ABUAD Journal of Social and Management Sciences (AJSMS),
Vol. 3, No. 1, 2022, pages 109-113 https://doi.org/10.53982/ajsms.2022.0301.07-j

Published by the College of Social and
Management Sciences (SMS), Afe Babalola
University, Ado-Ekiti (ABUAD), Nigeria.
E-mail: ajsms@abuad.edu.ng

ISSN: 2714-3740

- Commentary -

Security and Business Operations in Nigeria: The Moderating Role of Politics

Ademola AZEEZ[1]

The Nigerian state is currently faced with multiple security threats. These threats include the prevalence of jihadism in the Northeastern part of the country, armed banditry and kidnapping in the Northwestern, Northcentral and Southwestern zones, insurrection in the Southeastern region, oil conflict in the Niger Delta, as well as armed robbery and ritual killings across the country. The criminal activities of terrorists, bandits and kidnappers have adversely affected Nigeria's security landscape. Several thousands of lives have been lost and major sources of livelihood destroyed. Business activities have been crippled in several conflict spots. Many firms have relocated to new environments, while others have withdrawn their officials and representatives due to security threats and the challenges affecting key operations. Many farmers have also left their farmlands, leading to high rate of waste, losses and the looming threat of food insecurity (Faminu, 2019). Though insecurity affects every aspect of live, its impact on business operations represents the focus here.

Macro insecurity affects business operations in several ways. First, there is the difficulty in generating raw materials. Businesses are largely dependent on the regular supply of important raw materials for production and other purposes. However, in areas where there is large scale insecurity, many businesses would be unable to get raw materials for production thereby jeopardising other important business activities that are contingent on production (Chukwu et al, 2018). Second, there are constraints on marketing and sales. Insecurity affects the marketing of finished products. A business enterprise does not only generate raw materials for production, it also creates channels and mediums for marketing and sales. Insecurity has always limited market availability in a number of ways: areas prone to insecurity are unattractive to marketers; there is continuous migration or exodus of people to other relatively peaceful areas within or

[1] Ademola Azeez is a Professor of Political Science at Afe Babalola University, Ado-Ekiti, Nigeria. He is currently serving as the Provost of the College of Business and Social Sciences, ABUAD.
Author's e-mail: demazez@gmail.com

outside the space, with an adverse effect on the customer base. These are the experiences of several businesses in many parts of Nigeria, particularly in areas where terrorism and armed banditry are prevalent (Aluta, 2021; Chukwu et al, 2018).

Third, there is an increase in security spending. Criminal attacks have ruined a lot of businesses in Nigeria and led to losses. Insecurity increases business organisation's security spending, which exists as precautionary expenditures for private security services. Most of the business organisations operating in the country deploy resources for the employment of security personnel and the erection of certain security devices to ensure the protection of their investments, staff and customers (Aluta, 2021; Chukwu et al, 2018; Achumba et al, 2013). Fourth, insecurity creates manpower shortages for businesses. There is usually the dearth of skilled labour as a result of violent deaths or physical injury to staff, the migration of professionals to safer places, and the unwillingness of fresh people to move to insecure locations for employment. Therefore, manpower shortage affects all business operations, from production to sales (Aluta, 2021). Already, there are several factors responsible for the collapse of businesses in Nigeria, such as: unfriendly government policies and difficult business environment, poor infrastructure (including energy), among many others. Insecurity has recently emerged as a major factor that constrains business operations in Nigeria.

Furthermore, while the ascendency of the Internet of Things (IoT) has boosted business operations in Nigeria, it has also increased the vulnerability of businesses to cyber-attacks. As argued by He, Huang and Yang (2020, p. 1), the security of IoT network is 'difficult to manage because IoT devices are heterogeneous. Based on these features, attacks against IoT network like distributed denial-of-service and system intrusion are easier than traditional network.' Without a doubt, cyber-crime is a major threat to business everywhere. As more and more businesses migrate to online platforms to increase productivity, visibility and the ease of doing business, cloud sharing technologies have become more susceptible to attacks. Cyber-crime affects businesses in a number of ways. First, the distasteful posts shared to followers and customers of companies, products and business personalities by hackers could harm or damage reputation across board. Second, businesses could lose out to competitors, particularly if hackers gain access to new products or services and sell such stolen information to interested parties (Gingerich, 2022). Other problems include loss of customers and finances, and legal consequences.

With the increasing migration of businesses to online platforms, BusinessDay (September 7, 2021) reports that Nigeria is experiencing unprecedented cyber-attacks, particularly on commercial and individual platforms. From the report, major countries in Africa (including Nigeria) experienced close to 90 million malware attacks in 2021.

Countries most targeted were South Africa (32 million attacks), Kenya (28 million attacks), and Nigeria (16.7 million attacks). However, when compared to the pre-COVID year, Nigeria recorded the highest rise in cyber-attacks in 2021 (23 per cent). The figures could be more staggering if all cyber-attacks were reported by businesses (Idris, 2020). The point must be made that as more businesses migrate to IoT, they will increasingly come under cyber-attacks with implications for reputation, productivity, customer relations, sales and marketing. Because businesses in Nigeria have lost about 5.5 trillion naira to fraud and cyber-crimes in 10 years, it has been noted that the phenomenon of cyber security threats could become the next pandemic in Nigeria (Adepetun, 2021).

This commentary argues that politics plays a major role in addressing issues relating to macro and business security in Nigeria. To start with, the provision of business security is a multi-layered effort, involving different actors such as business owners themselves and government, among others. The concept of politics is deliberately explored here to imply the role of government in guaranteeing business security. The provision of security as a public good is the primary responsibility of government. In that light, a functioning security architecture should guarantee the full functioning of the entire public sphere, including the business environment. Although the business environment is influenced and affected by a variety of issues in the context of Nigeria, none has the capacity to instantly annihilate businesses like a collapsed security. A secured business environment will allow businesses to thrive, encourage local and foreign investments, guarantee ease of doing business, aid marketing and sales, and facilitate returns on investment. Nigeria's existing frameworks for promoting national security are limited by operational issues and dilemmas. The Nigerian government must therefore scale up efforts to reverse and address the multiple security threats currently confronting the country. The remediating measures recommended by this commentary include:

i. The ungoverned and under-governed spaces that criminals often exploit must be adequately manned and come under the firm control of government and state actors. If insecurity is to be adequately addressed, then every part of Nigeria's territory should have the benefit of adequate deployment of security forces to quell violent attacks, deter criminals, and support business operations.

ii. To achieve the above, there should be an increase in the enrolment of people into the Nigerian security forces. As things currently stand, Nigeria is grossly under-policed, and this has affected the effectiveness of the Nigerian police force in fighting crimes. The Nigerian armed forces are also not adequately manned to be able to respond to existential security threats,

which confront the country and constrain businesses. In terms of personnel, the size of the Nigerian security forces must be expanded.

iii. The Nigerian security sector requires adequate financing as this would ensure that more security posts are created across the country. It would also ensure that members of the security forces are provided with the required operational materials such as patrol vehicles, weapons, uniforms, surveillance devices for intelligence gathering, robust welfare package and insurance, among others, to fight crimes effectively.

iv. Insecurity is largely a product of bad politics – that is, the failure of governance. In the context of Nigeria, many undercurrents and precipitants of insecurity are governance-related. Rising poverty, unemployment and inequality (that have produced fertile grounds for criminality) are products of poor governance. As provided for in the 1999 Constitution of Nigeria (as amended), the primary purpose of politics is to guarantee good governance and promote the welfare of all persons. The government (national and sub-national) must live up to this onerous responsibility.

v. With reference to fighting cybercrimes, the overall political and legal frameworks are the responsibility of government in modern times, albeit businesses also have some roles to play. Governments usually play the grandest role because it is their responsibility to keep the citizens safe and regulate businesses (Redins, 2021). Therefore, governments must develop coherent and clear national cyber security defence strategies to combat cyber-threats faced by citizens and businesses. As argued by Fadia, Nayfeh, and Noble (2020), a comprehensive national cyber security strategy must have elements such as a dedicated national cyber security agency, a national critical infrastructure protection programme, a national incident response and recovery plan, defined laws pertaining to all cybercrimes and a vibrant cyber security ecosystem. Nigeria already has some of these elements in place. For instance, Nigeria has the Cybercrimes Act (2015) and a Cybercrime Advisory Council responsible for promoting cyber security in the country, with the National Security Adviser (NSA) as the Chairman. However, the Advisory Council has been inactive over the years. It is my recommendation in this commentary that the Nigerian government must be more deliberate and proactive in creating a safe digital environment for citizens and businesses. Governments should also produce comprehensive plans and strategies that businesses can leverage on, while increased cyber-awareness is engendered and promoted as matter of policy and priority.

References

Achumba, I. C. et al. (2013). Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development. *Journal of Economic and Sustainable Development* 4(2), 79-99.

Adepetun, A. (2021). Cyber-Crime may become the Next Pandemic. *The Guardian*, December 10.

Aluta, C. (2021). *Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development*. Paper presented during the Nigeria-South Africa Chamber of Commerce Webinar, with the theme 'Security Challenges in Nigeria and the Implications.' January 28.

Chukwu, G. C. et al. (2018). Insecurity and Distribution of Consumer and Industrial Products. *Scholars Journal of Economics, Business and Management*, 5(9), 813-821.

Fadia, A., Nayfeh, M., Noble, J. (2020). Follow the Leaders: How Governments can Combat Intensifying Cybersecurity Risks. *McKinsey & Company*, September 16.

Faminu, G. (2019). How Insecurity Impacts Business. *BusinessDay*, January 31.

Gingerich, M. (2022). *How Cyber-Crime can affect your Marketing Strategy.* Indiana: Digital Hill Multimedia.

He, S., Huang, J., Yang, P. (2020). Build with Intrinsic Security: Trusted Autonomy Security System. *International Journal of Distributed Sensor Networks*, 16(11), 1-10.

Idris, A. (2020). Why some of Nigeria's Worst Cyber-Attacks are not reported. *TechCabal*, July 21.

Redins, L. (2021). Cybersecurity: Who is Responsible? *Cybersecurity Guide*, November 19.