions, terrorist threat, and drones: Anger drives support for drone strikes. *Journal of Conflict resolution*, 63(4), 976-1000. https://journals.sagepub.com/doi/pdf/10.1177/0022002718770522

Gadzala, A. (2018, November 14). Coming to life: Artificial intelligence in Africa. Atlantic Council, Africa Center. https://www.atlanticcouncil.org/in-depth-research- reports/issue-brief/coming-to-life-artificial-intelligence-in-africa/

Google. (2019). AI in Nigeria. Google whitepaper. https://research.google/pubs/pub48985.pdf

Haenlein, M., & Kaplan, A. (2020). A brief history of artificial intelligence: On the past present and future of artificial intelligence. California Management Review, 61(4), 1- 10. https://doi.org/10.1177%2F0008125619864925.

Hoadley, D. S., & Lucas, N. J. (2018). Artificial intelligence and national security. Congressional Research Service. https://fas.org/sgp/crs/natsec/R45178.pdf

Lappin, Y. (2021). How Israel is adapting to the growing threats of terror armies. BESA Perspective, The Begin-Sadat Center for Strategic Studies. https://besacenter.org/wp- content/uploads/2021/01/1882-How-Israel-Adapts-Growing-Terror-Threat-Lappin- final.pdf

McCorduck, P. (1979). *Machines Who Think*. A. K. Peters Ltd.

McKendrick, K. (2019, August). Artificial intelligence: Prediction and counterterrorism. Chatam House. https://www.chathamhouse.org/sites/default/files/2019-08-07- AICounterterrorism.pdf

National Counter Terrorism Strategy (NACTEST). (2016). National Counter Terrorism Strategy (NACTEST), 2016. https://ctc.gov.ng/national-counter-terrorism-strategy- 2016/

National Cybersecurity Policy and Strategy (NCPS). (2021, February). National Cybersecurity and Strategy, 2021. Federal Republic of Nigeria. http://ctc.gov.ng/wp- content/uploads/2021/02/national-cybersecurity-policy-and-strategy-2021_e-copy_24223825.pdf

National Defense Strategy (NDS). (2018). Summary of the 2018 national defense strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018 -National-Defense-Strategy- Summary.pdf

National Identity Management Commission (NIMC). (2020). National Identity management Commission Privacy Policy. https://nimc.gov.ng/docs/NIMC_privacy_policy.pdf

National Institute for Defense Studies (NIDS). (2020). NIDS China Security Report, 2021: China's Military Strategy in the New Era. National Institute for Defense Studies, Japan. http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_ A01.pdf

National Security Commission on Artificial Intelligence (NSCAI). (2021). Final Report: National Security Commission on Artificial Intelligence. https://www.nscai.gov/wp- content/uploads/2021/03/Full-Report-Digital-1.pdf

National Security Strategy (NSS). (2019). National Security Strategy, December, 2019. Federal Republic of Nigeria. https://ctc.gov.ng/wp-content/uploads/2020/03/onsa- updated.pdf

Odeyemi, T. O. (2019). Global digital capitalism: Mark Zuckerberg in Lagos and the political economy of Facebook in Africa. *International Journal of Communication*, 13, 2046- 2061. https://ijoc.org/index.php/ijoc/article/viewFile/8774/2639

Olufemi A. (2020, October 24). Buhari's 2021 budget share for education is Nigeria's lowest in 10 years. Premium Times. https://www.premiumtimesng.com/news/headlines/4228 29-buharis-2021-budget-share -for-education-is-nigerias-lowest-in-10-years.html

Onuoha, F. C. (2020). Review and Analysis of Nigeria's National Security Strategy 2019. Technical Report.

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of Cyber Criminology (IJCC), 9(1), 120-143.

Russell, S. & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson Education Limited

Russell, S. & Norvig, P. (2016). Artificial intelligence: a modern approach. Pearson Education Limited.

Russell, S. & Norvig, P. (2003). Artificial Intelligence: A Modern Approach (2nd ed.). New Jersey: Prentice Hall.

Sayler, K. M. (2020). Artificial intelligence and national security. Congressional Research Service Report, R45178. https://fas.org/sgp/crs/natsec/R45178.pdf

Sprengel, F. C. (2021, June). Drones in hybrid warfare: Lessons from current battlefields. Hybrid CoE Working Paper 10. The European Center for Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wpcontent/uploads/2021/06/20210611_Hy brid_CoE_Working_Paper_10_Drones_in_hybrid_warfare_WEB.pdf

Suleiman, M. N., & Karim, M. A. (2015). Cycle of Bad Governance and Corruption: The Rise of Boko Haram in Nigeria. Sage Open, 5(1), 1-11. https://doi.org/10.1177%2F2158244015576053