ISSN 2643-6388

IJCSS

INTERNATIONAL JOURNAL OF COMMUNICATION & SOCIAL SCIENCES

VOLUME 1 NO. 4

PUBLISHED BY THE FORMER DEAN OF GRADUATE SCHOOL
BOWIE STATE UNIVERSITY, BOWIE, MD, USA
in collaboration with
THE DEPARTMENT OF MASS COMMUNICATION
GODFREY OKOYE UNIVERSITY, ENUGU, NIGERIA

International Journal of Communication and Social Sciences (IJCSS)

VOLUME 1 No. 4

INTERNATIONAL JOURNAL OF COMMUNICATION AND
SOCIAL SCIENCES (IJCSS) VOLUME 1 NO. 4

ISBN (print): 978-1-09-906198-1
ISSN (print): 2643-6388
ISSN (online): 2643-6396

Printed in the United States of America
Fourth Printing, 2024

Editor's note: The material in this Journal is presented with minimal edits for technical items only. Contributors' content, regional and cultural verbiage, locution, spelling, and language usage in their original form to retain each authors' narrative voice and authenticity.

9

SPYWARE AND SURVEILLANCE OF JOURNALISTS AFRICA

Desmond Onyemechi Okocha, Ph.D.
Department of Mass Communication,
Bingham University, Nigeria
Email: desmonddoo@yahoo.com

Michael Faloseyi
Department of Mass Communication
Bingham University, Nigeria
Email: mfalosh@gmail.com

ABSTRACT

Information and communication technology has aided the practice of journalism as much as generated concern over an observable growing trend in the deployment of spyware and surveillance technologies around journalists in Africa. This study investigated the integrity of this trend and the level of awareness about this development among journalists on the continent. Additionally, the motivating factors among governments on such deployment were investigated. Notwithstanding some of its shortcomings over its inability to produce consistent results, the protective motivation theory provided the theoretical framework for this investigation. Fear as a stimulus factor motivates individuals or the government, in this instance, to act to mitigate or evade inevitable consequences. The government's consideration of journalists as a source of fear motivates the deployment of spyware and surveillance technology. The study used the qualitative research approach. Twenty-two participants, including journalists, security experts, and other media professionals, were purposively selected from Nigeria, Ghana, Liberia, South Africa, Kenya, Uganda, and Rwanda for focus group discussions. The study findings align with previous examinations of this phenomenon as they confirmed the growing trend of deployment of spyware among governments around journalists. Nonetheless, the rising incidences of those using spyware for fraudulent activities obfuscate journalists' ability to perceive when being watched by the government. Therefore, the need for media houses to invest in journalists' capacity to detect spyware and surveillance. Governments must draw a clear distinction between public interest and national security, which was identified as the only justification for using spyware and surveillance around journalists.

Keywords: Journalists, national interest, public interest, spyware, surveillance

■ ■ ■

INTRODUCTION

Information and communication have immensely benefited journalists in discharging their responsibilities. Observable developments also point to the fact that technology could pose specific security challenges for professionals in the media industry. Chapter 4 Section 39 of the 1999 Nigerian Constitution as amended recognises citizens' right to freedom of expression and the press. Arguments can be posited that the constitutional provision does not guarantee special protection for journalists other than what other citizens are entitled to in exercising their freedom of expression and the press. Even in countries without such constitutional provisions, freedom of expression is considered one of the Fundamental Human Rights to which United Nations member states consented.

Nonetheless, journalists, as members of the fourth estate of the realm, have both the ethical and professional responsibilities to hold the government and those in authority to account. The performance of that responsibility may be considered one of the reasons media professionals are exposed to bruises from security agencies and politically exposed individuals wielding power and instruments of office. There have been instances of death in controversial situations. For example, in Nigeria, Mr. Dele Giwa, Editor-in-Chief of the then flagship magazine, Newswatch, in 1982, and Mr. Bagauda Kaltho of The News Magazine in 1995 died in controversial circumstances through explosions (Adike, 2013). In a report published in the April 14, 2023, edition of The Guardian, Mr. Anas Aremeyaw Anas, a Ghanaian journalist reputed for his interest in exclusive stories, lamented the fate of African journalists who are being subjected to repressive security surveillance and death threat calling attention to this trend in his country and the continent. The story narrated the circumstances surrounding the death of Martinez Zogo, a Cameroonian radio journalist while investigating a corruption allegation around a businessperson, Jean-Pierre Amougou Belinga.

Notwithstanding the right of expression and the press, there is a constitutional provision for the right to privacy under which individuals can resist press investigation. Ironically, both are fundamental human rights enshrined in the 1966 International Covenant on Economic, Social and Cultural Rights and the International Labour Organisation Conventions on Fundamental Human Rights. Despite the constitutional provisions and safeguards at the international relations levels, governments across development profiles have found reasons to oppose exercising these rights. Some scholars like Adeyeri and Ogunniyi (2016) have argued that these rights are observed in breach by most governments as strict application of the rights sometimes implies curtailing state power. This submission resonates with the 2022 Reports by the States Department on Human Rights Practices, where most governments, especially Nigeria, were indicted for their interest in the media through surveillance activities aided lately by the deployment of spyware technology.

For instance, the Moroccan government upscaled surveillance activities immediately after the Spring through massive deployment of spyware around media houses and journalists (Iddins, 2019). Similarly, in a report by Woodhams (2021) for the Center for International Media Assistance and National Endowment for Democracy on Pegasus Initiative, it was unraveled how over 180 journalists, activists, lawyers, and diplomats, among other professionals from over a dozen countries, have had their telephones or computers targeted by their respective government using the Israeli spyware company NSO Group's products. Eighty journalists promote the Pegasus Initiative from 17 media houses to investigate how

autocratic regimes use NSO Group's products against journalists, human rights activists, and political opposition. McCullagh (2013) disclosed that NSO's products are made exclusively for law enforcement agencies and intelligence communities to facilitate their careful monitoring of individuals. Nevertheless, another Italian company, Hacking Team, before being bought by Memento Laboratory, produced products capable of remotely invading a victim's telephone and computers (Vardalaski, 2014). The company, whose initial market was limited to Italy and Spain, now have among its clientele over forty countries, including African countries, which are massively these products around journalists.

While it is observable that surveillance around journalists may not be a new phenomenon, the prevalence of African governments' engagement in its technologically advanced forms necessitated this study. Beyond the general musing on the rising incidents of spyware surveillance around journalists on the continent, there are limited investigations on the level of spyware surveillance around journalists and the extent of awareness among journalists about the phenomenon. This development is further encapsulated in the statement of the problem.

STATEMENT OF THE PROBLEM

The introduction of the Internet and computers in the media space could be argued as an enabler of almost limitless possibilities, and the media industry is one of the most beneficiaries of technological advancement. Chen et al. (2022) submit that technological advancement has become a two-edged sword. They opined that communication technologies enable limitless interface and communication across devices just as they allow adversaries to cause havoc, including breach of personal privacy, loss of property, money and sometimes lives. Relatedly, Lauer (2011), writing on the advent of the portable camera in the media space, submitted that it was an amusing and enraging innovation due to its capacity to invade people's privacy. The people, as of then, dubbed it a 'surveillance camera.' Meanwhile, advancement has upscaled camera possibilities as it now accessories our telephone, eyeglasses, pen, and computers, among other items. Ironically, these technologies facilitate journalists' access to information and confer authenticity on their reports through voice recording and discreet photographs, among other possibilities.

However, some technologies are now accompanied by software and code that could remotely access information from our system or crash the system outright. They are called spyware, which, according to Iddins (2019), most governments are now investing under the guise of security and national interests to curtail freedom of expression and the press and invade citizens' privacy. For instance, a report by the Washington Post detailed how a US-based television station that beams to Ethiopia had employees' computers and email accounts hacked through suspicious spyware deployed by the Ethiopian authorities. Further reference was made to how Moroccan authorities upscaled its surveillance activities through spyware in the aftermath of the Arab Spring.

Similarly, Hacking Team, an Italian cyber security firm, was, according to McCullagh (2013), listed as a "Corporate Enemies of Free Press." Before it was taken over Memento Laboratory, the Hacking Team touted that its "Remote Control System" or spyware could infiltrate targets' computers and telephones and access information, notwithstanding manufacturing claims against such infiltration. Specifically, one of its products – DaVinci Remote Control, could break encryption and allow access to files, pinpoint target locations, activate microphones and cameras remotely, and control hundreds of thousands of computers remotely several thousand kilometers away, among other possibilities. Meanwhile,

Hacking Team was one of the earliest lawful intercept companies that started operations in about 2003 and specialised in producing spyware and surveillance technologies.

However, beyond massive production and deployment of these items, there are observable concerns about the level of awareness among would-be targets, especially journalists and their ability to adapt to this trend. According to Okocha and Ola-Akuma (2022), there is limited awareness and adaptation technology among media professionals in Nigeria. The study further explored the justification for using spyware for national security or public interest.

OBJECTIVES OF STUDY

The study objectives are to:

1. Examine African journalist's awareness of surveillance technologies.
2. Investigate monitoring of African journalists through spyware surveillance technologies.
3. Ascertain national security and public interest as justifications for spyware surveillance.

THEORETICAL FRAMEWORK

As a professor of health communication at Michigan State University, Rogers (1975) developed the protection motivation theory to explain fear appeal in health communication. Since then, the theory has been used in persuasive and effective audience communication. Other areas of Rogers' (1975) interest include anti-smoking campaigns, communication strategies for family planning, and fear and attitude change. Meanwhile, the protection motivation theory has been used to explain why people act the way they do in certain circumstances. It shall be found suitable as the theoretical basis for this investigation.

Protective motivation theory suggests that people are bound to act in specific ways to protect themselves in threatening situations. Fear was constructed as an affective state that stimulates individuals in self-defenses against danger. The interpretation of an individual problem will provoke an equal reaction to mitigate and avoid the negative consequences of the problem. The theory has been explained by two traditions, one of which conceptualises fear as a motivational intervening variable that makes one act to mitigate or avoid danger. Fear is constructed as the intervening variable that elicits a reaction to either escape or avoid noxious events. Similarly, the protection motivation variable tradition aligns with the positions of some other communication theories about expectancy and value — this entails using communication concepts similar to expectancy and value to explain people's reactions or handling of certain situations. The nature of the expectation or outcome of a problem will dictate the course of action in a specific direction, and the value attached to that outcome will determine the following line of action.

Both ways of explaining protective motivational theory identified three conditions precedent as crucial stimulus variables.

1. The magnitude of the noxiousness of a depicted event explains the estimation of the toxic event, which could indicate the nature and reaction of the individual.

2. The conditional probability that the event will occur provided that no adaptive behaviour is performed, or modification of an existing behavioural disposition is modified.
3. The availability and effectiveness of a coping response that might reduce or eliminate the noxious stimulus.

The theory suggests that fear appeal could present information in any of the three or a combination of the condition's precedent. Notwithstanding, a cognitive mediational process would instigate the necessary response to take care of the fear stimuli. This theory has been used to explain individuals' propensity to engage in attitudes that mitigate fearful situations.

Meanwhile, the protective motivation theory can be criticised for its inability to produce consistent results in its applications or tests. Another shortcoming is that concepts such as fear and emotions with which the theory is built are not measurable.

Notwithstanding this shortcoming, the theory is relevant to this study in finding an explanation for government considerations of journalists or their reportage as a source of fear, especially when activities and policy implementation of the government come under media scrutiny in a manner that could embarrass the government or its agents. This theory shall apply to this study to explain the government's treatment of investigative reporting by journalists as a fear stimulus that could elicit premeditative reactions. The theory could explain the journalist's response to mitigate possible consequences of spyware and surveillance.

The study further explores the digital repression theory, an emerging approach to explaining the use of spyware surveillance to monitor or discourage dissensions. According to Earl et al. (2022), in its original conception, digital repression entails targeted efforts at raising the cost of digital or social media to limit access and, by implication, restrain dissenting voices on social media. However, scholars like Feldstein (2021), in his work on digital technology reshaping power, politics and resistance, have attempted to narrow the approach to the use of Internet and communication technology in carrying out surveillance, coercion, and prevention of individuals or groups from specific activities or beliefs that challenge the position of the state or individuals in authority. This concept explains the attempt by governments to prevent the media from pursuing a line of story or investigation. Nonetheless, this emerging school of thought requires further elaboration and conceptualisation.

LITERATURE REVIEW

The Emergence of Spyware and Surveillance on Journalists

Communication scholars' interest in conducting studies on the application of spyware and surveillance is a recent development. The Merriam-Webster's Dictionary (2004) defines spyware as software secretly installed in a computer or mobile device to monitor or transmit information to the installer without knowing the equipment's owner. Surveillance, however, entails closely monitoring an individual to extract information. It could be argued as the terrain of private security and military professionals. Besides, technological advancements have transformed surveillance from mainly physical to a more discreet and remote activity, especially with the deployment of spyware (Richard & Rigauds, 2014). The study investigates the extent of deployment of spyware for surveillance purposes

around media professionals on the one hand. The study further explored the conditions predisposing journalists and media houses to spyware and government surveillance.

Subsequently, previous literature and studies by communication scholars like Lubber (2015) and Di Salvo (2022) on the deployment of spyware on journalists and reactions generated by media professionals shall be reviewed in this section. Submissions by communication scholars like Bissell (2000) on the impact of photography on journalism agree with that of Okocha and Ola-Akuma (2022) in their study on the adaptation of robots to journalism practice in Nigeria when they submit that technological adaptations could enhance communication. The study's findings with 378 participants revealed that Nigerian journalists know the latest technologies, especially robots and their usefulness in their profession. However, certain conditions and factors ranging from economic, financial, and sentimental attachment to the old ways of doing things still limit such adaptation. That study finding shall be relevant to this investigation as it explains the awareness among African journalists about spyware technologies.

Notwithstanding the level of awareness, media scholars have further argued that technological advancement is a double-edged sword that empowers the government to monitor citizens' communication just as it assists media professionals with their profession while providing platforms for the citizens. For instance, the mobilisation for the 'End SARS protest in Nigeria and the Arab Spring across northern African countries could be argued as benefiting immensely from communication technology.

Nonetheless, scholars like Dragu and Lupu (2021), in their studies on digital authoritarianism, submit to the divided opinion among communication scholars that communication technology assists journalism practices and aids authoritarian regimes to fester. Specifically, the administration in Nigeria, though democratic, became more determined to control the Internet-based communication platforms immediately after the End of SARS, almost bringing the government to its knees. Also, Botswana, rated with the highest incidence of cyber attacks per population ratio on January 12, 2022, passed the Criminal Procedure and Evidence Bill. Part 3 of the Bill permits the interception of citizens' telephone conversations and Internet use by investigating authorities. More governments in Africa are getting more interested in censoring the Internet. It is, therefore, not enough that media professionals are aware of the Internet and other communication technologies but that governments, specifically on the African continent, are becoming more interested in using the same technology to censor the journalism practice, a development identified as digital authoritarianism.

Therefore, this study examines journalists' awareness level about the African government's increasing deployment of spyware and surveillance and the motivating factors for the phenomenon.

Journalists' Awareness of Spyware and Surveillance

Mare (2019), in an exploratory study using qualitative policy examination, document analysis and in-depth interviews on spyware and surveillance, indicates a massive deployment of unlawful communication surveillance occurring in the southern African country of Namibia. However, the study, which has participants drawn from the media, Civil Society Organisations, Windhoek City Police, and regulatory authorities, indicates no data to show Namibia's capacity for spyware and surveillance technology. Nonetheless, there is massive deployment of different types of spyware and surveillance technologies, cameras and equipment targeted at investigative journalists, opposition parties, factions within the rul-

ing party and members of Civil Society Organisations. The report discloses that the deployment is done haphazardly. The study, however, cannot ascertain the level of awareness among journalists and the extent to which they are monitored. Meanwhile, a 2019 United Nations-sponsored study coordinated by the Media Policy and Democracy project identified Namibia as one of the countries with massive deployment of surveillance technology primarily due to political tension and the plural press in that country (Mare, 2019 & Nwilima, 2008).

Similarly, a qualitative study using an in-depth interview study by Lubbers (2015) confirmed that spy infiltration of journalists and activists involves not just secret services but corporate organisations and that such practice in the United Kingdom in the last forty years. At the same time, a content analysis of a BBC television interview by Salter (2015) brought another dimension of awareness to the extent of collaboration, even by media personalities.

Relatedly, Mills (2019) reported on the intensity of surveillance and spyware in twelve countries across three continents: North America, Europe and Africa. He submits the prevalence of surveillance of journalists across liberal, illiberal, and authoritarian democracies. Specifically, the report indicates that 64 per cent of investigative journalists and 71 per cent of foreign relations and security correspondents in the United States were conscious that the US government had collected information about them. They considered using spyware and other electronic surveillance technologies on their telephone, computers, and other work equipment. The findings further indicate that Western democracies increasingly come under the guise of security and national interest to constitute a surveillance society by monitoring social media usage to collect information on citizens.

Contrarily, while a figure can be quoted on awareness of the development in Western democracies, there have been no available statistics on the extent of spyware and surveillance activities on journalists in Africa or the importance of awareness if they are being monitored. For instance, while there has been some pushback through media reports on the Federal Government of Nigeria's attempt to enact an act of the National Assembly to regulate the use of social media, suggestions are rife that some level of monitoring and surveillance of journalists is already going on. Nevertheless, no one could put a tab on the integrity of such suggestions. The scenario may not differ across the continent primarily due to the official secrecy in most bureaucracies.

CONSIDERATION BETWEEN NATIONAL SECURITY AND PUBLIC INTERESTS

Unlike other business entities, the media is not assessed based only on the profit-making yardstick. According to Davis (2014) and Fawzi (2018), the media is assigned a different and more complicated responsibility of watchdogs of our freedom and alert on possible abuse of power by political officeholders. In that capacity, the media hold public officeholders and those in authority accountable. Consequently, communication scholars like Croteau and Honeys (2006) and Christina (2022) submitted that the mass media is the screen on which diverse images are projected for all to see. In performing the responsibility, the media could be argued as the protector of the public interest.

Nonetheless, as identified above, the boundary of what constitutes public interest is sometimes not easily demarcated as governments and political offices gravitate between public and national interests to justify decisions that hamper the free press. According to Ota and Ecoma (2022), the national interest could be ambiguous and omnibus other than

the public interest. It could include items identified as public interest plus national security, as well as the common good of society. Moreover, acting in the national interest, governments have made decisions that limit the people's privacy and freedom of the press. Such actions could include surveillance activities and the deployment of spyware.

Likewise, according to Basu (2000), national interest revolves around maintaining territorial integrity and enhancing a country's status, perception, image, and position about other states. A further argument could be advanced on the fluidity between the two interests as the government sometimes uses those items listed as public to drive national interests. It is, therefore, easy for the government to gravitate between national and public interests in defending its actions. Most governments, therefore, find it easier to explain all actions and activities, including surveillance and deployment of spyware, as acting in the national interest or security. Observably, strong institutions like the Chinese Communist Party, authoritarian leaders like Adolf Hitler, or any other war situation leaders weigh a strong, if not ultimate, influence on their countries' national interest (Ota & Ecoma, 2022).

RESEARCH METHOD

The qualitative research method was used for this study, and data collection was done through focus group discussion. The choice of qualitative method was informed by need for an experiential knowledge, which could be considered best suited for investigating a discreet and complex phenomenon as spyware and surveillance. Consequently, invitations were purposively sent to thirty participants from South Africa, Ghana, Uganda, Rwanda, Kenya, Liberia, Cote d'Ivoire, and Nigeria. The choice of these countries was informed by factors such as history of adversarial press, experience with repressive political government or administration at point or the other and lastly the use of English language as the major medium of expression by their media houses. Five focus group discussion sessions were conducted between April 1 and 16, 2023, with a maximum of five participants in two of the sessions. However, eight invited participants who indicated interest in participating did not turn up for various reasons despite reminders sent about 30 minutes before the appointed hours.

While deciding to participate in the study group was consensual, participants were invited based on their professional background in the media and communication, public relations, security, information and communication technology and public office. The instrument for data collection is a discussion guide with nine (9) open-ended questions. The instrument guided the focus group discussions. In line with ethical practice with the conduct of focus group discussion and the assurance of confidence in the information provided, participants were identified with numbers one (1) to twenty-eight (22) with the prefix SSR to their numbers.

FINDINGS OF STUDY

Demographic representation

S/N	Country	Frequency	Percentage
1	Nigeria	8	36
2	Kenya	3	14
3	Ghana	3	14
4	Cote d'Ivoire	1	5
5	Liberia	2	9
6	Rwanda	2	9
7	South Africa	1	5
8	Uganda	2	9
	Total	22	100%
	Profession		
8	Journalism	8	36.7
9	PR/Advert	9	40.56
10	Security Expert	2	9.09
11	Lawyer	1	4.55
12	ICT Expert	1	4.55
13	Academic	1	4.55
	Total	22	100
	Work Experience		
14	21 years and above	10	45.45
15	16 – 20	8	36.36
16	19 and below	4	18.18
	Total	22	99.99
	Age Range		
17	70 and above	Nil	
18	60 – 69	3	13.6
19	51 – 59	7	31.8
20	41 – 50	8	36.4
21	31 - 40	4	18.2
22	18 – 30	Nil	100
	Total	22	
	Sex		
23	Male	18	82
24	Female	4	18
	Total	22	100

Source: Primary Data (2023)

Demographic details of the study participants indicate four females and 18 males to make up the sample size 22. A breakdown of the data shows that participants were from (8) African countries, including eight (8) Nigerians, three (3) participants apiece from Kenyan and Ghana, two participants from Liberia, Rwanda, and Uganda and one participant apiece from South Africa and Cote D'Ivoire. Professional representations include eight journalists, nine public relations and advertisers, two security experts, one academic and a lawyer. A further breakdown of the data indicates there are four age groupings represented among the participants, with eight (8) of the participants within the age range 41 to 50, age 51 to 59, seven (7) participants within the age of 60 and above were three (3). In contrast, those aged 31 to 40 are four (4) in number. Further findings of the investigations were analysed in line with the study objectives.

RO1: Levels of Awareness and Frequency of Spyware and Surveillance of Journalists in Africa

Most participants demonstrated reasonable awareness of spyware and surveillance technologies. The consensus among the participants was that exposure to any electronic gadget, particularly the Internet, makes one susceptible to surveillance and spyware. Furthermore, being a journalist increases that possibility. On the contrary, using the Internet and developing communication technologies has expanded media opportunities and conferred credibility on media stories. SSR 3 opined that the print media at inception was not conceptualised to run live coverage of events. That was an exclusive preserve of the broadcast media.

On the contrary, the Internet has enabled online newspaper versions to update their reports as events unfold. He concluded with his interventions that the possibility of conducting a focus group interview across international borders using Google Meet is one of the enablements of ICT. That same technology was said to have spyware and surveillance.

Further, on the level of awareness, many of the participants indicated they could detect when under surveillance or spyware monitoring. Most cited instances include repeated emails from the same source and sometimes requesting information about personal identification numbers. However, SSR 10, a security expert, submitted that there are levels of sophistication at which individuals or the uninformed may find it very difficult to detect spyware attacks, especially if they are from security agents.

Notwithstanding, a few other participants confessed to their limited understanding of how spyware and surveillance could be carried out and were unaware of how they prevent or avoid such attacks. For instance, SSR 8, an online publisher, said most people would hardly survive a spyware attack, especially from the government. This disclosure was further affirmed by security experts who said there are levels of sophistication in spyware that many may find difficult to detect. For instance, SSR 7 and 13, staff of major media outlets in Abuja and Freetown, Liberia, recounted their ordeals with their respective governments. They narrated similarly about their computer system crashing following infiltration by the security agents. Another participant, SSR 15, a freelance journalist in Nigeria with a knack for investigative stories, recounted how he lost his computer to a spyware attack and subsequently received threatening telephone calls over a storyline he was pursuing.

RO2: The Pervasiveness of Spyware Surveillance of Journalists

However, this study confirmed the acquisition of African governments' prevalent spyware and surveillance technology. Additionally, there is a high incidence of spyware attacks across media space in Africa. Specifically, the two security experts who are participants at the FGDs confirmed that African governments are actively acquiring spyware and surveillance technology. One of the West African countries, according to SSR 12, recently purchased a particular brand of spyware products. Notwithstanding, participants could hardly distinguish when being under spyware surveillance from their respective governments or unscrupulous individuals and fraudsters. We further observed a scenario whereby those who have been victims are more knowledgeable either through personal efforts and investment in training and capacity workshops by the media organisations.

Despite the claim of awareness of potential attacks by some participants, SSR 10 explained, based on his experience as a security expert, that some of the instances cited by participants cannot be attributed to the government or security agencies. He explained that many repeated emails requesting private information might likely be from unscrupulous individuals who use the technologies as scammers and fraudsters. In essence, the pervasiveness of spyware is attributed to these two sources.

RO3: How Justified Are Governments to Put Journalists Under Spyware and Surveillance

From Nigeria to Ghana, Liberia to Rwanda, and Kenya to South Africa, participants agreed there is one form of constitutional recognition for the freedom of expression and the media in their countries. Contrarily, many countries are also pushing to enact laws to control social media and Internet access. Participants opined that war, public unrest, and the fight against terrorism across West and Eastern African countries justify their governments' investment in and deployment of spyware and surveillance technologies. Contrarily, participants observed that African governments have not limited spyware surveillance to terrorism terrorists and other security threats. Instead, its deployment has been extended to journalists and political opposition. Specifically, SSR 13, a participant from Liberia, cited how, during his country's civil war, the government hid under national security to hound down journalists, invade media houses, and put journalists under surveillance physically and remotely through spyware. Relatedly, a democratically elected government in Nigeria justified the physical invasion and spyware attack of journalists' computers with the excuse that their publications were projecting Boko Haram, a terrorist group, as gaining the upper hand against the military.

Relatedly, SSR 13 and 10 believed the structure to profile and conduct surveillance of opposition had been created by authoritarian regimes, which some African countries had experienced. They concluded that some countries, even though they had transited to civil rule, inherited structure structures to perpetrate spyware surveillance around journalists. For instance, SSR 12, a prominent Abuja-based Nigerian newspaper staff member, said in 2000, "The military came in seven (7) trucks and collected all our laptops for scrutiny. They wanted to know the sources of our stories on Boko Haram. They hacked into our social media accounts. When our laptops were returned, we had to donate them to the orphanages and other charity organisations because they had all been infested with spyware."

Another participant, an international public servant based in Accra, SSR 5, submitted that a thin line separates national security and shared interests, and that security agencies and journalists must apply caution in discharging their responsibilities. He said, "There is

no clear boundary of what constitutes national security and public interest most of the time. Both journalists and security agencies have demonstrated a poor understanding of national security and public interests. Journalists, more importantly, need to know where to draw the line. However, African leaders are not transparent and are therefore always on the edge when journalists write stories that challenge their position or call them to accountability." His position agreed with SST 7, a public relations manager who argued that there are instances when the government has enough justification for preventing certain publications that threaten national security. He said there are occasions where people who claim to be journalists have gone beyond their bounds. Some people get confused about their professional duties for whatever reason. He retorted that if it is in all instances of allegations of espionage against journalists, the government is wrong.

Notwithstanding, journalists, while plying their practice with the justification of public interest, should know where the boundary lies and weigh options if their story constitutes a security threat. Another participant, SSR 4, specifically submitted, "There are occasions where journalists have gone beyond their bounds."

Participants commented on the factors that disposed journalists to spyware and surveillance, that the nature of their job grants them easy access to high-net-worth individuals in government. They need clearance before they are allowed to certain places that dispose of spyware monitoring. Nevertheless, more importantly, investigative journalists often put those in public offices on edge and would, therefore, want to monitor the next move before such stories are published. The fear of being exposed and the need for an upper edge are among other considerations to disposing government to deploy spyware and surveillance on journalists.

Discussion of Findings

One of the objectives of this study was to investigate the level of awareness about spyware and surveillance of journalists in Africa. Most participants demonstrated high levels of awareness, as 15 of the 22 participants demonstrated their understanding of the spyware surveillance by citing possible indications to include repeated emails from the same source and that on most occasions. They explain other symptoms, including a request to click on a link or supply certain vital information. Specifically, two participants who had been victims lately recounted their experience as their computers crashed after the incidents. These findings readily agree with the reviewed literature about this subject of study.

Notwithstanding, a security expert clarified the integrity of some indicators provided as evidence of spyware surveillance as insufficient to conclude that an attack could be from security agencies. While the study findings would agree with the submission by Mare (2019) and Lubbers (2015) on the massive deployment of spyware around journalists in Africa, much work needed to be done on the quality of experience displayed by journalists about spyware. Notwithstanding, we shall align with a report by Skelton (2021) that listed Nigeria, Egypt, Sudan, South Africa, and Kenya as the countries with high incidences of illegal spyware surveillance by security agencies. The report identified Botswana, with the highest incidence of spyware per citizen, as having legalised its infraction of careful monitoring of citizens' telephones.

Furthermore, most participants who had been victims of spyware surveillance entertain fear when in contact with any suspicious correspondence or possible source of spyware surveillance. This argument readily agrees with the theoretical postulation that people are bound to act in a certain way in reaction to a source of fear. Journalists and media

organisations that had been victims of surveillance were discovered to have invested more in training and other preventive measures to avoid the recurrence of possible spyware attacks. Those who have not been direct victims entertain the suspicion but are not as alert as those who have been victims. They also invested in education. However, spyware surveillance of journalists could instill fear and possibly reduce the quality of reportage or investigative journalism through self-censorship.

Further implications of this development are that the role of journalists in bringing those in political office to accountability would not be effectively performed. In the final analysis, society could be worse off as constant self-censorship by media professionals could, in a way, reduce the quality of public discussion and, by extension, the quality of the government's public-spirited policies. The findings of this study agree with the literature review on the extent to which communication technologies assisted with journalism practice on the one hand and the government's ability to monitor citizens and media communication, as argued by Dragu and Lupu (2021) on digital authoritarianism. A significant implication of this development is that the freedom of communication is being curtailed, and the quality of public discussion, which could be argued as an essential input to policy formulation in a democratic setting, is also being curtailed.

The second study objective pertains to the frequency of spyware surveillance around journalists in Africa. However, beyond confirming occurrence, this study could not validate a figure to describe the extent of pervasiveness of the occurrence of spyware surveillance of journalists. Whereas, in his research on the extent to which governments in Africa perpetuate surveillance of journalists in twelve (12) countries across North America, Europe and Africa, Mills (2019) was able to confirm that 64 per cent of investigative journalists and 71 per cent of foreign relations and security correspondents in the United States were conscious that the US government put them on surveillance. Notwithstanding, six (6) countries of Egypt, Kenya, Nigeria, Senegal, South Africa, and Sudan were identified as those with the highest incidence of surveillance of journalists, as confirmed by two separate studies by Skelton (2021).

However, neither the primary nor reviewed literature could pin down an exact figure on the extent of spyware surveillance in Africa. Admittedly, Skelton (2021) listed the six countries with the most acquisition of spyware technologies. This report is amid limited understanding among journalists, who are most likely to be affected. Therefore, African journalists need to increase their capacity on the workings of communications technologies and how to insulate themselves against possible attacks.

This study's third objective is to consider national security and public interests as a possible justification for the government's action on spyware surveillance around journalists. Most participants consented that national security could be enough justification for journalists, or anyone suspected of acting contrarily. A high number of participants believed that while the government could have national security as a reason for specific actions, there is a need for a proper definition of what constitutes national security. A further distinction should be made between national security and public interest, which should not be misconstrued as personal interest, as many of those in public offices often do. However, Ota and Ecoma (2022), in their definition of national interest, opined that making such a distinction could be an arduous task considering the influence of strong institutions like the Chinese Communist Party, authoritarian like General Sani Abacha in Nigeria from 1993 to 1998, who would not blink on a particular line of action, not even at the risk of Nigeria becoming a pariah nation or Idi Amin Dada of Uganda between 1971 and 1979 or

charisma leaders like Hiale Saleisse of Ethiopia between 1930 to 1974 who the people are ready to obey at all time.

Participants consented that there is a thin line separating national security and the public and personal interests of those in authority sometimes. Nonetheless, suspicion of an investigative story could be argued as a source of fear among the political office holders who could subsequently act in a way to either mitigate or eliminate the source of the anxiety using spyware surveillance. From the theoretical perspective, this explains the attitude of political officeholders in reaction to investigative journalists. The implications of politicians' attitudes could be a reduction in the quality and number of investigative journalists and their reportage, thereby reducing public space for discussion and accountability. The role of the media in bringing about accountability is, therefore, reduced or hampered. In contrast, the media indulges in self-censorship and subsequently slack in their constitutional duty as the fourth estate of the realm. However, study findings further confirmed that more prominent media organisations, especially those whose operations have been attacked, are spending more on enhancing the capacities of their staff to detect spyware surveillance and possible preventive measures. The twin implications of these developments are that while some other media organisations might be self-censored to protect themselves, the more daring and well-to-do ones invest in their capacities to detect when they are under spyware surveillance. These findings agree with the theoretical proposition that individuals will act in specific ways to eliminate or mitigate the possible consequences of toxic events.

CONCLUSION

Like most previous investigations, this study confirmed the high incidence of journalists being subjected to discreet analysis by their respective African governments. While the governments hide under national security to perpetuate surveillance, participants were mindful of the need for a more explicit definition of what constitutes national security instead of the public and personal interests. The increasing tendencies of deployment of spyware surveillance were further discovered as capable of shutting down the space for the public discourse and bringing public officeholders to accountability. It is a phenomenon capable of installing an authoritarian regime. There is also the need to define national security and personal interests.

RECOMMENDATIONS

1. Journalists and media houses should be interested in building their capacity to identify and be on alert for possible spyware and surveillance monitoring.

2. Media and communication training institutions should include trends in cyber security, spyware and surveillance technologies in their curriculum.

3. The government should implement more precise policy guidelines defining public interest and national security to prevent a lack of accountability in public offices and possible installations of autocratic rulers.

LIMITATIONS

A major limitation to this study is that choice of countries was limited to English speaking. Argument could be submitted that the choice of countries may not be representatives enough of the practices on the continent. It could be further argued that respondents may be reluctant is disclosing certain unwholesome practices about their governments and countries especially when there has been not enough familiarity between them and the interviewer ahead of the focus group discussions. Cautions, therefore, should be exercised with generalizing the outcomes of this study.

Notwithstanding these limitations, this study has contributed to the body of knowledge with the finding that journalists on the continent, even though are aware of the incidences of spyware surveillance, they can barely determine the extent of their exposure to it. It is therefore suggested that further studies be undertaken about this phenomenon in other countries where English is not their official languages to validate or otherwise the outcome of this investigation.

■ ■ ■

REFERENCES

Adeyeri, J. & Ogunniyi, J. (2016). Conflicts between national interest and human rights: Britain policy towards African immigrants, 1960 – 2013. *African Development*, 41(4).

Adike, A. (2013). Problems and prospects of investigative journalism in Rivers State, Nigeria: A study of the Tide and Hard Truth newspaper. *New Media and Mass Communication*, 17.

Anas, A. (2023). *African journalists are dying. They need the world's help to hold power to account.* The Guardian. https://www.theguardian.com/commentisfree/2023/apr/14

Basu, B. (2000). Russian national security thinking. *Strategic Analysis*, *24* (7) 12 – 85. https://doi.org/10.1080/09700160008455287

Beirut, A. (2014, July 16). *We are watching you. The Economist.* https://www.economist.com/pomegranate/2014/07/16/were-watching-you

*Botswana Criminal Procedure and Evidence Bill (2022).*https://cpj.org/wp-content/uploads

Chen, H., Liu, J., Wang, J., Xun, Y. (2022). Towards secure intra-vehicle communications in 5G advanced and beyond vulnerabilities, attacks, and countermeasures. *Vehicular Communications,* 39. https://doi.org/10.1016/j.vehcom.2022.10054

*Constitution of the Federal Republic o*f Nigeria, Act No. 24, May 5, 1999. https://www.refworld.org/docid/44e344fa4.html

Christina. P. (2022). Media coverage as a mirror or moulder? An inference-based framework. *Media and Communication.* 10 (3), 183–195.

Croteau, D. & Hoynes, W. (2006). *The business of media: Corporate media and public interest*. Pine Forge Press. https://books.google.com.ng/books

Davis, A. (2014). Media and politics. In Curran, J (Ed.) *Media and Society.* (pp. 83–102). Bloomsbury.

Dragu, T & Lupu, Y. (2021). Digital authoritarianism and the future of human rights. *International Organisation*. https://doi.org/10.1017/S0020818320000624

Iddins, A. (2019). The digital carceral: Media infrastructure, digital cultures, and state surveillance in post-Arab Spring Morocco. *International Journal of Cultural Studies*. https://doi.org/10.1177/ 1367877919842575

Di Salvo, P. (2022). We must act like our devices are already infected: Investigative journalists and Internet surveillance. *Journalism Practice*, 16 (9).

Earl, J., Maher, T., & Pan, J. (March 9, 2022). The digital repression of social movements, protest, and activism: A synthetic review. *Science Advances,* 8(10). https://doi.org/10.1126/sciadv.abl8198

Fawzi, N. (2018). Beyond policy agenda-setting: political actors' and journalists' perceptions of news media influence across all stages of the political process. *Information, Communication & Society*, 21(8), 1134–1150. doi:10.1080/1369118X.2017.1301524

Feldstein, S., (2021). The rise of digital repression: How technology is reshaping power, politics, and resistance. Oxford University Press.

United Nations Human Rights (1966). *International Covenant on Economic, Social, and Cultural Rights.* https://treaties.un.org/doc/treaties

Lauer, J. (2012). Surveillance history and the history of new media: An evidential paradigm. *New Media & Society*, 14(4), 566–582. https://doi.org/10.1177/1461444811420986

Lubbers, E. (2015). Undercover research: Corporate and police spying on activists. An introduction to activist intelligence as a new field of study. *Surveillance & Society,* 13(3/4), 338–353.

Mare, A. (2019). Communication surveillance in Namibia: An exploratory study. *Media Policy and Democracy Project*.

McCullagh, D. (2013). *RSF unveils 20/2020 list of press freedom's digital predators.* RSF unveils 20/2020 list of press freedom's digital predators | RSF

Mills, A. (2019). Now you see me – Now you do not: Journalists' experiences with surveillance. *Journalism Practice*, 13(6), 690–707.

Okocha, D., & Ola-Akuma, R. (2022). Journalistic metamorphosis: Robot journalism adoption in Nigeria in the digital age. *An African Journal of Arts and Humanities*, 8 (1).

Ota, E. & Ecoma, C. (2022). Power and national interest in international relations. *European Journal of Humanities and Social Sciences*. 2, 23-30. doi:10.24018/ejsocial.2022.2.4.268.

Richard, L. and Rigauds, S. (2021). Spyware can make your phone your enemy. Journalism is your defence. https://www.theguardian.com/world/commentisfree/2021

Rogers W. R. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1).

Skelton, C. (2021). *Illegal state surveillance in Africa is carried out with impunity*. Computer-Weekly. www.computerweekly.com.

Mare (2019). *Communication surveillance in Namibia: An exploratory study.* Media Policy and Democratic Project. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia

Merriam-Webster (Ed.). (2004). *Merriam-Webster's collegiate dictionary*. Merriam-Webster.

Nwilima, F. (2008). Practical reality of media freedom: An examination of the challenge facing Namibia. *Global Media Journal: African Edition*, 2(2). doi: 10.5789/2-2-24

United Nations Human Rights (1966). *The International Bill of Human Rights* .https://www.ohchr.org/sites

United States 2022 country reports on human rights: Nigeria. https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/nigeria

Vardalaski, K. (2021). A long-term discussion for ransomware as an intelligent threat. *Research Institute for European and American Studies*.

Woodhams, S. (2021). *Spyware: An unregulated and escalating threat to independent media*. Center for International Media Assistance.