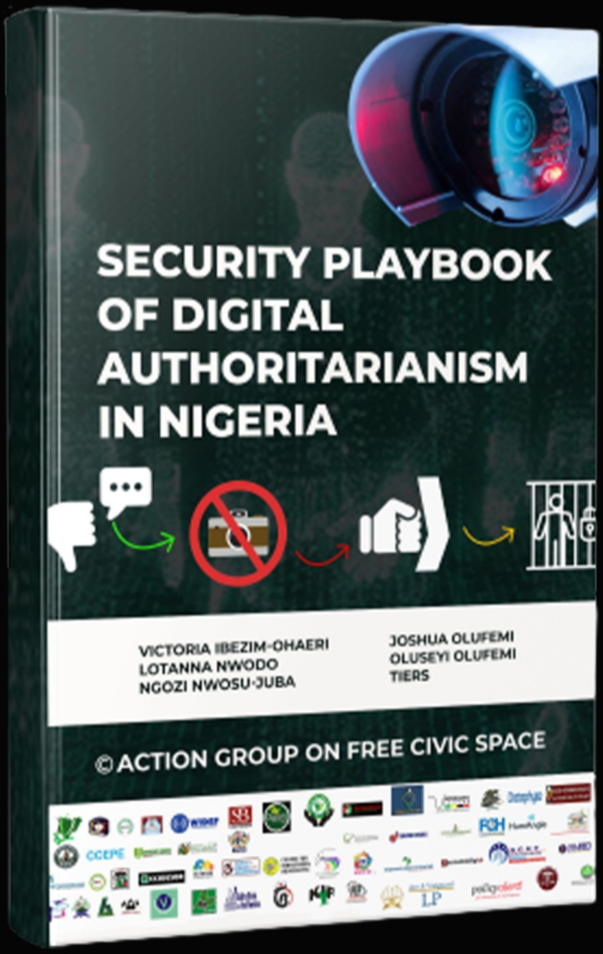
SECURITY PLAYBOOK OF DIGITAL AUTHORITARIANISM IN NIGERIA



SECURITY PLAYBOOK OF DIGITAL AUTHORITARIANISM IN NIGERIA

VICTORIA IBEZIM-OHAERI
LOTANNA NWODO
NGOZI NWOSU-JUBA

JOSHUA OLUFEMI
OLUSEYI OLUFEMI
TIERS

©ACTION GROUP ON FREE CIVIC SPACE

VICTORIA IBEZIM-OHAERI
LOTANNA NWODO
NGOZI NWOSU-JUBA

JOSHUA OLUFEMI
OLUSEYI OLUFEMI
TIERS

ACKNOWLEDGEMENT

The Security Playbook is a three-part research study collectively undertaken by eleven (11) members of the Action Group on Free Civic Space (AGFCS) to identify and analyze the use and misuse of the security agenda to shrink the civic space in Nigeria. The eleven organizations are Spaces for Change | S4C, Interactive Initiative for Social Impact (Dataphyte), The Initiative for Equal Rights (TIERS), Justice Rights Initiative (JRI), Centre for Citizens with Disabilities (CCD), Vision Spring Initiatives (VSI), World Impact Development Foundation (WIDEF), Rule of Law and Accountability Advocacy Centre (RULAAC), Youths and Environmental Advocacy Centre (YEAC), Building Blocks for Peace Foundation (BBforPeace), SB Morgen Intelligence (SB Intelligence). S4C, Dataphyte, TIERS and VSI co-authored the first part, **The Security Playbook of Digital Authoritarianism**, focusing on the use of technologies, regulations, and other computerized devices to jeopardize the right to privacy, censor free speech and stifle dissent in the online civic space in Nigeria.

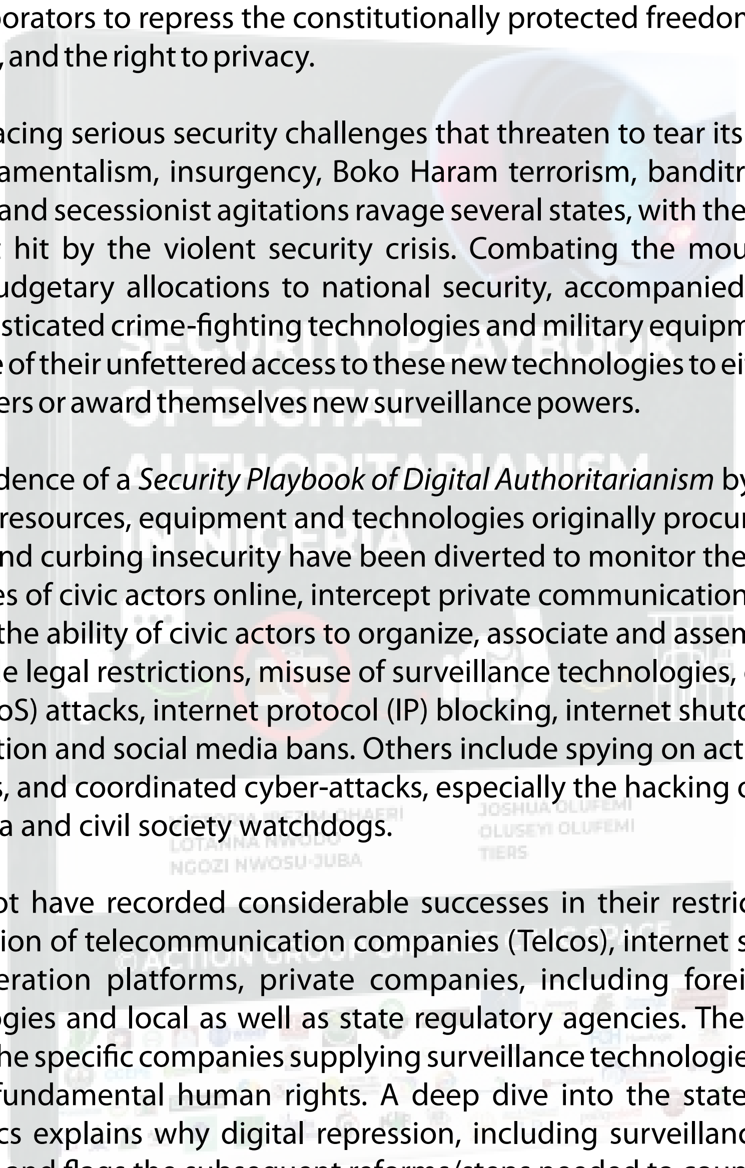
Many thanks to the following persons whose backend support and robust fieldwork greatly eased the implementation of this collective action research project: Joshua Olufemi, Oluseyi Olufemi, Ode Uduu and Charles Mba (Dataphyte researchers), Ngozi Nwosu-Juba, Tobi Ayodele, Anita Graham and Folake Kuti (VSI researchers and consultants), Ohotuowo Ogbeche, Olufunso Alufoge, Omolara Oriye, Olumide Makanjuola, Dr Michael Akanji, Akudo Oguaghamba, Juliet Nnedinma Ulanmo, Fisayo Owoyemi, Bala Mohammed Salisu, Olubiyi Oludipe, Amara the Lesbian, Ani Kayode Somtochukwu and Nwamaka Mbagwu (TIERs research team and enumerators); and Zikora Ibeh (S4C's Program Officer, Defending the Civic Space), David Olakunle and Rejoice Imozemeh (S4C's Finance Team) and Olusola Oluwafemi (S4C's Research and Communications Officer). S4C's Executive Director, Victoria Ibezim-Ohaeri, supervised and coordinated this project from start to finish including editing, proofreading and absorbing vital feedbacks on preliminary drafts to ensure a final appreciable work.

We deeply thank friends and allies at various international research and advocacy organizations—specifically Dr. Tony Roberts of Institute for Development Studies (IDS), Steven Feldstein & Sarah Gordon at the Carnegie Endowment for International Peace, Lydia Cocoon & James Savage of the Fund for Global Human Rights (FGHR)—who reviewed several drafts of this report and provided guidance for restructuring the order and flow of the overall argument.

The research team leveraged the diversity of connections and expertise within the Action Group on Free Civic Space to reach and capture the disparate experiences of civic actors actively using digital platforms to push for social change in the nearest to the farthest locations across the country. For giving us the wings to fly and laying a solid foundation for the **Action Group on Free Civic Space** to thrive, we generously thank FGHR for the generous support which made this collective action research project possible. We are super grateful to James Savage and Lydia Cocoom of FGHR for offering us invaluable guidance, assistance, support and feedback throughout this journey.

INTRODUCTION

This report presents the findings of a three-part study examining the overapplication or abuse of security infrastructure to crack down on civic actors in Nigeria. Undertaken by 11 member organizations of the Action Group on Free Civic Space (AGFCS), the research documents how security rhetoric and misuse of counterterrorism laws and tools are potentially becoming dominant driver of closing the civic space in Nigeria. In this first part, the report identifies and documents the new technologies, regulations, laws and tactics employed by state actors and their corporate collaborators to repress the constitutionally protected freedoms of expression, assembly, association, and the right to privacy.



Currently, Nigeria is facing serious security challenges that threaten to tear its sovereign fabric apart. Religious fundamentalism, insurgency, Boko Haram terrorism, banditry, farmer-herder conflicts, kidnapping and secessionist agitations ravage several states, with the northern region of the country worst hit by the violent security crisis. Combating the mounting insecurity necessitated huge budgetary allocations to national security, accompanied by the massive procurement of sophisticated crime-fighting technologies and military equipment. State actors have taken advantage of their unfettered access to these new technologies to either expand pre-existing policing powers or award themselves new surveillance powers.

This report builds evidence of a *Security Playbook of Digital Authoritarianism* by showing how the massive financial resources, equipment and technologies originally procured in the name of counterterrorism and curbing insecurity have been diverted to monitor the movement of citizens, track activities of civic actors online, intercept private communications, restrict online civic space, and limit the ability of civic actors to organize, associate and assemble freely. The popular tactics include legal restrictions, misuse of surveillance technologies, distributed denial-of-service (DDoS) attacks, internet protocol (IP) blocking, internet shutdowns, biometric data collection and social media bans. Others include spying on activists and opposition politicians, and coordinated cyber-attacks, especially the hacking of the servers and websites of media and civil society watchdogs.

State actors could not have recorded considerable successes in their restrictive adventures without the cooperation of telecommunication companies (Telcos), internet service providers (ISPs), content moderation platforms, private companies, including foreign suppliers of surveillance technologies and local as well as state regulatory agencies. The report provides detailed accounts of the specific companies supplying surveillance technologies to the Nigerian state for repressing fundamental human rights. A deep dive into the state's most popular techniques and tactics explains why digital repression, including surveillance abuses in the country is on the rise, and flags the subsequent reforms/steps needed to counter these trends. The report concludes by proffering recommendations to end misuse of digital technologies to stifle dissent, mitigate the effects of illegal surveillance practices, and increase the ability of citizens to freely access information and exercise their legal freedom of expression and right to privacy.

Summary of Key Findings:

A. A Rising Digital Economy and the Authoritarian Agenda

1. **Technological Boom of the 90s:** Nigeria began to witness significant turnarounds in its digital landscape following the deregulation of the telecommunications industry in the 90s, which dismantled state-run monopolies and opened the markets to new competitors and suppliers of digitized goods and services. As of December 2000, Nigeria had 450,000 connected fixed lines, no connected digital mobile line and 1 licensed mobile line operator. By 2021, the figure has increased to 298 million digital mobile lines out of which 187 million are active, 65 operating internet service providers, over 80 licensed fixed-line operators and over 14 licensed mobile line operators. The evolution of the internet, mobile telephony and the various hybrid telecommunications systems laid the foundation for real-time social connections and political influence on digital spaces to wax stronger.

2. **Activism moves from offline to online platforms:** Nigerians have an average of seven social media accounts per internet user and spend an average of 3 hours and 41 minutes per day on social media[1]. WhatsApp, Facebook and YouTube platforms are the most-used social media platforms by 93%, 86.2% and 81.6% respectively among users aged 16-64 in 2021. With more Nigerians with smartphones and gadgets now than ever, Nigerian civic actors evolved from rallying the populace using placards, pamphlets, posters, print and electronic media to using social media and other digital platforms to convene digital assemblies and expose government's excesses, speak truth to power, demand accountability from powerful state and corporate actors and ultimately mobilize citizens for behavioural, cultural and regime change. At these assemblies coordinated by means of digital communication technologies—such as mobile phones, cameras, or social media networking sites and hashtags—civic actors galvanize urgent actions, influence change and spread the word across continents at great speed and less cost.

3. **Digitalization Spurs Heavy Regulation:** The technological boom spurring the expansion of digitalized goods and services coupled with the increasing power of social media to trigger public censure prompted the formulation of a wide array of laws, policies and regulations to regulate both the industry and the activities that take place online as well as the recent attempts to censor and regulate social media platforms. Sitting atop the telecommunications industry is the Federal Ministry of Communications and Digital Economy (FMoCDE) and the industry regulator, the Nigerian Communications Commission (NCC) established pursuant to the Nigerian Communications Act 2003. other major regulators for the telecoms and communications industry include the National Information Technology Development Agency (NITDA), the National Broadcasting Commission, the National Identity Management Commission (NIMC), the Cybercrime Advisory Council and law enforcement agencies such as the Nigerian Police, Economic and Financial Crimes Commission, Nigeria.

4. **The Rise of Biometric and Other Intrusive Data Collection Initiatives:** In Nigeria, biometric data is collected for almost every registration process such as the national driver's license, national identity card, international passport, national voter's card, university examination registration, secondary school examinations, opening bank accounts, visa applications etc. Every Nigerian that is at least 18 years old, has to interface with a minimum of seven data collection agencies of the government to be able to exercise the basic rights to vote,

[1] Simon Kemp, DATAREPORTAL: Digital 2021: Nigeria, Published 11 February 2021, Accessed via Https://Datareportal.Com/Reports/Digital-2021-Nigeria

bank, drive, call or travel. Biometrics make it quite easy for every individual to be easily and accurately identified by their unique physical or behavioural traits. Official reasons for intensifying data collection include fraud/corruption prevention, countering terrorism and impersonation, crime detection, revenue mobilization, policy development, expanding e-government service delivery and so forth.

5. **Data Privacy Concerns Surge Amid Intrusive Data Collection:** The government's enhanced digital surveillance capacities have been made possible by the collection of big data in the form of biometric data collection, centralized databases, compulsory digital identification programs, data-warehouses, algorithm mapping and so forth. There is evidence that large volumes of personal data, including biometric information stored on multiple centralized databases have been frequently compromised, increasing citizens' exposure to privacy intrusions, targeted advertisements, identity fraud and blackmail. Citizens report that they receive a barrage of unsolicited messages, emails and phone calls from telecommunication companies (TELCOs), telemarketers of various products and political campaigners during elections, a sign that personal information stored in numerous databases littered across the country are being accessed, exploited for economic, commercial and political purposes.

6. **How Intrusive Data Collection Enhances Surveillance:** Personal data is the fuel for government's surveillance operations. Biometrics make it quite easy for every individual to be easily and accurately identified by their unique physical or behavioural traits. Human rights concerns have been raised where governments use biometric data for profiling and mass surveillance.[2] Corroborating the misuse of personal data for arbitrary surveillance, a new study finds evidence of extensive and invasive biometric data collection practices and use in Nigeria and a number of other countries.[3] Beyond the findings of independent studies, the clampdown on protesters in the wake of the October 2020 #EndSARS protests against police brutality, particularly the monitoring of their financial activities and locations, which culminated in the freezing of some protesters' bank accounts, cryptocurrency ban and the confiscation of some activists' passports, vividly illustrate how intrusive data collection makes surveillance and targeting of civic actors quite easy for governments. The protestors/holders of the frozen accounts are currently facing criminal charges on the grounds that they are suspected to be involved in "terrorism financing using their bank accounts."[4]

7. **The Role of Private Telecom Companies in Enhancing Surveillance and Data Privacy Breaches:** The government's surveillance operations are enabled by a horde of private actors comprising tech corporations, telecom operators, internet service providers, content moderation platforms and related initiatives. They assist governments to perpetrate privacy breaches using tracking apps, GPS devices, drones, facial recognition technologies, content moderation platforms, intercepting communications and outrightly releasing

Concerns over the rising state of insecurity and banditry prompted the December 16, 2020 directive to telecommunications companies and all Nigerian nationals to engage in a compulsory exercise linking all active SIM cards to registered National Identity Numbers (NINs) or face disconnection. Similarly, in 2015, the NCC directed all telecommunications firms to deactivate unregistered or partly registered SIMs. The regulation, according to government, is aimed at ensuring that all subscribers are traceable for security reasons. Official directives hinted that non-compliance would attract disconnection from the subscribed communication networks within two weeks from the day of the announcement.

[2] Financial Nigeria, Nigeria risks lower score on biometric data practices, February 2021; Accessed via http://www.financialnigeria.com/nigeria-risks-lower-score-on-biometric-data-practices-feature-403.html

[3] Comparitech, Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it, January 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/

[4] Human Rights Watch, ibid.

personal data. Regulatory obligations and profit-making stand out as the predominant motives for private sector participation in data breaches and surveillance initiatives. On the regulatory side, certain regulations and legislations impose obligations on private actors, especially tech corporations to render assistance to the government's surveillance agendas based on national security, disaster management, crime prevention and detection, public safety or other considerations. On the profit side, the online ad industry procures loads of personal data to achieve aggressive marketing objectives and the targeting of ads to specific groups of users. [5]

8. Methods Used by Private Companies to Assist Governments Censor Speech and Stifle Dissent: The various methods through which private actors facilitate the government's use of technology to silence dissent include regulatory action, network shutdowns, pulling down posts and disinformation, releasing subscribers' information and records to state authorities, retention and interception of communication details, release of subscriber records and information, lawful interception of communications, disclosure of registered identity information, and the disclosure of registered identity information for commercial, political and health purposes. A very sensitive provision to note is the legal requirement for licensees like telecommunication companies, network facilities providers and internet service providers to surrender "subscriber information on the Central Database" to security agencies upon a written request.

9. Legal Impetus for the State's Data-collection and Surveillance Operations: A host of national laws provide the legal impetus for the states' surveillance operations. The overt and covert operations of state security agencies to investigate and prevent crime, enforce rules, preserve the peace and counter terrorist activities are backed by numerous laws such as Section 45 of the 1999 Constitution, Official Secrets Act 1962: Sections 4-9 of the Nigerian Communication Act 2003:, Sections 146 -149 of the Cybercrime (Prohibition and Prevention) Act 2015, Section 29 of the Terrorism Prevention Act, S.119 & 120 of the Corporate and Allied Matter Act (CAMA) 2020:, Part V of the Mutual Assistance in Criminal Matters Act 2019, Lawful Interception of Communications Regulations: 2019/Section 10; Sections 19 & 20 Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 and many others, More often than not, state actors especially security agents exploit the gaps in these laws to expand pre-existing policing powers or award themselves new surveillance powers.

10. How State Agents Misuse Security Laws: While existing security laws and counterterrorism initiatives are necessary in a clime ravaged by organized crime, mounting evidence shows how extant security laws provide a legal foundation for the suppression of civil rights and freedom under the pretext of counterterrorism or protecting national security. Top on this list is Section 45 of the Constitution of the Federal Republic of Nigeria which legitimizes derogations to personal liberties in certain circumstances such as in the interest of defence, public safety, public order, public morality or public health. The second is the Terrorism Prevention Act, amended in 2013 ("TPA"), and the regulations made thereunder. The biggest flaw of the TPA is the failure to clearly delineate what amounts to terrorism. The definitional uncertainty has opened the doorway for the government to brand any dissenting group of

[5] Emma Woolacott, Forbes, Ad Industry Accused Of 'Massive' Privacy Breach, Accessed via https://www.forbes.com/sites/emmawoollacott/2019/01/28/ad-industry-accused-of-massive-privacy-breach/?sh=73c6bc076822

persons or movements as "terrorists" and then visit the consequences prescribed under the law upon such persons or movements. Persons accused of terrorist activities face immediate repercussions even before being found guilty of the offence such as arrest without bail, freezing of accounts and incalculable reputational damage. Other ways security and CT laws are misused include making new laws where none exist to justify their action;[6] abuse of government discretionary powers;[7] and the diversion of the country's legal security structures.[8]

11. Misuse of Security Laws to Close the Civic Space: The way security laws have been applied on a wide range of civic actors establishes the connections between the existing legal apparatus with the government's repressive intent. There are four major ways the Nigerian state applies security laws to repress the activities of the civil society. The most popular is by (a); recharacterizing organised dissent as terrorism (b); proscription of self-determination movements; (3) criminalizing free expression and (4) restrictions on open democracy. Nothing illustrates the misuse of security laws to stifle free speech more than the recurrent practice of framing social media commentary as terrorism. Hardly any week passes in Nigeria without a Facebook or Twitter user being arrested on account of their commentary critical of the government and charged for terrorism. Ali Yakubu,[9] Amudat Babatunde,[10] Joseph Odok,[11] Ambrose Nwaogwugwu[12] and Emperor Ogbonna[13] were charged with terrorism on account of Facebook posts that were critical of state executives. The swiftness with which bloggers, activists and commentators are arrested, prosecuted and jailed on account of critical commentary posted on social media strongly corroborates that a well-coordinated surveillance operation is effectively going on, monitoring the activities of citizens online. Particularly undergirding this inference is the huge disconnect between merely critical commentary on social media and the terrorism charges frequently slammed on their authors.

12. The Government is Thirsty for More Power: Despite the litany of existing enactments at the federal and state levels granting unfettered powers on state actors to surveil citizens and restrict their civic freedoms at the altar of national security, the Nigerian federal legislature is littered with assorted legislative proposals seeking to increase governmental powers to regulate the social media, control the digital spaces, undertake surveillance operations and intrude upon personal privacy. The numerous bills—National Information Technology Development Agency (NITDA) Act Amendment Bill, Protection from Internet Falsehoods, Manipulations and Other Related Matters Bill, 2019(Social Media Bill), National Commission for the Prohibition of Hate Speeches Bill 2019 (Hate Speech Bill), National Broadcasting Commission Amendment Bill—before the federal legislature containing amendment proposals for expanding state's regulatory powers underscore the popularity of weaponizing legislation to silence dissent. Where legislative measures are foiled by pushback by civil society, alternative routes can be explored to achieve the same objectives. One such alternative route is using fake news or disinformation as an excuse for imposing restrictive measures. The fake news narrative was used to ban social networking sites like Twitter.

[6] Over the years following FATF Recommendation 8, the government has sought to enact various restrictive legislation including several bills for the regulation of NPOs in Nigeria; the Bill Prohibiting Frivolous Petitions which would have required citizens to depose to affidavits in law courts before posting any statement on social media with respect to the government or its officials; regulations increasing the cost of data in another bid to restrict citizen activities online; etc.

[7] Twitter has been a preferred platform for civil engagement in Nigeria and was a major driver of the #EndSARS movement, #RevolutionNow, and so forth. However, following Twitter's censoring of a tweet by the Nigerian President for being inciting, Nigeria suspended Twitter in Nigeria on 4 June 2021. See Brookings "Nigeria's Twitter ban is a misplaced priority." Available at https://www.brookings.edu/blog/africa-in-focus/2021/08/11/nigerias-twitter-ban-is-a-misplaced-priority/, accessed 26 September 2021

[8] See the typologies in Section 2.2

[9] Closing Spaces Database, Businessman Jailed For Allegedly Calling Adamawa Governor 'Father Of All Thieves', Accessed via https://closingspaces.org/incident/businessman-jailed-for-allegedly-calling-adamawa-governor-father-of-all-thieves/

[10] Closing Spaces Database, DSS Files Terrorism Charges against Blogger who Streamed Igboho's House Raid on Facebook; https://closingspaces.org/incident/dss-files-terrorism-charges-against-blogger-who-streamed-igbohos-house-raid-on-facebook/

[11] Closing Spaces Database, Nigerian Lawyer Slammed with Terrorism Charges for Criticising State Governor, Please see: https://closingspaces.org/incident/nigerian-lawyer-slammed-with-terrorism-charges-for-criticising-state-governor/

[12] Closing Spaces Database, At Last, PDP New Media DG, Nwaogwugwu Granted Bail In High Court, , https://closingspaces.org/incident/at-last-pdp-new-media-dg-nwaogwugwu-granted-bail-in-high-court/

[13] TV360: 70 Days in Custody; The Case of Emperor Ogbonna, https://www.youtube.com/watch?v=-7AIhPYzCOY&feature=youtu.be

B. Digital Repression in the Name of Combating Insecurity and the War Against Terror in Nigeria

13. A Nation Besieged by Insecurity: The country's security landscape has radically transformed over the past five years, with the six geographical regions overwhelmed by varying degrees of internal security challenges. The northern region is the epicenter of violent crimes such as banditry, farmer-herder conflicts, illegal gold mining, insurgency and terrorism. In the North-West region, numerous armed groups working independently of[13] each other—collectively identified as "bandits" by the Nigerian government—have emerged. These groups are responsible for kidnappings along highways, mass abductions and indiscriminate attacks on communities. Historically entrenched injustices against the Igbo of south-east Nigeria are fuelling the separatist agitations in that zone. The secessionist campaigners, Indigenous Peoples of Biafra (IPOB), have been proscribed and designated a terrorist organization, with hundreds of members killed by security forces and their leader, Nnamdi Kanu, still in custody and facing terrorism charges. In the oil-rich south-south region, irresponsible oil exploration activities by multinational corporations, environmental degradation, underdevelopment, poverty, youth restiveness and unemployment lie at the root of the protracted violent conflicts in the area. The south-west's determination to take charge of their own economic independence and regional security to curtail the deadly invasion and land encroachments by herdsmen is igniting fresh demands for secession.

14. Nigeria's Counterterrorism Framework: The Terrorism Prevention Act (TPA), first passed in 2011, guides the implementation of the diverse counterterrorism initiatives in Nigeria. In addition to specifying punitive measures for various offences that fall within the purview of terrorism, the TPA aggregates provisions of preexisting security laws relating to the suppression of terrorist activities. The Office of the National Security Adviser (ONSA)[14]—solely appointed and answerable to the Presidency—oversees Nigeria's counterterrorism initiatives embodied in the National Counterterrorism Strategy (NACTEST) and coordinates the activities of all security and law enforcement formations. The ONSA's coordination role includes hosting the Counter-Terrorism Centre (CTC), Joint Terrorism Analysis Branch (JTAB) and the Behavioural Analysis and Strategic Communication Unit enabling it to facilitate intelligence sharing and cooperation amongst agencies.

15. Influx of Invasive Technologies in Nigeria to Counter Terrorism and Insecurity: Beginning from 2010, there has been a marked increase in the influx and use of sophisticated surveillance and hacking technologies for suspected nefarious ends. The array of surveillance technologies that have been imported into Nigeria, and currently used to monitor and surveil citizens include mobile call monitoring and communication interception technologies, drones, and geo-position interceptor and location of GSM, Wise Intelligence Network Harvest Analyzer System, Open-Source Internet Monitoring System and Personal Internet Surveillance System, Closed Circuit Television (CCTV) cameras, 6,000 streetlights and security sensors, Universal Forensic Extraction Device (UFED) and Forensic Toolkit (FTK), internet firewall and so forth.

[13] TheCable, Over 150 groups of bandits operate in the forests, says Masari, September 21, 2021, Accessed via https://www.thecable.ng/there-are-over-150-groups-of-bandits-in-the-forests-says-masari

[14] Known as Coordinator on National Security under the National Security Services Act

16. Motivations for the Massive Acquisition of Surveillance Technologies: Motivations for these acquisitions vary, but evidence shows these procurements are largely driven by partisan and political considerations on the one hand, and the fight against terrorism on the other. A third reason for these massive acquisitions is political corruption. National elections are primary drivers of surveillance operations. It is the time fierce and obscenely expensive electoral contestations between political heavyweights prompt candidates to know what their opponents are saying or planning to do. Along with using spying tools to track their prime challengers, targeted surveillance is often extended to family members of the opposition, including their wives, children, aides and loyalists in the run-up to elections. Old and new start-ups in surveillance systems around the world latch onto the opportunity to sell spying technologies to willing and ready customers determined to spy on and weaken the oppositions' political base.

The federal government also intensified its digitalized undercover activities through humongous budgetary provisions and acquisition of sophisticated surveillance hardware and software to repel Boko Haram-led terrorist activities in northeastern Nigeria. For instance, the 2013 budget included provisions for the purchase of a Wise Intelligence Network Harvest Analyzer System, Open-Source Internet Monitoring System and Personal Internet Surveillance System at a cost of N9.496 billion ($61.26 million)[16]. Between 2011 and 2021, government security agencies have budgeted at least N104.46 billion for tracing and monitoring communication systems. Analysis show that the Defence Space Administration planned to spend N31.23 billion on surveillance. This figure represents 29.9% of the total figure of N104.46 billion for the years under review. The Office of the National Security Adviser (ONSA) budgeted N18.62 billion while N15.89 billion was set aside for the Defence Intelligence Agency (DIA). Recently too, the Nigeria federal legislature approved the procurement of 4.87 billion naira worth of surveillance technologies “to intercept Thuraya mobile calls and solution” and WhatsApp's voice and text messages.[17]

17. Political Corruption is Another Driver of Arbitrary Surveillance Operations: Corruption is another major driver of the massive acquisitions of security-based technologies, hence the exponential rise and proliferation of surveillance capitalism in Nigeria. Beyond spying on opposition politicians to weaken their political capital, the importation of hacking expertise and tools has become a lucrative industry and conduit pipe for politicians[18] and their cronies to divert and siphon public funds offshore. Politicians and their cronies have used own private companies to secure shady cybersecurity contracts intended to shut down online media platforms perceived to be sympathetic to opposition politicians. Most of these contracts were ultimately used to secure the services of different security firms to monitor political opponents' communication and obstruct the online presence of newspapers considered unfriendly to the re-election campaign of the administration. Despite overwhelming evidence of monumental corruption, the veil of “security”, “intelligence” and “secrecy” surrounding the contract negotiations makes it easier for culprits to escape scrutiny and accountability. Because corrupt enrichment often lies at the core of these transactions, politicians secure these contracts through companies incorporated as special purpose vehicles (SPVs) or through legal partnerships with the supplying companies, holding out the SPVs as their local partners.

[16] Ogala Emmanuel, Premium Times, EXCLUSIVE: Jonathan awards $40million contract to Israeli company to monitor computer, Internet communication by Nigerians | Premium Times Nigeria (premiumtimesng.com)

[17] Ode Uduu and Charles Mba, Dataphyte, Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians, Accessed via Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians | Dataphyte

[18] Ogala Emmanuel, Premium Times, INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack 'unfriendly' websites, January 18, 2016; Accessed via https://www.premiumtimesng.com/investigationspecial-reports/196964-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websitesinvestigation-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websites-2.html

18. Major Suppliers of Invasive Spywares and Surveillance Technologies to Nigeria: The Israeli-owned company, Circles, is the highest supplier to Nigeria, with clients spanning states, federal and independent security agencies. Circles is a surveillance firm reputed for its abusive spyware technology system with a capacity to listen to phone conversations and also monitor the location of phones around the world.[19] Circles telephone tracking technology is primarily delivered through its start-up called V&V Limited. Surveillance companies like Cellebrite and FTK and the U.S.-based Access Data Group are also operating in Nigeria. Others include Elbit Systems, Romix Technologies, together with Packets Technologies AD, another Israeli company operating out of Bulgaria. On the demand side, there are customers or state agents who use the technologies to violate the privacy rights of citizens. State and federal governments, comprising mainly the federal security agencies, are the major patrons of surveillance technologies in Nigeria.

Numerous surveillance companies such as Isreali-owned Circles, Cellebrite and FTK and the U.S.-based Access Data Group are operating in Nigeria. The entrance of these companies into Nigeria's unregulated internet surveillance market widens the range of Nigerians susceptible to surveillance and privacy abuses.

19. The Role of China in Nigeria's Drift towards Digital Authoritarianism: In the wake of the Twitter ban, the Nigerian government, through the office of the Presidency, reached out to the Cyberspace Administration of China (CAC) to discuss plans to build an internet firewall similar to the internet filtering system China operates, called the Great Firewall. The internet firewall is expected to create a separate network for the Nigerian Internet, giving the government greater control over social media platforms such as[20] Twitter and Facebook. If this firewall is installed, the Nigerian government will be able to block virtual private networks (VPN), which many Nigerians are using to access Twitter while the ban is in force. This firewall initiative is not just evidence of the government's determination to control online speech, but also shows how cooperation and bilateral relations with countries like China known for their authoritarian strategies and with a track record of suppressing the civic space facilitates digital repression in Nigeria.

20. How State Agents Use Spywares and Hacking Technologies on Civic Actors: The entrance of spyware companies into Nigeria's unregulated internet surveillance[21] market widens the range of Nigerians susceptible to surveillance[22] and privacy abuses.[23] At least, three online newspapers—Premium Times, Gazette and Sahara Reporters—have accused the federal government of using hacking tools to shut down their websites at different times. A 2018 report used three case studies to illuminate how police authorities[24] use phone records to lure and arrest journalists on account of their journalistic undertakings. This tactic often involves the seizure of journalists' mobile phones and computers, and the use of forensic technology with capabilities to extract and decode every ounce of data stored within digital devices. Records further reveal

[19] Marczak, B. Scott-Railton, J. Rao, S. Anstis, S. Deibert, R. (2020, December 1). Running in circles: Uncovering the Clients of cyberespionage firm circles. The Citizen Lab. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[20] Foundation for Investigative Journalism, EXCLUSIVE: Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall (2021) Accessed via https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

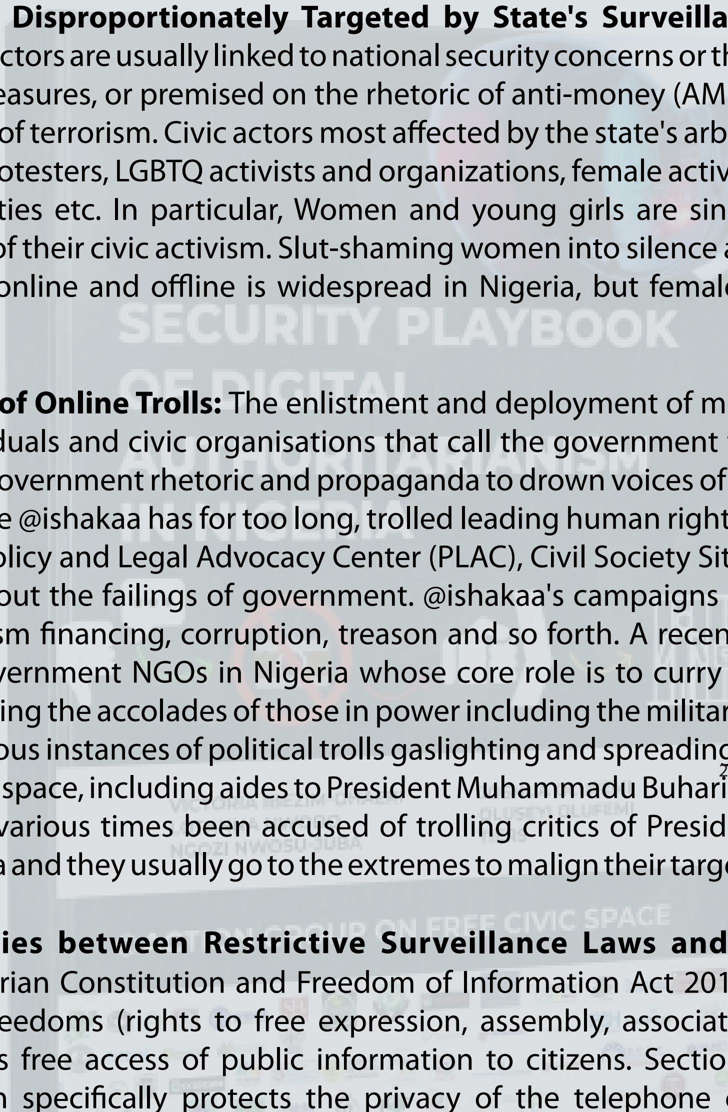
[21] Ogala, E. (2016, June 9). Ibid.

[22] Qurium, Nigeria Attempts to Silence the Investigative Media Peoples Gazette by Ordering Blocking, –Nigeria attempts to silence the investigative media Peoples Gazette by ordering blocking Qurium Media Foundation

[23] Victor Ekwealor, Sahara Reporters Targeted In A Website Hack Techpoint Africa, January 11, 2017:

[24] Jonathan Rozen, Committee to Protect Journalists, How Nigeria's police used telecom surveillance to lure and arrest journalists

how law enforcement agents easily obtain call records of individuals from network providers without a judicial warrant, consistent with the NCC Act of 2003. Telecommunication regulatory agencies can block access and regulate the internet through several technical protocols. The common methods include[25]: Domain Name Server (DNS) tampering, IP Blocking, transparent HTTP Proxy and outright ban of social media platforms.



21. Civic Actors Disproportionately Targeted by State's Surveillance Operations: Crackdowns on civic actors are usually linked to national security concerns or the enforcement of health emergency measures, or premised on the rhetoric of anti-money (AML) laundering and countering financing of terrorism. Civic actors most affected by the state's arbitrary surveillance include journalists, protesters, LGBTQ activists and organizations, female activists and bloggers, persons with disabilities etc. In particular, Women and young girls are singled out for slut-shaming on account of their civic activism. Slut-shaming women into silence and tagging them as 'prostitutes' both online and offline is widespread in Nigeria, but female activists remain undeterred.

22. Proliferation of Online Trolls: The enlistment and deployment of more vicious online trolls to attack individuals and civic organisations that call the government to account. These trolls, promote pro-government rhetoric and propaganda to drown voices of dissent. By way of illustration, the handle @ishakaa has for too long, trolled leading human rights organizations in Nigeria such as the Policy and Legal Advocacy Center (PLAC), Civil Society Situation Room and other groups calling out the failings of government. @ishakaa's campaigns on Twitter accuse civic actors of terrorism financing, corruption, treason and so forth. A recent study identified about 360 of pro-government NGOs in Nigeria whose core role is to curry the favour of the government by chanting the accolades of those in power including the military.[26] The local media is replete with numerous instances of political trolls gaslighting and spreading fake news within Nigeria's social media space, including aides to President Muhammadu Buhari.[27] The Buhari Media Centre (BMC) has at various times been accused of trolling critics of President Muhammadu Buhari on social media and they usually go to the extremes to malign their targets.[28]

23. Inconsistencies between Restrictive Surveillance Laws and Human Rights Provisions: The Nigerian Constitution and Freedom of Information Act 2011 provide for the protection of civic freedoms (rights to free expression, assembly, association and personal privacy) and legalises free access of public information to citizens. Section 37 of the 1999 Nigerian Constitution specifically protects the privacy of the telephone conversation and telegraphic communication of citizens without interference. These surveillance regimes are inconsistent with privacy guarantees while numerous legal provisions have been invoked to justify clampdowns by state actors such as the Official Secrets Act, Cybercrime Act, Terrorism Act, Criminal Code and Penal Code –especially those relating to treason, sedition etc.[29] Despite enacting the Nigerian Data Protection Regulation (NDPR) 2015, compliance lags. Incidents of violations have not attracted serious consequences for the unlawful intrusion and exploitation of personal data as espoused under section 2.10 of the NDPR.

[25] Terman, R. Internet Censorship (Part 2): The Technology of Information Control. Townsend Center for Humanities, University of California, Berkeley. https://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control

[26] Mathew T.Page, Fake Civil Society: The Rise of Pro-Government NGOs in Nigeria, Carnegie Endowment for International Peace, (2021) Accessed via https://carnegieendowment.org/2021/07/28/fake-civil-society-rise-of-pro-government-ngos-in-nigeria-pub-85041

[27] Queen Esther Iroanusi, ANALYSIS: How Nigerian politicians, supporters use fake news as campaign strategy https://www.premiumtimesng.com/news/headlines/311532-analysis-how-nigerian-politicians-supporters-use-fake-news-as-campaign-strategy.html

[28] https://www.premiumtimesng.com/opinion/466420-digital-authoritarianism-and-the-echoes-of-decree-4-by-bamidele-ademola-olateju.html

[29] Henry Ojelu, Vangaurd, Lawyers divided over superiority of FOI to Official Secret Act, September 6, 2018, https://www.vanguardngr.com/2018/09/lawyers-divided-over-superiority-of-foi-to-official-secret-act/

24. Transnational Drivers of Digital Repression in Nigeria: The Financial Action Task Force (FATF) and the regional body for West Africa, Intergovernmental Action Group Against Money Laundering (GIABA) strongly recommend surveillance by countries as part of their customer due diligence obligations and as tools for tracing and curbing the financing of terrorism. Nigeria's bank verification number (BVN), programme exemplifies the country's effort to comply with FATF's Recommendation 10, which makes BVN a compulsory requirement to open and operate bank accounts. UNSC resolutions empower states to conduct physical surveillance on persons. For example, Nigeria can justify its surveillance programme on the basis of Resolution2(c) of UNSC Resolution 1373 which mandates states to "take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information."The international CT narrative has also provided security agencies like the State Security Services (SSS) with undefined powers to proceed against citizens even where there is no perceivable act of terrorism or security threats. In absence of definitional certainty regarding what constitutes terrorism, states are enabled to flexibly determine what falls within the purview of countering or preventing terrorism and violent extremism. As evidence in numerous chapters demonstrate, this permission is often overstretched to include virtually anything so designated as terrorism by state agents.

25. Roadmap for Change: The opportunities to disrupt, to reform and, over long-term, transform the misuse of technology to suppress dissent hinge on a holistic five-pronged approach involving different stakeholders and calibrated to strike a balance between the competing agendas of the government, the private sector, civil society, and the media. With national security and foreign policy considerations in mind, Nigeria can use import controls as a strategy to limit the influx of sophisticated spyware technologies into the country. Nigeria can borrow best practices from the United States of America's Commerce Department which issued a new set of rules titled, information security control,[30] imposing export controls on items used in surveillance of private citizens and other malicious cyber activities. The rules aim to check the misuse of technology to abuse human rights or conduct other malicious cyber-attacks, and ensure that U.S. companies are not fueling authoritarian practices.[31] Businesses cannot effectively respect human rights and the rights of persons that may be disproportionately impacted by their operations unless they have certain data privacy policies and processes in place. Since the Twitter ban, Nigerians have massively and proactively downloaded anti-censorship software like VPNs in order to survive internet shutdowns and effectively evade censorship. These sorts of measures may be the most effective steps that Nigerians can take until more holistic legislative and normative changes occur.

[39] Federal Register, Information Security Controls: Cybersecurity Items, https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items

[31] US Department of Commerce: Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities; Accessed via https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private

ACTION GROUP ON FREE CIVIC SPACE

ACTION GROUP ON FREE CIVIC SPACE SECRETARIAT:

SPACES FOR CHANGE | S4C
35B AJAKAIYE STREET, ONIPETESI ESTATE, MANGORO, IKEJA, LAGOS, NIGERIA
Email: info@closingspaces.org
Telephone: +234 703 620 2074 | +234 909 453 9638
Website: https://closingspaces.org/group-activities/