Mapping the supply of surveillance technologies to Africa

Ghana country report

Oyewole Adekunle Oladapo and Gifty Appiah-Adjei

DOI: 10.19088/IDS.2023.027

1. Introduction

This report focuses on Ghana and addresses the types of surveillance technologies Ghana has acquired, the suppliers of those technologies, and their impacts on society. Ghana is central to the discourse on freedom in Africa. In 1957, it became the first British West African colony to attain political independence and, although the democratic governance instituted then was short-lived due to military interventions, Ghana's sustained peaceful transition of power since the restoration of democracy in 1993 has been a key democratic advancement on the continent. However, given Ghana's fast-changing intelligence-gathering technological capability, it is imperative to map Ghana's surveillance technologies to have a view of what the future of human rights in the country holds.

The report is structured in six sections: this introduction provides a general justification for the report; section 2 presents the background, which situates surveillance practices in Ghana in a historical and political context; section 3 documents Ghana's technological policies and practices which create a favourable atmosphere for surveillance; section 4 presents existing evidence on the impact of illegal surveillance in Ghana; section 5 recommends measures to make surveillance compatible with human rights; and section 6 presents cases of individuals whose life stories illustrate the dangers of rights-violating surveillance.

2. Background

Independent Ghana inherited the baggage of a colonial intelligence system. Codenamed Special Branch, and started in 1948 by the British colonial government, it was said to have masterminded the coup that truncated Ghana's nascent democracy in 1966 (Africa 2009; Arnold 2020). The Ghana Police Special Branch was saddled with the responsibility of collecting security-relevant information and disseminating it to a select few members of the government (Arnold 2020). Arnold noted that before the independence of Ghana, the colonial government either destroyed or relocated to the UK all records relating to the country's security and intelligence matters. However, the attempt at completely erasing any memory of colonial intelligence was unsuccessful and Special Branch's structure persisted in independent Ghana. It was noted that from the 1966 coup to the late 1980s there was a sustained decrease in the staff strength of Ghana's intelligence agencies (Africa 2009). However, nothing suggests that this resulted in a weakened state capacity for intelligence-gathering. Rather, it has been revealed that none of Ghana's intelligence agencies were referred to in the laws of the country until the passage of Act 526 of 1996 (*ibid.*), suggesting that operations of the intelligence agencies in Ghana from independence to 1996 were in fact extra-legal (*ibid.*). In such an environment, where no explicit laws guided the operation of intelligence-gathering agencies, abuse could hardly be ruled out.

These historical trajectories point to the likelihood of independent Ghana using its intelligence-gathering agencies for citizen surveillance. Yet Ghana's democratic profile has remained stellar compared to most African democracies. For example, Freedom House has consistently ranked Ghana free (Freedom House 2022) and only Mauritius ranked ahead of Ghana in the Economist Intelligence Unit's (EIU) typology of African democracies. Although Ghana and five other African countries were considered 'flawed democracies' in an EIU ranking, they performed better than the scores of other African countries ranked as either 'hybrid' or 'authoritarian regimes' (Economist Intelligence 2021). In addition, with a score of 43 out of 100 and a rank of 73 out of 180 countries in 2021, Ghana's corruption perception index is low compared to most African countries (Transparency International 2022). Regarding adherence to the principles of the rule of law, the World Justice Project ranked Ghana 58 out of 139 countries globally, and seven out of 33 countries regionally, in its Rule of Law Index 2021.

Despite the relatively positive outlook, Ghana has recently witnessed a slight regression in its rankings. Its Rule of Law Index decreased by 2.2 per cent

in 2021 and its Freedom House Ranking dropped by two points in 2022. Its Internet Freedom Ranking has been consistently ranked 'partly free' for the past five years (Freedom House 2022). On a closer look, it can be seen that what is going wrong with rights and freedom in Ghana did not start in just those five years. Freedom of expression and the right to privacy have been compromised for some time. Odartey-Wellington (2014) chronicled eight cases of leaked tapes of personal, confidential conversations involving highly placed politicians of ruling and opposition parties, all the leaks taking place between 1999 and 2013 in a democratic Ghana. Although the means through which the tapes were recorded remains largely unknown, and interested parties to the leaked conversations questioned their authenticity in some cases, illegal surveillance cannot be ruled out.

As its positive democratic ratings are decreasing, so Ghana's cases of human rights abuse are increasing. There are documented cases of arbitrary arrests and excessive use of unnecessary force against journalists, civil society actors, and protesters (Freedom House 2022). In February 2021, Ibrahim Mohammed, an activist in the Ashanti Region, was attacked by assailants and died two days later (*ibid*.). In February 2022, Oliver Barker-Vormawor, founder of the #FixTheCountry protest movement, was arrested, imprisoned for two months, and had his passport confiscated (Akinwotu 2022). In June 2022, 29 Arise Ghana protesters were arrested by the police, while a combined force of the police and the military shot dead two protesters and wounded four others at Ejura Sekyedumase in the Ashanti Region (Freedom House 2022).

These growing cases of intolerance for dissent coincide with the government's increased possession of surveillance technologies and citizens' private data. Amidst growing concern about human rights violations, Ghanaian and foreign media houses have published stories alleging that Ghana has taken possession of and used surveillance technologies to spy on its citizens in recent years (Dogbevi 2022). Ghana is among countries implementing the safe city project powered by Chinese Huawei artificial intelligence (AI), and Ghana's Cybersecurity Act, passed in 2020, makes it legal for the government to conduct surveillance on citizens and retrieve data from the country's mobile network service providers in the interest of national security.

Reactions to the news of Ghana's purchase of NSO Group's Pegasus spyware reinforced this need, generating as it did considerable concern about citizens' rights to privacy and general human rights in Ghana (Dadoo 2022a). While Ghanaian activists and civil society organisation actors believed they were targets of illegal surveillance (*ibid*.), Pegasus software was found to have been used to target journalists and opposition politicians

in other countries that purchased it, confirming their fears (Dogbevi 2022). Although key actors in the spyware purchase and use were tried, only former government officials involved were jailed while NSO's local representative in Ghana was discharged and acquitted (*ibid*.). The situation became even more worrisome when a Ghanaian high court found the Government of Ghana guilty of breaching the country's Data Protection Act by collecting mobile phone subscribers' personal information (Dadoo 2022a).

With this record of violation of the country's privacy law to access citizens' sensitive data, and its confirmed digital technological capability for surveillance, it is incontrovertible that there is a need for a strong system of oversight from different sections of society. This is to keep the Ghanaian state's use of surveillance technologies both legal and sensitive to human rights and freedom.

3. Supply of surveillance technology

Having established that the Ghanaian state possesses the digital technological capability for surveillance and has a record of illegal access to citizens' personal information, it is important to know the sources and types of surveillance technologies Ghana has acquired. This is necessary as suppliers of surveillance technologies vary in their compliance with good international practices. It is also useful to map the type of surveillance technologies as their capabilities vary just as their potential for illegal use.

The documentation will serve two purposes: it will, first, guide local and international efforts to keep the country's use of the technologies under check; second, it will guide efforts to know exactly what signs to look out for to determine if the technologies are being used for illegal surveillance. Of interest are surveillance technologies that can intercept the internet and mobile telecommunication services, monitor social media, record citizens' public lives, and capture citizens' biometric information. These are examined in the next five sections.

Internet interception

Before the Ghanaian general elections of 2016 and 2020, there was widespread fear that the government would shut down the internet. Election-related 'fake news' was becoming a threat to the peaceful conduct of a free and fair election. Just before the 2016 election, the then country's Inspector General of Police, John Kudalor, revealed that the security agency considered shutting down access to social networking sites to curb the spread of disinformation. The development coincided with the launch of the #KeepItOn campaign,[1] with its primary objective of fighting internet shutdowns worldwide. Civil society groups in Ghana and other countries pressured the government to abort the planned shutdown, and a few months before both the 2016 and 2020 elections, the government assured Ghanaians there would be no shutdown, living up to its word (Akwei 2016; Olukotun 2016; Christian 2020; Muya 2021). Ghana thus remains one of the African countries without a history of internet shutdown or denial of access to social media platforms.

1 Founded in 2016, the **#KeepItOn** coalition comprises over 280 organisations from 105 countries mobilising against internet shutdowns around the world.

Mobile interception

Ghana's Anti-Terrorism Act 2008, Electronic Communications Act 2008, and Cybersecurity Act 2020 provide legal grounds for the interception of mobile communications, and the power of mobile interception may be used in the interest of 'national security'. Worryingly, the term 'national security' is not defined explicitly in law, its interpretation being left open to whatever those authorised to exercise the power consider national security to mean. In the Cybersecurity Act 2020, this power is reserved for top government officials such as the president or security personnel from the rank of Assistant Commissioner of Police and above.

Despite the procedures established by the relevant laws for mobile communication interception, Ghana was found to have acquired Pegasus from NSO Group, an Israeli company, for US$5.5m in 2016 (Dadoo 2022a; Dogbevi 2022). Pegasus is a powerful spyware that can remotely access a mobile phone's contents and location information and use its functions such as the microphone and camera to generate live feeds. An advanced version of the Pegasus spyware can secretly install itself on the target's phone without the target needing to click a link; all that is needed is access to the phone through a vulnerable application (Gurijala 2021).

Although NSO Group claimed that Pegasus was never operational in Ghana, evidence points to the contrary as some of its employees confessed to having trained Ghanaian officials on how to use the spyware (Benjakob 2022). Some Ghanaian activists alleged that they, alongside journalists and political opposition, were the targets of the spyware (*ibid.*). To allay public fears, the Government of Ghana tried former government officials for their roles in procuring the spyware and those found guilty were jailed (Dogbevi 2022). Nevertheless, investigators were reported to have hit a brick wall in their attempts to talk to Ghanaian journalists, government officials, and security personnel about the spyware, creating grounds to suspect that it is still in use in the country (Dadoo 2022a, 2022b).

In addition to its array of surveillance technologies, Freedom House (2021) cites a report of the then director of Ghana's Criminal Investigation Department (CID), Maame Yaa Tiwaa Addo-Danquah, confirming that the country's security forces had access to Israeli company Cellebrite's digital forensics, a tool she stated was used for decrypting encrypted devices. The Government of Ghana claimed that the hacking tool was a gift from the US, UK, and Interpol (Rozen 2020).

Ghana acquired spyware technology from two other Israeli companies, Quadream and Mer Group. Ghana also acquired telecommunication interception technology from an unnamed Swiss company. The details of these technologies and their costs are shrouded in secrecy.

Social media monitoring

Social media monitoring is another popular means through which governments illegally access citizens' personal information and Ghana was found to have engaged the services of Cambridge Analytica, a British ('political consulting') company known for the illegitimate use of Facebook data to covertly target voters. Cambridge Analytica rose to infamy with the revelation that it had meddled in the 2016 US presidential election and influenced the UK's Brexit referendum of the same year with information from the Facebook accounts of millions of voters that they had illegally accessed (*Ghana Web* 2020). However, available information shows that the operation of Cambridge Analytica in Ghana was not based on social media data, but on a dataset generated from a 30,000-respondent survey commissioned in 2014 by the country's Ministry of Health for the purpose of health policy planning (*ibid.*). Proof of Cambridge Analytica's hacking of Ghanaians' social media accounts has been hard to find as the company's operation in the country became public.

Nevertheless, the social media space in Ghana is not free from political influence. As Freedom House (2021) reported, Ghanaian politicians employed the services of paid social media commentators to shape opinions on social media platforms. Whether they employed technology to achieve the same goal is not yet public knowledge.

Meanwhile, Reporters Without Borders cited two cases in which journalists were either arrested or imprisoned over their social media posts. Kwabena Bobie Ansah, a presenter at Accra FM, was jailed for falsely alleging in a social media video that Ghanaian President Nana Akufo-Addo's two wives acquired state land through fraudulent means, and Oheneba Boamah Bennie, a journalist and owner of Power FM, was handed a two-week jail term and a fine over a Facebook video alleging that President Nana Akufo-Addo bought over judges to secure victory over his rival in the courts. These cases, both involving the president, offer up an understanding about the Government of Ghana's low tolerance level for social media freedom.

Smart city/safe city projects

Ghana is implementing a comprehensive smart city project that cuts across different aspects of societal life. A memorandum of understanding for a US$300m component of the project, ArisCel, was signed in 2019 by Celltel Networks, Roberta Annan Consulting, and China National Electronics Import & Export Corporation. Celltel secured approval to start implementing the project in December 2021 (Techfocus24 2021). The project seeks to provide countrywide WiFi connectivity and access to digital devices such as mobile phones, tablets, laptops, and smart TV sets – a good initiative considering

the number of opportunities that come with it. Nevertheless, such connectivity increases the government's potential to conduct technology-enabled surveillance, even in the remotest locations.

More importantly, Ghana is implementing a safe city project, the Integrated National Security Communications Enhancement Network (ALPHA) project. Of particular interest is its facial recognition CCTV camera component. These CCTV cameras are being installed around Accra, Ghana's capital city, its regional capitals, entry ports, and other state infrastructure, and are powered by Chinese company Huawei's facial recognition AI. The Government of Ghana signed a contract with Beijing Everyway Traffic & Lighting Technology and Huawei Technologies in 2012 for Phase 1 to install 800 CCTV cameras. The contract was worth US$176m. The contract for Phase 2 of the project, to install 8,400 CCTV cameras, was signed in 2018 (*Whatsup News* 2021). Phase 2 was financed with US$200m from the Export-Import Bank of China and US$35.5m from Barclays Bank of Ghana. Other components of the project, detailed in a project agreement document retrieved from the Parliament of Ghana Library, include the installation of 50 automatic number plate recognition (ANPR) devices at checkpoint sites, expansion of an existing data centre and establishment of a backup data centre, a video transmission network, and an intelligent video analysis system.

Although Huawei maintains that its surveillance system is for public safety and improved security, the abuse of the technology in other countries raises concerns. In Uganda, for example, the same Huawei AI-powered facial recognition technology was used to target for arrest hundreds of supporters of opposition politician Bobi Wine (Nkwanyana 2021). Since living under a siege of surveillance technologies leads to datafication of even private aspects of citizens' lives, there is the fear that governments, makers of the technologies, and hackers could use remote access to data for illegal or harmful purposes.

As surveillance technologies fast become a ubiquitous feature of major cities around the world, people are becoming tolerant of surveillance in public places. However, when the same technologies are used to target and access personally identifying information about individuals or groups, such use compromises their right to privacy and violates the legal protection that the constitutions of many countries assure their citizens.

Biometric ID

Ghana has multiple biometric identification systems. In addition to its national passport, which is strictly for citizens, the country is implementing a biometric identification system known as the Ghana Card for all Ghanaians

at home and abroad and all legal permanent residents in Ghana. Holders of the card are expected to link it to their SIM cards and proceed to the service centres set up by telecommunications companies to have their biometrics captured.

It is noteworthy that the Ghana Card is the exclusive means of identification that is acceptable for SIM card registration in the country. As of November 2022, about 30 million SIM cards had been partly linked to Ghana Cards while almost 21 million SIM cards had been fully linked, having completed the biometric capturing. In all, the two constituted about 70 per cent of SIM cards operational in Ghana at that time (Macdonald 2022). The Government of Ghana had issued deadline after deadline for the completion of the registration and threatened to disconnect all SIM cards not fully registered (Adu-Gyamfi 2022). The 31 October 2022 final deadline was eventually upheld with data access restriction placed on partly registered SIM cards and 5.7 million unregistered SIM cards – resulting in the disconnection of about a quarter of the subscribers to one mobile company, MTN, alone (Macdonald 2022).

In addition, the Bank of Ghana issued a directive to all banks operating in the country to accept only the Ghana Card for financial transactions from 1 July 2022. The effective date for implementation was later set as 1 January 2023, but with this development, all financial transactions in Ghana became linked to the biometrics of those who initiated them.

When the policies become fully implemented, the Ghana Card will become the exclusive means of identification for accessing both mobile telecommunication and banking services in Ghana.

Table 3.1 Supply chains of surveillance technology

Contract	Description (contract date, buyer/user)	Cedis	US$
Internet interception			
Unknown			Unknown
Mobile interception			
NSO Group (Israel)	Pegasus – mobile communication interception (2016)	21.45m	~ 5.5m
Cellebrite (Israel)	Digital forensics for decryption of encrypted devices (unknown)		A gift from the US, UK, and Interpol
Quadream (Israel)	Spyware (unknown)		Unknown
Decision Group (Taiwan)	Network monitoring (2016)		Unknown
Tactical Devices (Switzerland)	Telecommunications interception/jammer (2015)	22,000	~ 5,000
Intellexa, Greece	Unknown		5.66m
Social media monitoring			
Unknown			Unknown
Safe cities			
Phase I: Beijing Everway Traffic and Lighting Technologies (China); Huawei Technologies (China)	800 facial recognition CCTV cameras (2012)	334.4m	176m
Phase II: Chinese companies	8,400 CCTV cameras, 50 automatic number plate recognition devices, data centre, video transmission network, and intelligent video analysis system (2018)	10.81m	2.35m
Biometric ID			
Unknown			Unknown
	Total	366.7	184m

Source: Authors' own. Created using data from Edin Omanovic's Surveillance Technology suppliers' database, and Ghana's Safe City (ALPHA) project contract document retrieved from the Parliament of Ghana Library.

Note:The conversion rate for 2012 from **United States Dollar(USD) To Ghanaian Cedi(GHS) Exchange Rate on 31 Dec 2012 (31/12/2012)**. For all other years, from Statista: **Annual average exchange rate of U.S dollar in Ghanaian cedi (GHS) from 2016 to 2022.**

4. Impacts

The secrecy surrounding the procurement and use of surveillance technologies in Ghana makes it difficult to measure the impact of their use for illegal purposes. Nevertheless, knowledge of the Government of Ghana's surveillance capability has created a sense of siege among activists, journalists, and opposition politicians. This results from living under the gaze of CCTV cameras, with every item of personally identifying information stored up in government and organisational databases.

Fears have been intensified by the illegality involved in the acquisition of the Pegasus spyware and the later reports that it was used in the country, contrary to the government's initial claims. Activists and dissidents believe that the Government of Ghana used the technologies to spy on them (Dadoo 2022a).

Meanwhile, Oliver Barker-Vormawor founded Ghana's #FixTheCountry movement to demand accountability, good governance, and better living conditions for Ghanaians. The activities of the movement brought him into conflict with government and security agencies, and he shared a story of how the phone of a member of the movement he leads became hacked after meeting with National Security officials. It was observed that calls from the phone 'began being diverted to an unknown number' (Dadoo 2022a, 2022b).

Expressing his worries over illegal surveillance in Ghana, Dogbevi, a member of the International Consortium of Investigative Journalists, was quoted as saying: 'If a state agency can decode my system without access to my password, that is scary (Rozen 2020). While worrying that he too might be a target of illegal surveillance, Dogbevi was further quoted: 'Sources send me information, send me documents. I wouldn't want anyone to have access to that' (*ibid.*).

Secrecy in Ghana creates an environment in which illegal surveillance can thrive. Why? The public does not have sufficient information about surveillance technologies and their use. As a result, it is difficult to hold the Government of Ghana to account for them.

5. Solutions

With the Government of Ghana's growing capacity for surveillance and the possibility of the government and its security agencies violating the legal protection that laws of the country give citizens against illegal surveillance, Ghanaians, especially activists, journalists, and protesters, have no choice but to adapt to living and working in a state under surveillance.

First, it requires capacity building for improved data literacy and data security; individuals and groups have to adjust their actions, especially those carried out on digital devices. Investment in sophisticated anti-spyware solutions is also important. When kept up to date, anti-spyware solutions can save individuals and groups from attacks that compromise their privacy.

The laws guiding the procurement of surveillance technologies in Ghana must also be revisited to identify and block those loopholes that enable the government to execute secret procurement. For a full appraisal of Ghana's public surveillance situation to be possible, litigations may be necessary. The government has not shown a willingness to divulge information about its surveillance capacity, so it will take pressure from civil society organisations (CSOs), and the judgement of a court of competent jurisdiction, to compel it to do so. This will require CSOs to engage in coalition building to demand this accountability.

Meanwhile, for the courts to function effectively as a last resort for securing accountability in the use of public surveillance technologies, the independence of the Ghanaian judiciary must be protected and preserved. Relevant laws of Ghana make judicial approval a precondition for accessing citizens' information to ensure that government does not engage in the illegal surveillance of citizens. In cases of the violation of such laws, it takes a truly independent judiciary to convict the government of its illegality.

6. Surveillance stories

Illegal surveillance has devastating effects on people. Whether real or perceived, the threat of surveillance results in people modifying substantial aspects of their lives and work. For journalists, the extent to which they can use confidential sources is limited significantly (Waters 2017). Illegal surveillance costs investigative journalists access to important stories that could not be broken without others agreeing to provide information unobtainable through conventional journalistic approaches.

Further, the challenges are now real, not only for journalists but for everyone who uses digital devices (and the use of these has permeated every aspect of human endeavour). Victims of illegal surveillance tell of how the acts resulted in experiences that left them in excruciating pain, altered significant aspects of their lives, and curtailed their freedom of expression, rights to privacy, and personal liberty.

In the case of Ghana, such stories are hard to find – which is strange given the surveillance capacity of the Government of Ghana and the country's history of an unholy alliance between intelligence agencies and highly placed government officials. Confirmation that the Pegasus spyware was used in the country specifically to target journalists makes the situation disturbing. The absence of stories of people whose lives have been impacted by illegal surveillance does not prove there was no illegal surveillance. It is a pointer to something ominous: an environment that silences victims.

Stories of how Ghanaian security agencies brutalised citizens in recent years confirm the abusive credentials of these agencies. That they were always interested in the contents of their victims' digital devices is a pointer to their hidden surveillance agenda. Nyabor (2021) told how an editor for ModernGhana.com, Emmanuel Ajarfor Abugri, was arrested in July 2019 alongside a reporter, Emmanuel Yeboah Britwum, and tortured by the police:

> *They slapped me and used a taser on both arms… They also made me go 'head down legs up' against a wall. I did this till I could no longer continue then they hit my back and I fell. They commanded me to do some push ups. I got exhausted and couldn't do it anymore. One officer pulled me up by my trousers and another knocked my back with his elbow, and I fell again.*

Another journalist, Caleb Kudah, suffered a similar fate in the hands of Ghanaian security agents. Nyabor (2021) also related Kudah's account of his ordeals:

> *They pushed me in a chair and slapped me from the back… They took me under a mango tree. One officer came and asked me to kneel down. He kicked me in the groin and gave instructions for me to be beaten… The officers remarked that I'm a dead man since they've been instructed to 'deal' with me. I was commanded to do 30 push ups… I was so tired and fell on the ground. They hit me in the back… When they said I needed to write a statement, one officer said he will dictate some things for me to write.*

In the account provided by Nyabor, the officers accessed Kudah's mobile phone and communicated to a colleague of Kudah's who was later arrested for reasons not explained. Recounting his ordeals to *The Guardian*, the #FixTheCountry movement activist Oliver Barker-Vormawor stated that after having been severely tortured, he was blindfolded and taken in a convoy of police and military vehicles to a cell on the outskirts of the city, where he was stripped and forced to give officers access to his phone. Meanwhile, Emmanuel Ajarfor Abugri and his journalist colleague were arrested together and had their phones and laptops confiscated and accessed by police officers. Upon their release from custody, only their phones were returned; the police held on to their laptops (Committee to Protect Journalists 2019). These experiences confirm Ghanaian security agencies' interest in citizens' personal communication, the same interest behind illegal surveillance.

References

Adu-Gyamfi, K. (2022) '**Ghana to Block all Unregistered SIM Cards after October**', *Africanews*, 18 October (accessed 8 January 2023)

Africa, S. (ed.) (2009) ***Changing Intelligence Dynamics in Africa***, African Security Sector Network (ASSN) and Global Facilitation Network for Security Sector Reform (GFN-SSR) (accessed 10 February 2023)

Akinwotu, E. (2022) '**Ghana "Fix the Country" Activist Says He was Assaulted and Illegally Detained**', *The Guardian*, 14 July (accessed 10 February 2023)

Akwei, I. (2016) '**Ghana Stands to Lose if Internet is Shut Down on Election Day**', *Africanews*, 12 June (accessed 10 January 2023)

Arnold, C. (2020) ' "The Cat's Paw of Dictatorship": Police Intelligence and Self-Rule in the Gold Coast, 1948–1952', *The Journal of the Middle East and Africa* 11.2: 161–77

Benjakob, O. (2022) '**NSO Ghana Op Exposed: Never-Before-Seen Pegasus Spyware Footage, Workers' Passports**', *Haaretz*, 20 January (accessed 22 November 2022)

Christian, A. (2020) '**The Ghana Internet Shutdown Conundrum is Disturbingly Entangled in Press Mis-Reportage**', *WT*, 10 February (accessed 10 January 2023)

Committee to Protect Journalists (2019) '**Two Ghanaian Journalists Arrested and Interrogated, One Allegedly Tortured in Custody**', *CPJ*, 9 July (accessed 10 January 2023)

Dadoo, S. (2022a) '**Is Ghana's Government Using Israeli Kit to Spy on Activists and Dissidents?**', *The Africa Report*, 21 July (accessed 22 November 2022)

Dadoo, S. (2022b) '**Israel's Spyware Diplomacy in Africa**', *Orient XXI*, 12 September (accessed 10 January 2023)

Dogbevi, E.K. (2022) '**Revealed: Israeli Tech Company NSO's Pegasus Was Used in Ghana – Reports**', *Ghana Business News*, 22 January (accessed 22 November 2022)

Economist Intelligence (2021) ***Democracy Index 2021: The China Challenge*** (accessed 22 November 2022)

Freedom House (2022) ***Freedom in the World 2022: Ghana*** (accessed 22 November 2022)

Freedom House (2021) ***Freedom on the Net 2021: Ghana*** (accessed 22 November 2022)

Ghana Web (2020) '**Election Leaks: Did Cambridge Analytica Play NDC and NPP Ahead of 2016 Polls?**', 28 February (accessed 22 November 2022)

Gurijala, B. (2021) '**What is Pegasus? A Cybersecurity Expert Explains how the Spyware Invades Phones and What It Does When It Gets In**', *The Conversation*, 9 August (accessed 10 February 2023)

Macdonald, A. (2022) '**Ghanaians Encouraged to Complete Biometric Capture for SIM Registration as Deadline Nears**', *Biometric Update*, 28 November (accessed 9 January 2023)

Muya, C. (2021) '**Internet Shutdowns and the Future of African Democracy: What More Can We Do?**', *Open Internet for Democracy*, 7 April (accessed 8 January 2023)

Nkwanyana, K. (2021) '**China's AI Deployment in Africa Poses Risks to Security and Sovereignty**', *The Strategist*, 5 May (accessed 9 January 2023)

Nyabor, J. (2021) '**Ghana: Arbitrary Arrests & Torture of Journalists, How Free is the Press?**', *The Africa Report*, 26 May (accessed 9 January 2023)

Odartey-Wellington, F. (2014) 'Technological Invasion of Privacy: The Need for Appropriate Responses to the New Surveillance Society in Ghana', *CDD-Ghana Briefing Paper* 13.4: 1–10

Olukotun, D. (2016) '**Victory! President of Ghana Says No to Internet Shutdowns During Coming Elections**', *Access Now*, 16 August (accessed 10 January 2023)

Rozen, J. (2020) '**US, UK, Interpol Give Ghana Phone Hacking Tools, Raising Journalist Concerns on Safety and Confidentiality**', *CPJ*, 14 July (accessed 4 January 2023)

Techfocus24 (2021) '**Celltel Set to Begin US$300 Million Ghana Smart Cities Project**', *News Ghana*, 24 December (accessed 8 January 2023)

Transparency International (2022) ***Corruption Perceptions Index: Ghana*** (accessed 10 February 2023)

Waters, S. (2017) '**The Effects of Mass Surveillance on Journalists' Relations with Confidential Sources**', *Digital Journalism* 6.10: 1294–1313, DOI: 10.1080/21670811.2017.1365616 (accessed 24 April 2023)

Whatsup News (2021) '**Gov't 10,000 Surveillance Cameras to be Completed by December**', 4 November (accessed 9 January 2023)