FOREIGN DIRECT INVESTMENT AND NIGERIA'S NATIONAL SECURITY: THE NEED FOR A RETHINK

Chidozie Acholonu and Gerald Ifeanyi Okafor[1]

Abstract

This paper explores the risks of foreign direct investment (FDI) in Nigeria as a potential national security threat. While FDI offers capital, technology, and economic growth, it also presents challenges in critical infrastructure control, intellectual property theft, espionage, and foreign influence. The study cautions against FDI as a covert threat, advocating a reconsideration of engagement processes to safeguard Nigeria's national security. Employing a comprehensive analysis of secondary sources data, including reputable academic publications, government reports, and relevant open sources, this research delves into the potential and associated risks of FDI.

Keywords: Foreign Direct Investment, National Security, Critical Infrastructure, Espionage and Cyber-security

Introduction

Foreign Direct Investment (FDI) can help a country to grow its economy and increase its productive capacity by providing access to capital, modern technology, and management expertise. When countries are open to investment, FDI can create new jobs, increase exports, and stimulate local businesses, which can lead to a multiplier effect on the economy. FDI can help to transfer knowledge, skills, and technology from developed to developing countries, which can contribute to human capital development and help to build a stable country (World Investment Report, 2014). For example, foreign companies may bring in new management techniques and business practices, which can help to increase productivity and efficiency in the economy of the target

[1] Chidozie Acholonu and Gerald Ifeanyi Okafor, PhD are of Institute for Peace and Conflict Resolution, Abuja, Nigeria

country. This investment can be a significant driver of economic growth and political stability in a host country, particularly in emerging economies.

Overall, foreign direct investment has been identified as a driver of economic growth and development, however, it is important to recognize that there are potential risks and challenges associated with FDI, particularly with national security and control of critical infrastructure such as energy, telecommunications, and transportation. In recent years, foreign firms (especially technological companies) from China and the USA have been accused of using their FDI to access sensitive information to influence decision-making processes, leading to scepticism about the motives of software emanating from these countries. The increasing presence of foreign investors, in critical infrastructure, has raised concerns from several countries about potential threats to national security.

As a developing nation, Nigeria has been the recipient of significant foreign investment over the years, and the country's leaders have encouraged foreign businesses to invest in its economy. While FDI has brought many benefits to Nigeria, including job creation and infrastructure development, the issue of the implications on national security cannot be ignored. In recent years, there have been increasing concerns over the role of foreign firms in Nigeria's critical infrastructure projects. This has led to questions about the extent to which foreign firms are involved in Nigeria's national security infrastructure and the potential risks that may arise from such involvement. This situation has raised worrying questions for the Nigerian government concerning measures to safeguard the country's national security interests in the face of increasing FDI.

The purpose of this paper is to examine the threats to Nigeria's national security from FDI. Specifically, the paper argues that FDI has the potential to pose a significant threat to Nigeria's national security if not properly regulated. By examining the threats to national security from FDI and providing recommendations for regulation, this paper seeks to raise awareness and increase conversation to foster critical thinking and understanding of the national security challenges

associated with foreign investment in Nigeria. To achieve this, the paper will cover four main sections. The first section will define FDI and National Security. The second section will highlight cases of FDI and the risk to national security, including the risks of espionage. The third section will focus on FDI in Nigeria and the potential threats to national security. Finally, the paper will offer recommendations as to how Nigeria can regulate FDI to mitigate these threats and protect its national security.

Conceptualizing Foreign Direct Investment and National Security

Foreign Direct Investment (FDI) is an important aspect of international business and has become a popular means of economic development for many countries. According to the World Investment Report, (2014), FDI refers to the investment made by a foreign company or individual in the business of another country, to establish or expand operations. It is an important source of capital, technology, and managerial expertise that can contribute to the economic development of the host country. According to the International Monetary Fund (IMF), FDI can be defined as "an investment made to acquire lasting interest in an enterprise operating in an economy other than that of the investor, the investor's purpose being to have an effective voice in the management of the enterprise" (IMF, 2009). This definition suggests that FDI involves more than just investing money in a foreign country. It also involves a long-term commitment. Furthermore, Foreign Direct Investment (FDI) can be defined as a long-term investment by a foreign entity into a domestic company or production facility, to acquire a significant degree of control over its operations (OECD, 1993). FDI is considered to be a key driver of economic growth and development in many countries, especially in developing economies, as it brings in new capital, technology, and expertise (IMF, 2009). However, FDI can also pose significant risks and challenges, particularly to national security. It is also important to highlight within the context of this discussion that FDI further implies development and investment initiatives in a country, which have foreign participation through channels such as resources,

expertise, equipment, spare parts, etc. for purposes of economic growth and development, and other social benefits.

One of the main benefits of FDI is its ability to stimulate economic growth and development through the injection of new capital, technology, and expertise in the host country (IMF, 2009). FDI can also create jobs, increase exports, and promote the development of local businesses, which can have a multiplier effect on the economy (IMF, 1993). In addition, FDI can contribute to human capital development by transferring knowledge, skills, and technology from developed to developing countries, which can help to build a skilled workforce and improve productivity (World Investment Report, 2014). Research has shown that FDI can have a positive impact on economic growth, particularly in developing countries. According to the World Investment Report, (2014), FDI can increase a host country's productivity by transferring technology and know-how, which can lead to the adoption of more advanced production methods. Additionally, FDI can bring in new capital, which can be used to fund investment and increase production capacity. This can lead to the creation of new jobs and higher wages, as well as the development of new industries and the expansion of existing ones.

However, some scholars have argued that FDI can also have negative effects on host countries, particularly on national security. One concern is that foreign companies may use FDI to gain access to sensitive information or control over critical infrastructure, such as telecommunications, energy, and transportation. This has led to increased scrutiny of FDI by governments and policymakers, with many countries implementing regulations to limit foreign ownership of critical infrastructure. According to Bian (2020), FDI has serious implications for sovereignty in countries that rely heavily on foreign investment, particularly in sectors that are critical to national security. The study shows that states grapple with foreign companies using their investment to exert influence over government policy, which can undermine national security interests (Bian, 2020). Additionally, foreign companies may bring in their management practices and technology, which can lead to a loss of jobs and skills among local workers.

Another potential negative impact of FDI is that it can lead to increased inequality within the country, especially in developed and developing economies. While FDI can create new jobs and industries, these benefits may not be evenly distributed across the population. For example, foreign companies may only hire skilled workers or may pay their workers lower wages than domestic companies. This can exacerbate existing income inequalities and create social tensions.

Despite these potential negative impacts, many countries continue to attract FDI as a means of promoting economic development. Some studies have suggested that certain policies and conditions can maximize the benefits of FDI while minimizing the risks. The IMF (2009) found that countries with strong institutions and a high level of human capital tend to benefit the most from FDI. Many countries that implement policies to attract FDI, such as tax incentives and increased regulatory processes, may be more successful in attracting high-quality investments. While FDI can be a powerful tool for promoting economic growth, particularly in developing countries, it is important for policymakers to carefully consider the potential risks and benefits of FDI, particularly on national security (Centre for International Governance Innovation, 2021).

The concept of national security has been viewed in various dimensions. National security can be defined as the protection of a country's sovereignty, territorial integrity, political system, and economic prosperity from internal and external threats (Watson 2008). These threats can include military, economic, political, and environmental factors that may impact the security and stability of a country. In Ungerger, (2008), National Security is the fundamental duty of government but defining it in an increasingly globalized world is a difficult task. According to the US Department of Defense (2018), national security is defined as "the preservation of the values, institutions, and territory of a country from external threats or aggression." Indeed, national security can be broadly defined as the protection of a country's territory, people, and interests from internal and external threats. According to a report by the US Department of Defense (2018), national security encompasses four main dimensions:

military, economic, diplomatic, and informational. The military dimension involves the use of force to protect national interests, while the economic dimension involves the protection of a country's economic assets and competitiveness. The diplomatic dimension involves the promotion of international cooperation and alliances, while the informational dimension involves the protection of a country's information and communication networks. Furthermore, the National Security Strategy of Nigeria (NSS, 2019) in its consideration of national security places more emphasis on human security (people-centric) which is in tandem with the paradigm shift contemporarily. This human security dimension to understanding national security focuses on ways to address four critical security concerns in Nigeria, namely: the existential need to protect Nigerian people and territory; to promote Nigeria's prosperity and sustainable development; the need to promote national unity and peaceful co-existence; and the focus on realizing Nigeria's regional and international interests (Onuoha and Ogbonanya, 2020).

National security is a critical issue for all countries, as it involves the protection of a nation's citizens, economy, and institutions from internal and external threats. According to the Centre for International Governance Innovation (2021), military spending is a key component of national security. However, national security has become an increasingly complex and multifaceted issue, as advances in technology and the rise of non-state actors have created new challenges for governments and policymakers. This dynamism and developments in the international system tend to expand to thinking on national security and as such, it has evolved from the traditional military realm to a growing list of internal and external pressures that are important components of a country's overall well-being (Ungerger, 2008). Without effective national security measures, a country is vulnerable to external threats, which can lead to economic instability, political instability, and even violent conflict.

In recent years, the concept of national security has expanded to include non-traditional military threats as a result of globalization (Ungerger, 2008). The rise of the internet has also made it easier for state

and non-state actors to threaten national security by launching mass surveillance, conducting cyberattacks, stealing sensitive information, and disrupting communication systems (Unver, 2018). A report by the US Department of Defense (2018), found that cybersecurity is becoming an increasingly important aspect of national security, as governments and organizations work to protect themselves from cyber threats. In response to the growing threat of cyber-attacks, many countries have implemented policies and strategies to enhance their cybersecurity capabilities. For example, a study (Unver, 2018) found that countries with stronger institutional frameworks and greater investment in cybersecurity tend to be more attentive to cyber-attacks due to mass surveillance. Additionally, some countries have dedicated specialized agencies or units to focus specifically on cybersecurity, such as the United States National Security Agency (NSA), and Office of the National Security Adviser (ONSA) in Nigeria which is coordinating the efforts at mitigating the menace in line with the Cybercrimes (Prohibition and Prevention) Act, 2015.

Similarly, terrorism has become a major concern for national security in many countries. A study by the Institute for Economics and Peace (GTI 2022), found that Sub-Saharan Africa emerged as the global epicentre of terrorism. Terrorism can have a devastating impact on a country's economy, as well as its social fabric and political stability. The adaptability of non-state actors, such as terrorist groups and organized crime syndicates has been identified as a lingering threat to national security. These groups often operate outside of traditional state structures, making them difficult to identify and combat.

Interestingly, there is a global discourse on the plausible relationship between FDI and the significant risks to national security and espionage. Scholars have identified various dimensions of the risks and benefits of FDI, the role of governments in regulating FDI, and the potential impact of FDI on national security and economic development (Kucera, 2014). Despite these benefits, FDI can pose significant risks to national security, particularly with critical infrastructure and assets, political influence and intellectual property. Pointedly, it is this threat posed by FDI to national security that is at the core of this discussion.

Foreign Direct Investments and the Threat to National Security

Over the years there have been several high-profile reports of how FDI can pose a threat to national security, particularly when the investors are from countries with different geopolitical agendas or interests. One of the primary threats surrounding FDI is the potential for foreign investors to gain control over strategic assets of a country, such as ports, airports, telecommunication and energy infrastructure (Centre for International Governance Innovation, 2021). This can create vulnerabilities for the country, as foreign actors could use their control over these assets to disrupt critical infrastructure or gain leverage over the host government (Bian, 2020). Another concern is that foreign investment could be used as a tool for political influence. A foreign investor could use espionage and its economic power to pressure the government to take certain actions or adopt certain policies. This could create vulnerabilities for the country and compromise its sovereignty. Yet another threat is the potential for foreign entities to gain access to sensitive technologies and intellectual property (Rickards, 2009). This can occur when foreign investors acquire or invest in companies that have access to sensitive technologies or when foreign entities establish technology facilities in the host country (Rickards, 2009). In these situations, there is a risk that foreign actors could use the technology for malicious purposes, such as espionage. Another concern has to do with the location of the foreign investments in places that host the military, security and intelligence infrastructure of the country considering the tendency that such investments could serve multiple purposes and pose risk to national security (Centre for International Governance Innovation, 2021).

In this direction, for instance, several reports increasingly point to China, using the opportunity afforded by Chinese companies' FDI to gather intelligence, as Chinese law prioritizes that companies cooperate with the government above user privacy. According to Meservey, (2020), Chinese companies are legally obligated to help the Chinese government gather intelligence from devices in China and in countries where they are invested. Chinese government documents also reveal that data collected from software, apps, and hardware in

telecommunication devices are sent back to China for analysis to help the Chinese government in its public diplomacy efforts (Meservey, 2020).

In September 2020, Deutsche Welle (DW) news reported that the Indian government decided to ban 118 mostly Chinese mobile applications, including services provided by the China internet giant Tencent and the widely popular online game Player Unknown's Battlegrounds, also known as PUBG. India's Information Technology Ministry justified the ban by stating that these apps were promoting activities that posed a threat to the sovereignty and integrity of India, the defence of India, the security of the state, and public order. The decision was made to ensure the safety, security, and sovereignty of Indian cyberspace. The move was seen as part of the ongoing tensions between India and China, which have been experiencing a border dispute, and also as part of India's efforts to reduce its economic dependence on China. The decision was met with mixed reactions, with some praising the government's move to protect national security while others criticizing it for harming business and innovation.

For years, the US government has accused Huawei of aiding the Chinese government in conducting espionage (Hamilton, 2020). However, for the first time, it has given specific information on how it believes Huawei is doing this. According to officials, Huawei has created equipment that can secretly access telecommunications through interfaces that are only intended for use by law enforcement (Hamilton, 2020). Huawei has denied these accusations and has not disclosed this alleged access to its local customers or the host nation's security agencies. In 2019, former US President Donald Trump issued an Executive Order effectively banning Huawei from doing business with US companies, citing national security concerns (Bartz & Alper, 2022). The ban prevented Huawei from buying key components and technologies from American firms without prior approval from the US government. In 2021, five Chinese companies; Huawei, ZTE, Hytera Communications Corp Hikvision and Dahua, were added to the "covered list" as posing a threat to national security under a 2019 law aimed at protecting U.S. communications networks (Bartz & Alper,

2022). The US and India have also banned the downloading and use of Tik-Tok, a social media app owned by a Chinese company, on government devices.

In recent times, there has been a growing concern in America over China's interest in agriculture especially its deliberate efforts at owning foreign farmlands. The debate shows it is of strategic interest to America notwithstanding that China owns about 0.9% of all foreign-owned US agricultural land as of 2021, which is significantly low. But the concern arises from the point that China's agricultural investment abroad increased more than tenfold between 2009 and 2016 according to the United States Department of Agriculture (USDA). It is in this light that the South Dakota Republican Representative, Dusty Johnson, who is a member of the China-focused House Committee in the US Parliament avers that the Chinese Communist Party has increased their holdings of foreign farmlands by 1000%; owning 1,300 agricultural processing facilities outside of China in the recent years (Brandon, 2023). Therefore, American thinkers and policymakers are contending that this growing interest in agriculture has implications for national security considering the nexus between food availability and national stability. Indeed, the trends and dynamics of global politics and governance point to the fact that food security is national security. Another critical dimension of this discussion revolves around the locations of the farmlands. The blocking of the proposal for the construction corn milling facility on the edge of Grand Forks in North Dakota, less than 15 miles from the Grand Forks Air Force Base, by an American subsidiary of a Chinese company, Fufeng USA is an indication of the nexus between foreign investment and national security. Although there was an indication that the project would be beneficiary to the people in terms of economic opportunities associated with it, nevertheless, there is a strong contention between the economic boon and the geopolitical risk. While the US Air Force raised concerns about the security risks associated with the project, some people insisted that the facility would be used for spying on the Air Force. Despite the denial by the company of the allegation, there are strong indications of efforts to block the construction of the corn mill because

of the affiliation of the USA Company with the Chinese company (Smith, 2023).

China's growing FDI presence in Europe has also raised concerns and suspicion, particularly given its state-driven approach to investment. This suspicion over Chinese hardware played out during the rollout of 5G technology in Europe, about the potential for Chinese governments to exploit the technology for espionage or other malicious purposes (Meservey, 2020). In response, some European countries have imposed restrictions on the use of equipment from Chinese tech companies in their 5G networks.

This suspicion is exacerbated by disclosed backdoor vulnerabilities discovered in millions of cameras, including those sold by Dahua Technology and its larger stablemate Hikvision (Meservey, 2020). These cameras carry the potential to be used as eavesdropping devices, even when the audio on the camera is disabled. These cameras are deployed widely in the U.S. and Europe and sold under Dahua Technology, which is the second-largest Closed-Circuit Television (CCTV) manufacturer in the world (Hoffman, 2019). Both Dahua Technology and Hikvision were then prohibited from U.S. government contracts and applications with national security restrictions (Doffman, 2019). The incident highlights the potential risks associated with the use of foreign-made technologies.

The concerns surrounding FDI and national security are not restricted to China. The revelations by Edward Snowden show that the National Security Agency (NSA) routinely infiltrates American technology companies' products with backdoors that allow unauthorized access, and these companies are slow or refuse to fix them. For instance, a report in 2020 revealed that the FBI has been trying to gain access to the backdoor of Apple devices (Hamilton, 2020). Despite efforts by a leading Congressional critic, the U.S. National Security Agency is refusing to disclose whether it is still implementing "back doors" in commercial technology products, which is considered a controversial practice that is said to be harmful to both national security and the U.S. industry (Menn, 2020). The agency has allegedly been seeking arrangements with technology companies for a long time to

create a special access point for the spy agency in their products, as reported by Reuters and former NSA contractor Edward Snowden (Menn, 2020).

To address these concerns, some countries have implemented measures to restrict foreign investment in certain industries, such as defence or critical infrastructure, increased scrutiny of foreign investment, placed restrictions on foreign ownership of critical infrastructure, and promulgated stronger cybersecurity regulations. In the United States, the Foreign Investment and National Security Act of 2007 established the Committee on Foreign Investment (CFIUS) to review foreign investments in American companies and block deals that pose a threat to national security (Jackson, 2008). European countries also have implemented robust legislation that empowers their institutions to demand transparency around foreign investment and require foreign investors to disclose their ownership structure and ultimate beneficiaries of any investment (OECD Secretariat, 2020). This can help to identify potential sources of political influence and mitigate the risk of undue influence on the host government. Furthermore, some measures have been adopted by countries to restrict foreign ownership of strategic assets or require that foreign investors partner with local companies. For example, Australia has implemented a foreign investment review framework that includes investors and companies acquiring businesses and land in Australia to obtain Foreign Investment Review Board (FIRB) approval for acquiring direct interests in national security businesses (Ching and Montgomery, 2021).

According to a report by the OECD Secretariat (2020), since the middle of 2018, some governments that had previously privatized potentially sensitive assets have unexpectedly shown interest in returning to state ownership. They have proposed or implemented policies or practices to support this approach. For instance, in February 2019, the German government recommended the use of a state-owned fund to purchase companies and prevent foreign takeovers in certain situations (OECD Secretariat, 2020). At that time, Germany had just used an existing state-controlled entity to acquire stakes in a company that owned an important electricity distribution grid, which a foreign

company had attempted to purchase. The German government justified state acquisitions as necessary to protect the country's national security interests in the FDI acquiring critical infrastructure (OECD Secretariat, 2020).

Interestingly, the EU science hub has noted that China has equally taken measures to protect its national security by limiting foreign technology in certain sectors. For example, China has implemented a "cyber-security review" process for foreign technology companies seeking to sell products to Chinese government agencies or state-owned companies. This process has led to restrictions on products from companies such as Microsoft and Tesla, which have been deemed potential security risks.

From the foregoing, it is apt to opine that foreign direct investment (FDI) poses national security threats that cannot be ignored. Governments around the world are implementing measures to mitigate the risk from these threats, such as tightening laws, imposing restrictions on foreign ownership in certain sectors, and blocking foreign firms from sensitive areas. It is on this premise that the next segments of the discussion will take a closer look at FDI in Nigeria and the potential national security threats that may arise.

Foreign Direct Investment in Nigeria

Foreign Direct Investment (FDI) as we have discussed is a form of investment where a company from one country invests in another country to establish business operations or acquire an existing business (World Investment Report, 2014). FDI is usually made by multinational companies (MNCs) that seek to expand their market reach and access new markets. FDI can be in the form of equity, loans, or reinvestment of profits. Nigeria, with its vast natural resources and large population, has always been an attractive destination for foreign investors seeking to take advantage of the country's large market potential (IMF, 2009). Historically, foreign investment in Nigeria began in the colonial era when British colonialists invested in infrastructure such as railways, roads, and ports (U.S. Library of Congress, n.d.).

In the 1960s, FDI inflows into Nigeria were primarily from the United Kingdom, followed by the United States. These investments were mainly in the oil and gas sector, as Nigeria is a major oil-producing country. In the 1970s, the Nigerian government encouraged FDI as a way of diversifying the economy and reducing its dependence on oil. The 1960s and 1970s saw a significant increase in FDI inflows into Nigeria, mainly from Western countries, and multinational corporations began to establish a significant presence in the country (Ekpo, 1997). This period was also marked by the Nigerian civil war, corruption, and a lack of transparency, which led to the mismanagement of Nigeria's vast natural resources and economic decline (U.S. Library of Congress, n.d.).

The 1980s and 1990s saw a decline in FDI inflows into Nigeria, largely due to a combination of the global oil crisis and the structural adjustment program (Ekpo, 1997). With the end of military rule and the return to democracy in 1999, there was renewed economic activity by the incoming administration. The Nigerian government introduced a series of economic reforms aimed at making the country more attractive to foreign investors. The new government, led by President Olusegun Obasanjo, launched a series of economic reforms that included the liberalization of key sectors such as telecommunications, banking, and power, which attracted significant foreign investment. The telecommunications sector, in particular, saw a surge in FDI inflows following the privatization of the economy under the Obasanjo's Administration, 1999-2007 (Tribune Online, 2020).

From 2001-2003, Multinational corporations such as MTN, Econet (Airtel) and Etisalat (9mobile) entered the market in Nigeria, driving growth in the sector and improving access to telecommunications services for millions of Nigerians (Tribune Online, 2020). MTN has been in Nigeria for over two decades and has acquired the largest share of telecommunication subscribers with over 73 million Nigerians active on its platforms (Adepetun, 2021). The sectors that have attracted the most FDI inflows in Nigeria include the oil and gas sector, the telecommunications sector, transportation and the manufacturing sector. The oil and gas sector is the largest recipient of

FDI in Nigeria, with the majority of the investment coming from multinational oil companies such as Royal Dutch Shell, ExxonMobil, and Chevron. The top investors in Nigeria are currently China, the Netherlands, and the United States.

According to Ekpo (1997), Nigeria has consistently aimed to boost growth and development by incentivizing FDI in the oil sector. The government has created the Oil and Gas Investment Promotion Centre at the Ministry of Petroleum Resources to make it easy for prospective investors to enter the sector (In Quest for Increased FDI, Federal Government Sets Up Oil, Gas Investment Promotion Centre, 2022). The Nigerian government has used its oil revenue to play an active role in collaborating with both foreign partners and domestic entrepreneurs in the creation, ownership, and management of the oil sector. The rationale behind this approach is that foreign investment can help bridge the domestic resource gap. By bringing in foreign investment in the oil sector, Nigeria gains access to foreign exchange, which assuming all other factors remain equal, can enhance the country's ability to import goods. While FDI has brought some benefits to Nigeria, it has also posed some dangers to the country's national security.

Aside from the oil sector, other critical areas with visible foreign interest and presence include transportation-roads, railways, airport expansion and remodeling; agriculture; power and energy, tech-industry; etc.

The Potential Threats from Foreign Direct Investment to Nigeria's National Security

Foreign Direct Investment (FDI) has been a key driver of economic growth in many countries, including Nigeria. And yet, FDI can be a double-edged sword because it can also pose a significant threat to national security. Some of the primary concerns regarding FDI are foreign access to critical infrastructure and espionage. Foreign firms that may invest in Nigeria's energy, transportation, or communication systems, will gain access and have control over critical infrastructure. This can give them significant economic power that can be used as

leverage to influence or even undermine domestic policies, and national interests, thereby potentially threatening national security.

A report by Uzoho (2021) showed how FDI can be a threat to Nigeria's critical infrastructure. The concrete incident was the takeover of the Port Harcourt Electricity Distribution Company (PHED) by a Canadian firm, Manitoba Hydro International. With the privatization of generation and distribution companies under the defunct Power Holding Company of Nigeria (PHCN), the federal government in line with the power sector reforms, had given the company management of Transmission Company of Nigeria (TCN) for an initial period of three years (Uzoho, 2021). The company was given control of the distribution of electricity in 2012 and the contract was terminated in 2016, due to issues with poor distribution and management of the contract (Uzoho, 2021). This case resulted in a significant loss of revenue for Nigeria, as well as economic disruption and public outcry.

Another area that has generated concern among many Nigerians is the loans from China to develop Nigeria's critical infrastructure, which has been described as a "debt trap." According to Daily Trust, (2021), "Nigeria has requested loans from China for its major projects at railways, airport, seaports, highways, power stations, gas pipelines, and the country is now indebted to China to the tune of $3bn as of March 2020, according to the Debt Management Office (DMO). Projects so far executed with Chinese loans are the Nigerian National Public Security Communication System Project $399.5m; the Idu-Kaduna railway $500m; Abuja Light rail $500m; Nigeria ICT infrastructure backbone $100m; four airports expansion projects at Abuja, Kano, Lagos and Port Harcourt $500m; Zungeru hydropower $984.3m; 40 parboiled rice plants $325m; Lagos-Ibadan railway $1.267.3bn; Abuja-Keffi road upgrade $460.82; and supply of rolling stock for Abuja light rail $157m; and greater Abuja water project $381m." These projects are central to the economic development of the country with implications for national security.

Also, the case of the African Union (AU) building with the negative political reports over concerns of espionage due to the alleged bugging by China, which if true has significant implications for

Nigeria's national security. The building, which was constructed by the Chinese government as a gift to the AU, was reportedly bugged by Chinese engineers during its construction as reports emerged of Beijing's surveillance operations (Meservey, 2020). This allegation resonates with the fears of possible compromise of African government buildings beyond just the African Union headquarters (Meservey, 2020). This is also worrisome due to the increasing rate of contracting government buildings in Africa to foreign construction companies. The scope of these contracts includes construction, remodeling, furnishing, maintenance, etc. It is interesting to note that Chinese companies have been involved in the construction or renovation of at least 186 government buildings in Africa since 1966. This includes government buildings in at least 40 of Africa's 54 countries, including Nigeria (Meservey, 2020). However, due to the challenges in obtaining comprehensive data on China's engagement with Africa over the last seven decades, these figures can be disputed. The Chinese government has denied the allegations, but the incident has raised concerns about China's activities in Africa and its use of technology for espionage purposes.

Against this backdrop, it is essential to note that the use of Chinese and foreign ICT hardware and software has become increasingly common in Nigeria, as in many other countries. With the proliferation of Chinese devices, reports have emerged that some of these products may contain malicious code that could be used to collect personal data and track individuals, posing a significant threat to national security (Meservey, 2020). One example cited was the case of Chinese-made CCTV cameras that are used globally, including in Nigeria. The Chinese company Huawei, for example, has been accused of building backdoors into its products, which could be used to spy on users or disrupt critical infrastructure.

The implications for Nigeria are significant, as the country has also received significant investment and aid from China. There are concerns that China and other countries especially from Europe and America could be using their economic influence to gather intelligence and engage in espionage activities in Nigeria. This could include

economic intelligence gathering, the monitoring of communication networks, and the use of technology to gather sensitive information. The incident with the AU building highlights the need for Nigeria to be vigilant about foreign investment and aid, particularly from countries with a history of engaging in espionage activities. Nigeria must take steps to protect its critical infrastructure and ensure that foreign companies and governments do not have access to sensitive information or control over key systems as most of the hardware and software used in the country are foreign-made.

However, the use of technology for espionage purposes is not limited to China alone. Other countries have also been known to engage in espionage activities, which could pose a threat to Nigeria's national security. The use of foreign social media platforms like Facebook, Twitter, and Instagram, as well as other digital tools like email, text messaging, and mobile apps, media might seem harmless to the casual observer. In late 2018, Citizen Lab published a report that also found evidence of Pegasus throughout Africa, including Côte d'Ivoire, Togo, Uganda, Kenya, Rwanda, Zambia, South Africa, and most North African countries (Guterl, 2022). He explained that Facebook's disclosure showed that any phone can be infiltrated by surveillance software, and Pegasus, which was created by NSO Group, is the most well-known program for mobile surveillance. The spyware works by getting into smartphones and giving the infiltrator full access to the device. This includes access to the phone's camera and microphone, files and photos, network connections, contact information, message and browsing histories, passwords, email accounts, and recordings (Guterl, 2022). Pegasus allows the purchaser to listen to conversations, including those that take place over encrypted messaging apps such as WhatsApp (Guterl, 2022). The article emphasizes that the phone's owner may not even realize that their phone has been turned into an instrument of surveillance. Similarly, the Cambridge Analytica scandal during the 2015 Nigerian elections is a prime example of how personal data from Facebook was used to target political advertisements and influence voters. Cambridge Analytica was a data analytics firm that used information collected from Facebook to create targeted political ads

during the 2015 Nigerian elections. The company allegedly obtained personal data from millions of Facebook users without their consent and used it to create psychological profiles of voters. These profiles were then used to create targeted political advertisements aimed at influencing their behaviours.

In summary, while FDI in Nigeria can be a significant driver of economic growth, it can also pose significant threats to national security. The issues outlined above demonstrate the potential threat from foreign direct investment. Going forward it is essential that the Nigerian government empowers the right institutions and prioritizes measures to address the concerns raised in this discussion. These institutions should effectively implement strategies that protect Nigeria's national security interests from foreign influence and espionage operations against critical sectors such as energy, transportation, agriculture, mining, communication, etc. without isolating Nigeria from the benefits of FDI.

Strategies to Responsibly Protect National Security from Potential Threats from FDIs

Foreign Direct Investment is crucial to Nigeria but as we have seen there are several ways it can be used by bad actors to threaten national security. The threats can arise in a variety of ways that include; control and ownership of critical infrastructure, infiltration of sensitive technologies, espionage and influence operations by foreign entities. As a result, the Nigerian government needs to empower the relevant institutions to implement responsible strategies to mitigate these threats and ensure that FDI is not compromising national security. These strategies can include the following:

i. Screening of investors: The Office of the National Security Adviser, National Intelligence Agency and Department of State Services should be adequately empowered and authorized to oversee the careful screening of potential investors to ensure that they do not have any connections to global terrorist organizations or criminal syndicates.

ii. Limitation of FDI in strategic sectors: The Nigerian government should limit foreign investment in strategic sectors, such as telecommunications, energy, and defence, to reduce the risk of foreign interference.

iii. Setting up robust regulatory frameworks: The Nigerian government should work with the legislature to set up regulatory frameworks to monitor and control the activities of foreign investors in the country. The regulations should be balanced and aimed at safeguarding national interests, without neglecting economic interests.

iv. Transparency in FDI deals: The Nigerian government, civil society and the media should ensure that all FDI deals are transparent and that they adhere to international best practices. This would reduce the risk of corruption and ensure that national security interests are protected.

v. Collaborative intelligence sharing: The Nigerian government should collaborate with other governments and intelligence agencies to share information on potential security threats posed by foreign investors.

vi. Implementation of Due Diligence: The Nigerian government should ensure that due diligence is carried out on foreign investors to ascertain their source of funding, investment track records, and their allegiance that might pose security risks;

vii. Development of local capacity: The Nigerian government should prioritize the development of local capacity in strategic sectors to reduce the reliance on foreign investors and mitigate national security threats.

viii. Investment in security infrastructure: The Nigerian government should prioritize investment in security infrastructure and data analysis to combat the multifaceted threats it faces. This could include the acquisition of advanced technology and equipment, including Artificial Intelligence, the recruitment and training of more ICT

personnel, and equipping security agencies to combat cyber threats.

ix. National research institutions and Think Tanks in the country should constitute study groups to undertake empirical studies on FDIs and potential investors in different sectors of the Nigerian State to provide policymakers and implementers with reliable information on the potential threats of such investments on Nigeria's national security and interests.

Conclusion

Foreign Direct Investment (FDI) presents both opportunities and potential risks to Nigeria's national security. While FDI can bring much-needed capital, technological advancements, and job creation, it also has the potential to pose significant threats to the country's critical national security interests. To address the potential risks, the Nigerian government needs to develop a comprehensive strategy that balances the benefits of FDI with the need to protect national security. This strategy should involve measures such as robust screening processes for foreign investors, restrictions on foreign ownership of critical infrastructure, and the development of a comprehensive legal and regulatory framework to guide FDI. Additionally, the government needs to ensure that its security agencies are adequately equipped and trained to monitor and respond to potential threats to national security. Future research in this area could focus on the impact of FDI on Nigeria's socioeconomic development and the potential trade-offs between economic growth and national security. Further research could also explore the potential for leveraging Artificial Intelligence to enhance security and response capabilities.in managing threats to national security.

References

Adepetun, A. (2021). MTN's role in 20 years of Nigeria's telecoms revolution. The Guardian. Retrieved from https://guardian.ng/technology/mtns-role-in-20-years-of-nigerias-telecoms-revolution

Bartz, D. & Alper, A. (2022). U.S. bans new Huawei, ZTE equipment sales, citing national security risk. Reuters. https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/

Brandon, A. (2023). "China is buying up more U.S. farmlands. Some lawmakers consider that a national threat" NPR Politics Newsletter, March 3, <https//www.npr, org/2023/3/01/1160297853/china-farmland-purcahses-house-house-hearing-competition>

Centre for International Governance Innovation. (2021). Economic security, national security and prosperity: Economic security and the changing global economy. Retrieved from https://www.jstor.org/stable/resrep45134.8

Ching, J., Froelich, C., & Montgomery, H. (2021). Significant Changes to Australia's Foreign Investment Framework Commenced on 1 January 2021. Jones Day. Retrieved from https://www.jonesday.com/en/insights/2021/01/significant-changes-to-australias-foreign-investment-framework-commenced-on-1-january-2021

Daily Trust, (2021). Explaining Nigeria's China Debt Puzzle. Daily Trust. Retrieved from https://dailytrust.com/explaining-nigerias-china-debt-puzzle

Department of Defense. (2018). Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Doffman, Z. (2019). Warning as millions of Chinese-made cameras can be hacked to spy on users: Report. Forbes. https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/?sh=6cf229626bf2

Ekpo, A. H. (1997). Foreign direct investment in Nigeria: Evidence from time series data. Economic and Financial Review, 35(1). https://dc.cbn.gov.ng/efr/vol35/iss1/4

EU Science Hub. (n.d.). China's Restrictions on FDI are Much Stronger than in the EU and US. Retrieved from https://joint-research-centre.ec.europa.eu/jrc-mission-statement-work-programme/facts4eufuture/china-challenges-and-prospects-industrial-and-innovation-powerhouse/chinas-restrictions-fdi-are-much...

Guterl, F. (2022). Special report: When spyware turns phones into weapons. How zero-click surveillance threatens reporters, sources, and global press freedom. Committee to Protect Journalists. https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/

Hamilton, I. A. (2020). The US says Huawei has been spying through 'backdoors' designed for law enforcement — which is what the US has been pressuring tech companies to do for years. Business Insider Africa. https://africa.businessinsider.com/tech/the-us-says-huawei-has-been-spying-through-backdoors-designed-for-law-enforcement/hbh90yn

In Quest for Increased FDI, FG Sets Up Oil, Gas Investment Promotion Centre. (2022) This Day Live. Retrieved from https://www.thisdaylive.com/index.php/2022/09/26/in-quest-for-increased-fdi-fg-sets-up-oil-gas-investment-promotion-centre/

Institute for Economics & Peace. Global Terrorism Index. (2022): Measuring the Impact of Terrorism, Sydney, March 2022. Available from: http://visionofhumanity.org/resources

International Monetary Fund. (1993). Balance of payments manual (5th ed.). International Monetary Fund.

International Monetary Fund. (2009). Balance of payments and international investment position manual (6th ed.). International Monetary Fund.

Jackson, J. (2008). The Exon-Florio National Security Test for Foreign Investment. Congressional Research Service, https://fas.org/sgp/crs/natsec/RL33388.pdf

Menn, J. (2020). Spy agency ducks questions about 'back doors' in tech products. Reuters. https://www.reuters.com/article/us-usa-security-congress-insight-idUSKBN27D1CS

Meservey, J. (2020). Government Buildings in Africa Are a Likely Vector for Chinese Spying (No. 3476). Douglas and Sarah Allison Center for Foreign Policy. Retrieved from https://www.heritage.org/sites/default/files/2020-06/BG3476.pdf

Nigeria National Security Strategy, 2019. ONSA.

OECD Secretariat. (2020). Acquisition- and ownership-related policies to safeguard essential security interests: Current and emerging trends, observed designs, and policy practice in 62 economies. Retrieved from https://www.oecd.org/investment/OECD-Acquisition-ownership-policies-security-May2020.pdf

Organization for Economic Cooperation and Development (OECD). (1996). Detailed benchmark definition of foreign direct investment (3rd ed.). OECD Publishing.

Onuoha, F.C and M. Ogbonanya (2020). Review and Analysis of Nigeria's National Security Strategy. Accountability Brief: Policy Brief on Nigeria National Security 2019. Partners West Africa Nigeria, 20th May,

Rickards, J. G. (2009). Economic Security and National Security: Interaction and Synthesis. Strategic Studies Quarterly, 3(3), 8-49. https://doi.org/10.1080/10220461.2022.2075913

Smith, M (2023). "Air Force says proposed Chinese-owned Mill in North Dakota is significant threat" The New York Times, January 31

The World Investment Report 2014 provides a methodological note titled, Investing in the SDGs: An Action Plan.

Tribune Online. (2020, August 10). Ups and downs of MTN Nigeria 19 years after. Retrieved from https://tribuneonlineng.com/ups-and-downs-of-mtn-nigeria-19-years-after/

Ungerer, C. (2008). A new agenda for national security. Australian Strategic Policy Institute. https://www.jstor.org/stable/resrep03892

Ünver, H. A. (2018). Politics of digital surveillance, national security and privacy. Centre for Economics and Foreign Policy Studies. Retrieved from https://www.jstor.org/stable/resrep17009

United States Library of Congress. (n.d.). The Colonial Economic Legacy. In Nigeria: A country study (pp. 52-53). Retrieved from https://countrystudies.us/nigeria/52.htm

Uzoho, P. (2021). Nigeria's contract with Canadian firm pulled power sector. This Day. https://www.thisdaylive.com/index.php/2021/05/10/nigerias-contract-with-canadian-firm-pulled-power-sector/

Watson, C. A. (2008). U.S. national security: A reference handbook. (2nd ed.). ABC-CLIO. Retrieved from https://books.google.com/books?id=Zk4HRd0NbX4C