



SPACES FOR CHANGE | S4C

RESEARCH | POLICY | CITIZEN ACTION



Supported by:



**Spyware
Accountability
Initiative**



**Ford
Foundation**

OCTOBER 2024

The

PROLIFERATION OF DUAL-USE SURVEILLANCE TECHNOLOGIES IN NIGERIA:

**Deployment, Risks
and Accountability**

Compiled and written by:

VICTORIA IBEZIM-OHAERI

Contributors:

VICTORIA IBEZIM-OHAERI

TESTIMONY OMOLE

LAWRENCE OBOH

LOTANNA NWODO

EMMANUEL AKANDE

Graphic Design:

BRADE NETWORKS LTD.

ACKNOWLEDGEMENTS

A previous study, [Security Playbook of Digital Authoritarianism in Nigeria](#), examined the types of surveillance technologies imported into Nigeria, mapping the supply chains, and the implications for human rights and the civic space in Nigeria. The report provided ample evidence of misuse and repurposing of spyware imported for combating criminal threats to other purposes unrelated to security such as the arbitrary monitoring and surveilling citizens and activists, tracking the activities of civic actors online, intercepting private communications, censoring online free speech and restricting the ability of citizens to speak, assemble and associate freely.

Another important finding is that the proliferation of surveillance technologies—and the associated human rights abuses—have soared because of their dual-use nature and capacity to be used both for military and civilian uses, either for malevolent or benevolent objectives. More so, the deployment of dual-use technologies without proper checks and balances increases the potential for abuse, diversion and repurposing for harmful objectives. Who is responsible for the proliferation and harmful deployment of surveillance technologies? The manufacturers/exporting countries, the importing countries or both? This new report now sets out to explore the accountability pathways for spyware abuse both internally and externally.

We are grateful to all members of Spaces for Change's | S4C's research team—comprising Testimony Omole, Lawrence Oboh, Emmanuel Akande, Rejoice Imozemeh, Victoria Ibezim-Ohaeri and external research support by Lotanna Nwodo—for their primary research, data collection, analysis, structuring and formatting, at various stages of this project. S4C's research team received extensive inputs and proof-reading support from numerous friends and allies of the organization, especially James Savage, Program Director, Enabling Environment for Human Rights Defenders of the Fund for Global Human Rights (FGHR) and Danna Ingleton, Huridocs' Executive Director. Our special thanks also go to Victoria Ibezim-Ohaeri, S4C's Executive Director, for coordinating this research from start to finish, and synthesizing all the data collected from various sources.

S4C conducted this research under its Spy-Stop Campaign Project supported by the Spyware Accountability Initiative (SAI) managed by the Ford Foundation. We are very thankful to Michael Brennan and Ford Foundation's Technology and Society team for providing the necessary resources and access to the networks that made this research possible. We extend our deepest appreciation to fellow SAI grantees from Citizens Lab—Ron Deibert, John Scott Railton and Siena Anstis—who assisted generously with technical reviews of the initial drafts and provided guidance for enriching the report.

FOREWORD

Surveillance technology refers to “products or services that can be used to detect, monitor, intercept, collect, exploit, preserve, process, analyze, invasively observe, and/or retain sensitive data, personally identifying information, including biomarkers, or communications concerning individuals or groups.”¹ Across the world, the modes of surveillance have radically changed since the last century. The olden methods of surveillance ranged from physically monitoring a person's movement, bugging their homes, wire-tapping their telephones and other personal spaces, or intercepting their mail packages. With the help of new surveillance technologies, it is now possible, and even easier, to achieve these objectives without the need for physical contact.

Nowadays, surveillance technologies “probe more deeply, widely and softly than traditional methods, transcending natural (distance, darkness, skin, time and constructed (walls, sealed envelopes) barriers that historically protected personal information.”² A zero-click spyware like the Israeli's NSO Group-made Pegasus—can now be deployed to a person's phone remotely to extract everything from a target's mobile phone, including messages, contacts, photos and videos without the user having to click on a phishing link to give it remote access. It can also turn the mobile phone into a tracking and recording device.³

Most surveillance technologies are by nature either dual-use technologies or solely military equipment. Surveillance equipment solely used for military purposes pose fewer challenges since only the military can procure and use them exclusively for the purposes of defending the country against foreign adversaries. It becomes more complicated when new technologies with extreme surveillance abilities are rolled out daily and integrated into technological products and services used by civilian populations. As some authors rightly noted: “as surveillance technology is propagated and normalized, it has crept into ordinary commercial markets, putting tools or techniques designed for use

1. [Guiding Principles on Government Use of Surveillance Technologies \(state.gov\)](#)

2. [whatsnew.doc \(cmu.edu\)](#) page 2.

3. [Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker - The New York Times \(nytimes.com\)](#)

by intelligence and law enforcement into the hands of ordinary criminal actors and abusive spouses alike.⁴

There is no doubt that surveillance is necessary in certain circumstances. Developing countries like Nigeria facing daunting security challenges depend on foreign countries—such as the United States, United Kingdom, Russia, China, and Israel—to supply them technologies that can bolster the government's crime detection, internal security and self-defense operations. This dependency has opened the doors to the importation of various kinds of technologies into the country, including harmful technologies with sophisticated surveillance capabilities. Our previous report, [Security Playbook of Digital Authoritarianism in Nigeria](#), extensively examined the nature and patterns of use and abuse of surveillance technologies in Nigeria, resulting in civic space closures, human rights violations, including physical harm to civic actors such as activists, journalists, protesters, media houses and political opponents.

Building on the former report, this research focuses on accountability for the misuse of surveillance technologies in Nigeria. It finds that the proliferation of surveillance technologies has surged because of the increasing democratization of access to technologies across the globe, the dual-use nature of new technologies for constructive and destructive purposes, and the weak importation controls. While it is important to hold the Nigerian government accountable for the import regulatory deficiencies and the human rights abuses arising from the misuse of surveillance technologies, it argues that both the importers and exporters of these technologies are both duty-bearers, and therefore, share the obligation to ensure that procurement and use of spyware are strictly confined to national security purposes. That obligation requires putting the necessary controls and accountability measures in place to prevent misuse and diversion, ensuring that the national security exception does not provide a backdoor or license to erode human rights.

That is why this report looks externally to see what opportunities (or limitations) exist for demanding accountability and reform. If import controls are inadequate, can civil society watchdogs rely on the export controls of supplier-countries to demand accountability when surveillance technologies are used to violate human rights? Although export controls have comparatively more elaborate features than import controls, there are several factors diminishing their effectiveness in preventing the proliferation of surveillance technologies and in

4. [Advancing Human-Rights-By-Design In The Dual-Use Technology Industry | Columbia | Journal of International Affairs](#)

protecting citizens from harmful attacks. This report shed lights on these limitations and the extent developing countries can rely on the regulatory grace of exporting countries.

Against this backdrop, this study examines the nature and characteristics of dual-use surveillance technologies imported and used in Nigeria, shedding light on the legal and institutional frameworks for their importation, the licensing conditions as well as the domestic and international controls governing their importation and use. Finally, the report will discuss the enforcement mechanisms at the national and international levels in place to ensure compliance with these controls. The study proceeds upon the premise that understanding the gaps in the importation and regulation of dual-use surveillance technologies is crucial for safeguarding national security, protecting human rights, and fostering responsible technological advancement.



VICTORIA IBEZIM-OHAERI

Victoria Ibezim-Ohaeri

Executive Director
SPACES FOR CHANGE | S4C

METHODOLOGY

The Proliferation of Dual-Use Surveillance Technologies in Nigeria: Deployment, Risks, and Accountability is follow-up research to a previous study, **Security Playbook of Digital Authoritarianism in Nigeria** which examined how surveillance technologies, regulations, and other digitalized tools violate privacy rights, censor online expression, and constrict the online civic space in Nigeria. The focus of this follow-up report is accountability for the misuse of surveillance technologies in Nigeria. It proceeds upon the premise that the proliferation of surveillance technologies has surged because of the increasing democratization of access to new technologies across the globe and their dual-use nature for constructive and destructive purposes. Proliferation is aggravated by weak regulations and importation controls in developing countries like Nigeria. If regulation and import controls are inadequate, to what extent can civil society watchdogs then rely on the export controls of supplier-countries to demand accountability when surveillance technologies are used to violate human rights and shrink the civic space?

Researchers comprising internal and external staff of Spaces for Change conducted this research using primary and secondary data gathered from various sources, including incident-tracking on the Closing Spaces Database, literature reviews, desk studies, official reports of reputable local and international institutions, public dialogues, didactic convenings and technical reviews. The **Security Playbook of Digital Authoritarianism in Nigeria** was presented at a consultative dialogue on July 7, 2023—which assembled representatives from telecommunication and fintech companies, National Human Rights Commission, internet service providers, digital rights lawyers, journalists, cyber security experts, civil society organizations and federal agencies responsible for regulating telecommunication companies, digital identity authentication and the country's digital economy—to deliberate on the challenges and opportunities for private companies to safeguard the civic space and digital rights of citizens while accomplishing their business and economic objectives. The dialogue offered an opportunity to receive official clarifications regarding the regulation of surveillance and other dual-use digital technologies

in Nigeria as well as the perspectives of private (tech) companies on the performance and impact of applicable digital laws and policies.

S4C also leveraged secondary sources such as official reports, peer-reviewed journal articles, local and international media outlets, and its Digital Security Clinics held under Civic Space Resource Hub for West Africa project (CSR-Hub project) to gather additional information and document the experiences of activists, journalists and civil society organizations regarding the deployment and impact of surveillance technologies on civic actions. The experiences shared and documented during these Clinics were complemented by data extracted from the Closing Spaces Database —www.closingspaces.org— hosted by Spaces for Change. The Database is an online secure reporting and monitoring tool that systematically tracks and documents crackdowns on the civic space, including digital rights closures.

The preliminary draft report received peer-reviewed inputs and feedback from three independent expert institutions encompassing an interdisciplinary research laboratory, a philanthropic foundation and a conglomerate of advocates, researchers, and technologists committed to addressing the threat of surveillance and promoting accountability in the design and use of digital technologies.

TABLE OF

CONTENTS

- ◆ Acknowledgments
- ◆ Foreword
- ◆ Methodology
- ◆ Table of Contents
- ◆ Table of Acronyms

1	UNDERSTANDING THE DRIVERS AND JUSTIFICATION FOR SURVEILLANCE IN NIGERIA	13
1.1	Surveillance is a Relic of Colonial Rule.....	15
1.2	Surveillance is Legally-Permissible Under Numerous Statutes.....	16
1.3	National Security is a Major Driver of Surveillance.....	19
1.4	Surveillance is a Vestige of Military Rule.....	22
1.5	Spyware Trade is Highly Profitable.....	22
1.6	Nigeria's Population Has Increased Exponentially.....	24
1.7	The Global Drift Toward Authoritarianism is on the Rise.....	24
1.8	Secrecy Boosts Surveillance and Civic Repression.....	26
2	DUAL-USE NATURE OF SURVEILLANCE TECHNOLOGIES	29
2.1	Mapping Dual-Use Surveillance Technologies used in Nigeria.....	30
2.2	Arbitrary Deployment of Dual-Use Surveillance Technologies in Nigeria.....	32
3	REGULATING THE IMPORTATION OF DUAL-USE TECHNOLOGIES IN NIGERIA	37
3.1	Regulating the Importation of DUTs, in Nigeria.....	38
3.2	Are Items Not Included in ONSA List Deemed to be Excluded?.....	49
3.3	Typologies of Exploitation of Excluded Dual Use Technologies.....	50

TABLE OF

CONTENTS

3.4	Other Ways Dual-use Technologies Can Be Abused....	53
3.5	Opportunities for Increasing Regulatory Oversight on the Importation of Dual-Use Technologies in Nigeria.....	55
4	EXPORT CONTROL REGIMES FOR DUAL-USE TECHNOLOGIES	59
4.1	DUT Production Trends in Major Supply Countries.....	61
4.2	Export Control Regimes for Dual-Use Technologies in Nigeria's Major Supplier Countries.....	64
4.2.1	Israel's Export Control Regime.....	64
4.2.2	Export Control Regime in the People's Republic of China.....	67
4.2.3	Export Control Regimes in the United States of America (USA).....	73
4.3	International Export Control Arrangements for Dual-Use Technologies.....	74
5	THE LIMITATIONS OF EXPORT CONTROL REGIMES AND THE IMPLICATIONS FOR IMPORTING COUNTRIES	81
5.1	Human Rights Considerations Lack Clarity and Consistency.....	82
5.2	National Interest and National Security Considerations.....	83
5.3	Dependency on Foreign Technology and Expertise.....	85
5.4	Economic Sabotage, Corruption and Illicit Transfer Flows.....	86
5.5	Espionage Concerns.....	87
5.6	Data Privacy Breaches.....	88
5.7	Dual-use Surveillance Technologies, and the Civic Space in Nigeria.....	89
6	OPPORTUNITIES FOR LEGAL REFORM AND CIVIC ACTION	96
	BIBLIOGRAPHY	110

TABLE OF ACRONYMS

ACHPR:	African Charter of Human and Peoples' Rights
AG:	Australia Group
AGFCS:	Action Group on Free Civic Space
AU:	African Union
BIS:	Bureau of Industry and Security
BWC:	Biological Weapons Convention
CBW:	Chemical Biological Weapons
CBN:	Central Bank of Nigeria
CCCL:	Commerce Control List
CCTV:	Closed-Circuit Television
CEO:	Chief Executive Officer
COE:	Contingent-Owned Equipment
COINTELPRO:	Counter Intelligence Program
CIPESA:	Collaboration on International ICT Policy for East and Southern
CRISPR:	Clustered Regularly Interspaced Short Palindromic Repeats
DDoS:	Distributed Denial of Service
DECA:	Defense Export Controls Agency
DECL:	Defense Export Control Law
DSS:	Department of State Services
DUTs:	Devices Under Test
ECL:	Export Control Law
EUC:	End User Certificate
FBI:	Federal Bureau of Investigation
FMITI:	Federal Ministry of Industry, Trade and Investment
FTK:	Forensic Tool Kit
GSM:	Global System for Mobile Communications
ICT:	Information and Communication Technology
IMSI:	International Mobile Subscriber Identity
IPOB:	Indigenous People of Biafra
ISWAP:	Islamic State West Africa Province
ISIS:	Islamic State of Iraq and Syria
LICR:	Lawful Interception of Private Communications
LGBTQ+:	Lesbian, Gay, Bisexual, Transgender, and Queer

MDAs:	Ministries, Departments, and Agencies
MNJTF:	Multinational Joint Task Force
MSMEs:	Micro, Small, and Medium Enterprises
MOFCOM:	Ministry of Commerce of the People's Republic of China
MOE:	Ministry of Economics and Industry
MTN:	Mobile Telecommunications Network
MTCR:	Missile Technology Control Regime
NCAA:	Nigeria Civil Aviation Authority
NCC:	Nigeria Communication Commission
NCS:	Nigeria Customs Service
NDPC:	Nigeria Data Protection Commission
NIMC:	National Identity Management Commission
NITDA:	National Information Technology Development Agency
NRCC:	Nuclear Regulatory Commission Controls
NSG:	Nuclear Suppliers Group
NSO:	National Security Organization
NOTAP:	National Office for Technology Acquisition and Promotion
ONSA:	Office of National Security Adviser
OSINT:	Open Source Intelligence
PSS:	PC Surveillance Systems
RCS:	Remote Control System
RMB:	Renminbi
SARS:	Special Anti-Robbery Squad
S4C:	Spaces for Change
SSS:	State Security Service
UAVs:	Unmanned Aerial Vehicles
UDHR:	Universal Declaration of Human Rights
UN:	United Nations
UNSC:	United Nations Security Council
USA:	United States of America
USML:	United States Munitions List
VSS:	Visual Sub System
VPN:	Virtual Private Network
WA:	Wassenaar Arrangement
WMD:	Weapons of Mass Destruction
WIT:	Wise Intelligence Technology

CHAPTER

1



UNDERSTANDING THE DRIVERS AND JUSTIFICATION FOR SURVEILLANCE IN NIGERIA

Although surveillance is an age-old practice, its nature, motivations and sophistication assumed unprecedented proportions after the September 11 bombing incidents targeting the twin towers of the World Trade Center in New York, United States. That event sparked major shake-ups and reactions within the security architecture of the United States, and across the rest of the world. Just 45 days after the 9/11 attack, the Patriot Act was passed, significantly expanding the search and surveillance powers of federal law enforcement and intelligence agencies.⁵ The responses, both legal and extra-legal in nature and scope, triggered an inordinate gathering of intelligence, including allowing intrusions into personal privacy and derogation of certain individual rights in the name of national security. This 'securitisation' of the 9/11 response then created the foundations for the massive expansion of anti-terrorism frameworks and tools over the following 20 years.

It was in 2013 that the world realized the extent of surveillance being conducted by governments in the name of security, when a 29-year-old Edward Snowden blew the whistle on the existence of secret wide-ranging information-gathering programs conducted by the American National Security Agency.⁶ Despite Edward Snowden's staggering revelations showing how the US government spied on foreign governments, corporations, and individuals – including its citizens – at a mammoth scale,⁷ countries around the world, including Nigeria, have copied the American approach to develop sophisticated surveillance initiatives to preemptively detect and eliminate threats, combat terrorism and contain aggressors. Nigeria grapples with diverse security challenges such as terrorism and violent extremism, banditry, farmer-herder conflicts, secessionist agitations, kidnapping, and road robbery. Tackling these security challenges led the government to procure massive amounts of technological equipment over the years to increase national capacities in intelligence operations, information gathering, monitoring and tracking of criminal elements, hotspots mapping, etc.

When governments' appetite for surveillance is combined with the readiness of the corporate world to supply technology (camera, wireless technology, DNA, thermal sensors, chips, software, programs)⁸ to both the government and private persons, a "surveillance society"⁹ is born. Along this line, Nigeria's

5. [USA PATRIOT Act | Facts, History, Acronym, & Controversy | Britannica](#)

6. Britannica: "Edward Snowden", <https://www.britannica.com/biography/Edward-Snowden>, retrieved 8 July 2024

7. Britannica: "Edward Snowden", <https://www.britannica.com/biography/Edward-Snowden>, retrieved 8 July 2024

8. [whatsnew.doc \(cmu.edu\)](#) page 2

9. [The Surveillance Society | TIME.com](#)



When governments' appetite for surveillance is combined with the readiness of the corporate world to supply technology (camera, wireless technology, DNA, thermal sensors, chips, software, programs) to both the government and private persons, a “surveillance society” is born.

historical trajectory reveal certain trends, patterns and characteristics from which the main drivers and justification for expanding state surveillance could be inferred. We explore them in detail below.

1.1 SURVEILLANCE IS A RELIC OF COLONIAL RULE:

On November 24, 1929, scintillating demonstrations by over ten thousand Igbo women in the then eastern Nigeria swept through the Owerri-Calabar districts against the over-taxation of households by British colonialists. For months, the protests raged against the colonialists and the power-drunk warrant chiefs they imposed on local people to enforce exploitive taxation laws. The warrant chiefs went about seizing properties, forcefully marrying brides without paying dowry, invading and surveilling private homes to count the population and livestock for taxation purposes. Surveillance by warrant chiefs took the form of spontaneous intrusions into private homes to count their livestock, crop yields, family members. Over a two-month period of insurrection—December 1929 to January 1930—at least 50 people were killed, but the warrant chief system ended.¹⁰

10. The Open University, Resource 4: The Aba women's riot, <https://www.open.edu/openlearncreate/mod/oucontent/view.php?id=160512§ion=2.7#:~:text=In%201928%E2%80%931930%2C%20Aba%20women,they%20were%20to%20be%20taxed.>

The transfer of the warrant chiefs' surveillance powers to colonial penal systems and institutions such as the police, with a centralized command structure, suited the colonialists' objectives of asserting total control of populace and stifling dissent to colonial rule.¹¹ The colonial police went about at that time subjugating local populations, suppressing resistance to imperial conquests and exploitation.¹² Today, relics of the brutish policing and surveillance operations of the colonial era remain, but now fragmented across a broad spectrum of state institutions. For instance, the State Security Service (SSS) or Department of State Services (DSS)—established in 1948 the then “E” Department (Special Branch) domiciled in the Office of the Inspector General of the Nigeria Police Force —had its roots in pre-colonial Nigeria.¹³

As can be gleaned from the Aba Women's protests of 1929, the pre-independence movements and the pro-democracy struggles in Nigeria, state repression has always triggered mass resistance. The anticipation of resistance impelled authorities to explore and invent creative strategies for controlling the masses and suppressing opposition. Rolling out enactments dotted with restrictive clauses that provide justifications for executive overreach and curtailment of civic freedoms gained notoriety. These restrictive enactments, characteristically containing ouster clauses that usurped the powers of the judiciary to review executive decisions and actions framed around the objective of national interest or national security.

1.2 SURVEILLANCE IS LEGALLY-PERMISSIBLE UNDER NUMEROUS STATUTES:

Numerous national laws authorize law enforcement agencies to surveil citizens for various reasons. For instance, Section 45 of the Constitution of Nigeria permits the derogation of certain human rights, including the right to privacy, for specific purposes – (a) in the interest of defence, public safety, public order, public morality or public health, or (b) for the purpose of protecting the rights and freedom of other persons. Likewise, sections 146 – 149 of the Nigerian Communications Act 2003 require "telecom operators to cooperate with state authorities to frustrate the commission of crimes, to protect public revenue and preserve national security, including allowing authorized interception of communications".

11. Cheta Nwanze, A History of Nigeria's Police Service, published in Africa is a Country; Accessed via <https://Africasacountry.Com/2014/04/Historyclass-Nigerias-Police>

12. Victoria Ibezim-Ohaeri, #ENDSARS: Police Brutality, Protests and Shrinking Civic Space in Nigeria, (2020) <https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/>

13. See website of the Department of State Services, https://www.dss.gov.ng/dss_about

Section 13(2) of the recently-revised Terrorism (Prevention and Prohibition) Act, 2022, makes it illegal to support terrorist organizations by disseminating their propaganda online, through other electronic or digital channels, or by using printed materials. Section 13(2) implicitly grants security agencies the right to indiscriminately surveil citizens and keep tabs on their online activities, including their commentary on social media. To make matters worse, state actors are increasingly weaponizing anti-terrorism and security laws to dilute human rights protections, curtail civil liberties and securitize the spaces for civic engagement.¹⁴

The interception of private communications is governed by the Lawful Interception of Communication Regulation (LICR) 2019 which spells out the circumstances law enforcement agents can lawfully intercept private communications. Nigeria's Lawful Interception of Communications Regulations (LICR) 2019 makes it lawful for any authorized agency— (a) the Office of the National Security Adviser or his designee; (b) the State Security Services represented by the Director or his designee, who shall not be below the equivalent of an Assistant Commissioner of Police — to intercept any Communication based on a warrant issued by a judge. A warrant is required for intercepting any communication under five circumstances namely:— (a) in the interest of national security; (b) crime prevention or investigation; (c) public wellbeing ; (d) public emergency or safety ; or (e) in furtherance of international mutual assistance agreements.¹⁵ In other words, a warrant issued by the judge is required for surveilling and intercepting any communication under specified circumstances which includes national security and crime prevention or investigation. These safeguards have been inserted to preserve the right to privacy of residence and correspondence protected by Section 37 of the Constitution of the Federal Republic of Nigeria 1999.

The Nigerian government has taken additional steps to guarantee citizens' right to privacy by enacting the Nigerian Data Protection Act 2023 (NDPA) – the principal legislation governing data privacy. Additionally, other secondary legislations protecting data privacy in Nigeria includes the Guidelines for the Management of Personal Data by Public Institutions in Nigeria, Consumer Code of Practice Regulations 2007 (NCC Regulations), Freedom of Information Act, 2011 (FOI Act), Cybercrimes (Prohibition, Prevention Etc.) Act 2015 (as amended),

14. SPACES FOR CHANGE, *Civic Space in West Africa: Trends, Threats and Futures* (2023); <https://closingspaces.org/civic-space-in-west-africa-trends-threats-and-futures/>

15. See Section 12 of the Act

National Identity Management Commission (NIMC) Act 2007, etc. All these regulations insist on confidentiality of records, consent and prohibits the interception of, and access to personal records without authorization. For instance, the Cybercrimes Act criminalizes the unlawful interception of communications intentionally and without authorization by whatsoever means, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network.¹⁶

Although the Nigerian Constitution guarantees the right to personal privacy (Section 39 of the Nigerian Constitution), certain national regulations mandate cooperation between service providers and law enforcement officers. One such regulation¹⁷ requires licensed telecommunication companies to **“transmit all subscriber information captured and registered within the preceding month ... to the Central Database.”** In this section, service providers are obligated to release and transmit all subscriber information and phone records in their custody to relevant authorities.

The open language and lack of definitions in the numerous legislations that confer surveillance powers upon state authorities easily allows for subjective interpretation in ways that rationalize suppression of dissent or brings all sorts of misdemeanors under the purview of each law. For instance, the Department of Security Service (DSS) reportedly detained a businessman in 2021 for making comments in favor of the Indigenous People of Biafra (IPOB) on social media.¹⁸ Similarly, the DSS, invoking Section 13(2), charged a woman in the Federal High Court for making pro-IPOB comments on Facebook.¹⁹ In 2017, the Nigerian government proscribed the Indigenous People of Biafra engaged in secessionist agitations in the South-Eastern region of Nigeria.²⁰ For social media users and civic actors, this provision further raises the risk of exposure to online surveillance in sharp contrast to citizen's fundamental right to personal privacy.

16. Section 12 (1) of the Act

17. National Communication Commission. Guidelines for the provision of internet service.

<https://www.ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file>

18. Tribune 2021, [Businessman arrested by DSS over alleged IPOB comments on social media, lawyer alleges](#), accessed on Jul 13, 2023

19. [FG Arraigns Lady for Promoting IPOBs Activities on Facebook](#)

20. The declaration of the independent state of Biafra led to the Nigeria-Biafra civil war (1967-1970) which resulted in devastating loss of life, claiming millions of lives. Although the war officially ended on January 12, 1970, the legacy of Biafra continues to endure, with several pro-Biafran separatist groups, including the Movement for the Actualization of the Sovereign State of Biafra (MASSOB), Indigenous People of Biafra (IPOB), and the Biafra Zionist Federation, still advancing their separatist agitations. See PUNCH: Court affirms IPOB's proscription, designation as terrorist group.

Accessible at https://punchng.com/court-affirms-ipobs-proscription-designation-as-terrorist-group/#google_vignette

1.3 NATIONAL SECURITY IS A MAJOR DRIVER OF SURVEILLANCE:

Nigeria's version of the 9/11 terrorist attacks in New York is the August 2011 suicide car bombing at the United Nations headquarters in the Federal Capital Territory, Abuja, killing at least 18 people.²¹ Reproducing the United States' response to the 9/11 attacks, the government resorted to strengthening the legal architecture for combating terrorism and the expansion of the government's surveillance powers. The government also capitalized on the public outcry against the then frequent suicide bombing attacks in public places²² to gain massive public support for its surveillance operations. Acts of terrorism heightened despite the enactment of the Nigeria's Terrorism Prevention (Prohibition) Act (2011), leading to additional amendments that increased the number and the scope of the offences; broadened the definition of terrorism; significantly increased the sentences for terrorist offences; and increased the scope of the ancillary powers.²³ Apart from the tightened legal frameworks, numerous security initiatives involving mass surveillance operations were also rolled out to enhance national security, detect security breaches and terrorist



Source: Al Jazeera

21. BBC News, Abuja attack: Car bomb hits Nigeria UN building, Published 27 August 2011, <https://www.bbc.com/news/world-africa-14677957>

22. Andrew Walker, United States Institute of Peace, Special Report: What Is Boko Haram? Special Report 308 ~ June 2012, <https://www.usip.org/sites/default/files/SR308.pdf>

23. United Nations Office on Drugs and Crimes (UNODC), User's Guide to the Terrorism (Prevention) Act, 2011 (TPA) as amended by the Terrorism (Prevention) (Amendment) Act, 2013 (TPAA) Published 2021: https://www.unodc.org/conig/uploads/documents/UNODC_Users_Guide_to_Terrorism.pdf

activities, and make the country safer.²⁴ Since then, the term, national security, has become a fluid and nebulous concept that defies meaning in the strictest legal sense. In fact, security means anything the state regards as so.

Beyond legal provisions that mandate security operatives to conduct surveillance, training toolkits developed by independent entities encourage prosecutors, law enforcement and security operatives to use “surveillance records” of terror suspects to prove offences of terrorism. One such training user guide or toolkit emphasizes the importance of proving the criminal liability of suspects participating in terrorist meetings²⁵ by relying on “oral evidence of witnesses or suspects, **telecommunications and surveillance data**, written notes and records”.²⁶ Accordingly, surveillance operations are deemed necessary in the investigation of offences to gather as much evidence as possible about the details, circumstances, purpose and background of a wide range of meetings to ascertain their linkage with terrorist activity. The official use of surveillance as an anti-terror strategy is further buttressed by the Nigerian government's deployment of a web-based Enhanced Financial Analysis and Surveillance System (e-FASS) as well as the “harmonization of the activities and operations of GSM providers and users to enable control and proper monitoring of terrorist activities.”²⁷

The national security mantra has provided grounds for justifying arbitrariness by law enforcement agents as steps taken to protect public safety.²⁸ The state's repressive actions—whether military or civilian—could not have been accomplished without the help of security agencies undertaking surveillance and gathering intelligence. Regimes principally relied on the secret service to achieve their authoritarian objectives. Under the military era in the country, the fluid nature of the then National Security Organization's (NSO's)²⁹ mandate strengthened its image as an agency whose role covered all aspects of security

24. United Nations Office on Drugs and Crimes (UNODC), User's Guide to the Terrorism (Prevention) Act, 2011 (TPA) as amended by the Terrorism (Prevention) (Amendment) Act, 2013 (TPAA) Published 2021: https://www.unodc.org/conig/uploads/documents/UNODC_Users_Guide_to_Terrorism.pdf

25. As set out in section 3 of the Terrorism Prevention Amendment Act (2013)

26. See United Nations Office on Drugs and Crimes (UNODC), User's Guide to the Terrorism (Prevention) Act, 2011 (TPA) as amended by the Terrorism (Prevention) (Amendment) Act, 2013 (TPAA) Published 2021: https://www.unodc.org/conig/uploads/documents/UNODC_Users_Guide_to_Terrorism.pdf

27. See Statement by Dr. Fatima Akilu Director, Office of the National Security Adviser, *ibid*.

28. Isaac Olawale Albert, Terror as a political weapon: reflections on the bomb explosions in Abacha's Nigeria, IFRA Special Research Issue VOL. 1, p. 37-56

29. This agency is now known as the State Security Service (SSS) or Department of State Services

activities, exercising power to do a wide range of things such as **“obtain by secret sources or other means accurate intelligence regarding persons or organizations whether within or outside Nigeria, engaged in acts of espionage, subversion or sabotage against Nigeria, or engaged in acts which may threaten the security of Nigeria...”** and to **“...maintain records of individuals and organizations engaging in subversive activities.”**³⁰

Against this backdrop, incidents tracked on the Closing Spaces Database³¹ shows that criminal charges against activists and journalists are usually initiated by powerful intelligence bureaus and security agencies statutorily mandated to respond to highly-sensitive cases bordering on national security. An independent report also documented how an array of security laws governing the administration of criminal justice such as sedition, criminal defamation and treason/treasonable felony have been frequently invoked to harass, arrest, detain and prosecute private citizens including civil rights agitators and journalists for very benign activities such as peaceful protests, publication of critical and satirical commentary, and other forms of dissent.³²



30. Third World Legal Studies-1996-97, <https://core.ac.uk/download/pdf/303859358.pdf>

31. See www.closingspaces.org

32. Action Group on Free Civic Space, Nigeria: Shrinking Civic Space in the Name of Security, (2022) <https://closingspaces.org/7965-2/>

1.4 SURVEILLANCE IS A VESTIGE OF MILITARY RULE:

During the military era, Decree Number 2 of 1984, titled, State Security (Detention of Persons) Decree, empowered the Chief of Staff at Supreme Headquarters to detain anyone suspected of being a security risk indefinitely without trial. Detention was for three months initially, and then renewable for an unlimited period. This Decree provided legal justification for the detention and torture of many people considered "enemies" of the government in cells manned by the National Security Organization (NSO) now known as DSS. Decree 2' infamous siamese twin, Decree Number 4—Public Officers Protection Against False Accusation Decree 1984—drastically curtailed press freedoms and criminalized the publication of any material considered embarrassing to any government official.³³

Many journalists were placed under massive surveillance, detained without trial or were tried by Special Military Tribunals that disregarded the constitutionally-protected presumption of innocence.³⁴ Journalists and media organizations were regularly harassed by security agents while organized interest groups whose members dared to criticize the government openly or engaged in demonstrations, public gathering or strikes were proscribed.³⁵ More specifically, General Abacha banned the two political parties; dismantled political structures, including the National Assembly and civilian governorships; and proscribed all political associations, public processions and other activities perceived to be political in nature.

1.5 SPYWARE TRADE IS HIGHLY-PROFITABLE:

An independent study that extensively examined the supply of surveillance technologies to Nigeria found that many countries are raking in profits from the sale of spywares to Nigeria, with China, Israeli and the United States topping the list.³⁶ Examples include:

33. Michèle Maringues, The Nigerian Press: Current state, Travails and Prospects, contained in Nigeria During the Abacha Years (1993-1998) | 'Kunle Amuwo, Daniel C. Bach, Yann Lebeau at pp p. 185-218, <https://books.openedition.org/ifra/640?lang=en>

34. Michael P. Seng and Gary T. Hunt, The Press and Politics in Nigeria: A Case Study of Developmental Journalism, p.95, <https://lira.bc.edu/files/pdf?fileid=cad4a6b4-7fad-400f-a514-9309ecd62e4c>

35. Human Rights Watch: NIGERIA "THE DAWN OF A NEW DARK AGE" Human Rights Abuses Rampant as Nigerian Military Declares Absolute Power

36. Victoria Ibezim-Ohaeri et al, Action Group on Free Civic Space, Security Playbook of Digital Authoritarianism in Nigeria (December 2021): <https://closingspaces.org/the-security-playbook-of-digital-authoritarianism-in-nigeria/>

- China ~ (CASC CH-3A armed tactical unmanned aerial vehicle (UAV), Mugin commercial UAV, DJI Phantom and ZTE's Video Surveillance Subsystem (VSS))
- Israel (Elbit Systems' Open Source Intelligence (OSINT) solution and Elbit Systems' PC Surveillance Systems (PSS), ADS Aerostar UAV, Circles, C4i, and Wise Intelligence Technology (WiT))
- United States: Target Sight System, Forensic Tool Kit (FTK), Blue Coat System's Deep Packet Inspection, DPI; RayoByte, formerly known as Blazing SEO's Internet Protocol (IP) addresses for “scraping”.



The study found that Nigeria has spent at least US\$40m on internet interception technologies from various foreign companies across the world such as Elbit Systems (Israel), Romix (Cyprus), Packets Technology (Bulgaria), and Hacking Team (Italy). These technologies allow the government to spy on citizens' emails, instant messages, browsing histories, and other online activities. Nigeria has also invested heavily in public space surveillance projects with Chinese companies: ZTE and Huawei. The projects involve installing thousands of CCTV cameras with facial and car number plate recognition capabilities in Lagos and Abuja. The total cost of the projects is estimated at US\$470m for ZTE and US\$113m for Huawei.³⁷

In comparison to what other critical departments—like education, transport, health, social services—receive, security gets the lion share of national budgets, most of which are spent on procuring the most sophisticated military wares and

37. Security Playbook, *ibid.*

and surveillance devices. Out of the 982 billion Naira earmarked for Nigeria's 2021 supplementary budget, the DSS got a total of 17.5 billion Naira for the purchase of vehicles and arms etc, while the sister agency—National Intelligence Agency—got 4.8 Billion Naira to purchase sophisticated spywares for monitoring WhatsApp calls and Thuraya, a satellite telephone.³⁸ Enlarged security budgets is accompanied by significant expansion of domestic surveillance and policing by both state and non-state actors. While huge budgetary sums have been allocated to purchasing surveillance technologies to combat criminal activities, much hasn't improved in terms of security, and various reports showing that insecurity is on the rise, driving the country to the edge of fragility.³⁹

1.6 NIGERIA'S POPULATION HAS INCREASED EXPONENTIALLY:

Nigeria's population has exponentially increased, ballooning from an estimated population of 16,250,000 natives and 3,000 Europeans in 1920⁴⁰ to over 200 million people in 2023. Nigeria's population is projected to grow from more than 186 million people in 2016 to 392 million in 2050, becoming the world's fourth most populous country.⁴¹ The bloating population figures means that the manual or traditional surveillance practices are now inadequate to meet the state's policing needs and expanding appetite for control. Technology provided a respite, by ushering in an array of sophisticated alternatives that enable states to conduct mass surveillance just at the click of a button.

On one hand, these technologies enhance public security systems. On the other hand, they serve other darker purposes that breach privacy rights, repress political freedoms, and unleash severe limitations on human rights and civic agency. The dual use of these technologies poses potential threats and raise regulatory concerns while simultaneously accentuating the power dynamics fueling their substantial procurement in Nigeria.

1.7 THE GLOBAL DRIFT TOWARDS AUTHORITARIANISM IS ON THE RISE:

In 2020, an international investigative journalism collaboration, “Pegasus Project” revealed the staggering extent that governments around the world have

38. Sunday Aborishade, Punch Newspapers, NIA gets N4.87bn budget to track, intercept calls, messages, July 12, 2021, <https://punchng.com/nia-gets-n4-87bn-budget-to-track-intercept-calls-messages/>

39. [Tope Shola Akinyetun, Victor Chukwugoku Ebonine, Iyase Osariyekemwen Ambrose](#), Defence and Security Quarterly, Unknown gunmen and insecurity in Nigeria: Dancing on the brink of state fragility, Security and Defence Quarterly 2023;42(2):16-34, <https://securityanddefence.pl/Unknown-gunmen-and-insecurity-in-Nigeria-Dancing-on-the-brink-of-state-fragility.163462.0.2.html>

40. Colonial Annual Report No 1098, Report for 1920

41. CIA: The World Factbook, <https://www.cia.gov/the-world-factbook/countries/nigeria/>

conducted surveillance with the use of the spyware – Pegasus – provided by the Israeli spyware firm, the NSO Group. The project revealed that how NSO Group's Pegasus spyware has been used to facilitate human rights violations around the world on a massive scale, following the revelation of 50,000 phone numbers of potential surveillance targets. The targets included leading opposition politicians, heads of states, human rights activists, lawyers, political dissidents, and journalists.⁴² This swiftness with which countries are acquiring and deploying surveillance capabilities with minimal legal safeguards to protect human rights evinces states' thirst for authoritarian power.

Long before the “Pegasus Project” revelations, surveillance programs targeting dissenters and activists have always been critical components of the national security architecture both under the military and democratic rule. Under the military era, security forces routinely monitored and occasionally stormed conferences they perceived as forums for prodemocracy groups.⁴³ The Government routinely tape-recorded conversations while virtually all senior editors of the weeklies Tell, Dateline, The News, and Tempo, and the daily A.M. News were subjected to surveillance and harassment by security agents.⁴⁴ Security forces routinely seized entire runs of Tell magazine when cover stories offended the Government. Targeted surveillance of journalists and news editors were often accompanied by newspaper seizures, affecting their sales and dissemination, which caused great financial distress for media houses, forcing many to discontinue publication. As an author succinctly captured:

“Not long after its establishment, under General Obasanjo, the NSO started arresting individuals who had the courage to criticise government policies, clamping them into jail... Under civilian rule, between 1979 and 1983, the ruthlessness of the NSO persisted. The organisation was used to silence opposition political groups and individuals. Even the military was not spared, as some of its members presumed to be real or potential coup planners were put on the watch list... NSO cells brimmed with numerous detainees held mainly on unsubstantiable grounds. Consequently, Nigeria now represented the classical image of “Big Brother watching you.”⁴⁵

42. Forbidden Stories: The Pegasus Project, https://forbiddenstories.org/projects_posts/pegasus-project/, retrieved 8 July 2024

43. U.S. Department of State, Nigeria Country Report on Human Rights Practices for 1996, Released by the Bureau of Democracy, Human Rights, and Labor, January 30, 1997.

44. U.S. Department of State, 1997.

45. THIRD WORLD LEGAL STUDLES-1996-97, p. 75

Today, the "Big Brother watching you" mandate of the then NSO has been transferred to the State Security Service, now known as Department of State Security (DSS), but the patterns of infringement and the impact on civic participatory rights have not abated. The creation of the SSS has instead strengthened its use as an oppressive arm of the government against so-called critics and detractors.⁴⁶ To legalize the onslaughts on civic actors, an array of legal and policy provisions now gives express legal backing to the government's intrusive data-collection and surveillance activities. Most of these provisions are embodied in criminal and security laws, and other regimes designed to address transnational challenges—including terrorism, drug flows, organized crime and proliferation of weapons of mass destruction.⁴⁷

1.8 SECRECY BOOSTS SURVEILLANCE AND CIVIC REPRESSION:

What makes surveillance dangerous is that it thrives on secrecy. It becomes more complicated when covered with the veil of national security. Under that veil of secrecy and national security, authorities have monitored protesters' personal information, communications, travels, and finances, and slammed them with charges of terrorism financing. After surveilling their financial transactions, the Federal Government prosecuted and froze the accounts of 20 #EndSARS campaigners, alleging that the funds in their accounts might have been linked to terrorist activities.⁴⁸ Warrantless wiretapping of dissident groups and the political rivals of incumbent politicians is also quite commonplace, especially during election seasons.⁴⁹ A private telephone chat involving the major opposition candidate during the 2023 elections was wiretapped and leaked on the internet to discredit him.⁵⁰

Digital technologies make the state's surveillance operations easier by eroding privacy walls for citizens. In other words, secrecy is an instrument of power and of the retention⁵¹ of power. National security alone does not pose threats to individual freedoms. It is the secrecy that characterizes national security that makes it powerful, and even dreadful and dangerous. In this context, laws, national security and secrecy go hand in hand. Laws give legal backing to

46. THIRD WORLD LEGAL STUDIES-1996-97, p. 77

47. Ibezim et al...

48. [Eniola Akinkuotu](https://punchng.com/cbn-accuses-endsars-campaigners-of-terrorism/), Punch Newspapers, CBN accuses #EndSARS campaigners of terrorism, <https://punchng.com/cbn-accuses-endsars-campaigners-of-terrorism/>

49. Victoria Ibezim-Ohaeri et al...

50. The Cable: Obi-Oyedepo Leaked Audio: A Dangerous Slope; <https://www.thecable.ng/obi-oyedepo-leaked-audio-a-dangerous-slope>

51. Dennis Broeders, The Secret in the Information Society, Springer Link, [Published:14 April 2016, https://link.springer.com/article/10.1007/s13347-016-0217-3](https://link.springer.com/article/10.1007/s13347-016-0217-3)

repressive measures; national security provides the pretext for the repressive acts while secrecy frustrates scrutiny and accountability. Armed with three instruments—laws, security and secrecy—any country can stretch state power to authoritarian heights especially where systems and institutions are weak.

Whereas secrecy can be justified by the need to protect the confidentiality of the executive branch's intelligence sources and methods, preventing disruption to ongoing investigations, and averting diplomatic embarrassment,⁵² a right balance must be struck between freedom of information and state secrets.⁵³ In 2023, Nigeria enacted the Data Protection Act, establishing the Nigeria Data Protection Commission (NDPC) for the regulation of the processing of personal information and providing legal safeguards for the processing of personal data and the interests of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria. Similarly, Nigeria's Lawful Interception of Communications Regulations (LICR) 2019 makes it lawful for certain authorized persons to intercept any communication based on a warrant issued by a judge under five specified circumstances.⁵⁴

CONCLUSION

Officially, spyware companies provide tools to governments countering terrorism and combatting crime. For example, the NSO Group on their website described their activities as follows: “NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.”⁵⁵ Evidence is now showing that surveillance is not only used in the context of crime control and countering terrorism.

From the foregoing, while the intended purposes for government monitoring may vary, exerting control over citizens now forms part of the broader objectives of state surveillance. In the case of Nigeria, the advent of democracy in Nigeria

52. Nathan Alexander Sales, page 814

53. Cemil Kaya, Selcuk University Law Faculty

54. See Section 12

55. See NSO website - <https://www.nsogroup.com/>, retrieved 8 July 2024

neither eroded the colonial mentality to control local populations nor dismantled the heavily-flawed institutions and culture of intolerance for dissent that characterized the era of military rule. Whereas the colonialists' surveillance agenda aimed to protect their imperialists and economic interests, current political powerholders — whether military or democratic — mainly aim to entrench themselves in office by monitoring dissidents, intimidating, and suppressing all forms of opposition. Regardless of the surveillance agenda, they produce uniform consequences ranging from prolonged detentions, phantom criminal charges against critics, media censorship, forced disappearances, repressive legislation, arbitrary terrorism designation and human rights abuses.

Helped by the modern-day technological revolution, the manual forms of surveillance adopted under the military rule have been displaced by more sophisticated mass surveillance technologies. The proliferation of companies around the world supplying surveillance technologies has made it easier for governments to acquire intelligent monitoring systems and products with relative ease while diminishing the transparency and accountability of its use.

CHAPTER

2



DUAL-USE NATURE OF SURVEILLANCE TECHNOLOGIES

The word “dual-use” is rooted in a distinction between 'benign' versus 'malign', or 'civil' and 'military' uses. A common definition of DUTs refers to technologies capable of both civilian [primary purpose] and military/strategic [secondary potential use] applications.⁵⁶ The U.S. government's Code of Federal Regulations defines dual use as “items that can be used both in military and other strategic uses... and commercial applications.”⁵⁷ Dual-use technologies with surveillance capabilities therefore refers to 'items ... specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data from information and telecommunication systems.'⁵⁸ It is the responsibility of governments to develop a list of technologies qualifying as dual-use technologies (DUTs). The implication is that what constitutes DUTs will vary from country to country.

Surveillance technologies are extremely useful to many types of government and commercial activities, including national defense, local law enforcement, disaster assessment and relief, search and rescue, community planning, resource exploration, wildlife monitoring, property tax assessment, border patrol, camouflage detection, treaty negotiation and verification.⁵⁹ Intrinsically, surveillance technologies are considered non-civilian in nature, and as such, can only be legitimately acquired by military or intelligence agencies. “Military” applications refer to uses for the purpose of countering terrorism or insurgency, and national security applications.⁶⁰ They can be used lawfully and legitimately with appropriate safeguards, though they can also be used in an unacceptable manner by governments.”⁶¹

2.1 MAPPING DUAL-USE SURVEILLANCE TECHNOLOGIES USED IN NIGERIA:

An array of surveillance and DUTs are imported into, and used in Nigeria for a wide range of purposes not limited to civilian and military communications, surveillance, mobile telephony, broadcasting, cybersecurity, fiber optic networks, agriculture, investigative journalism, data protection, commercial delivery, border security, anti-theft services, disaster management, meteorology, business efficiency, project coordination and so forth. A vast

56. European Commission: Exporting dual-use items, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en, retrieved 8 July 2024

57. *ibid*

58. *ibid*

59. Julie K Petersen, *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications*, © 2000 by Taylor & Francis Group, LLC, Page 1-17

60. [Dual-Use Technologies and National Security | International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings | The National Academies Press](#)

61. [Guiding Principles on Government Use of Surveillance Technologies \(state.gov\)](#)

proportion of DUTs is used in the telecommunications sector to improve connectivity and support national development. While significantly enhancing the efficacy of communication networks, they can be exploited for covert communication by malicious actors.

Some kinds of surveillance equipment, encompassing both hardware and software, are used by law enforcement agencies to monitor and track criminal activities, thereby enhancing public safety. For instance, Unmanned Aerial Vehicles, (UAVs), commonly known as drones, often used by law enforcement for crime detection, have diverse applications ranging from agricultural monitoring, border security, environmental monitoring, and disaster response. They can also be used during military operations, including reconnaissance and targeted strikes. Beyond these legitimate purposes, the same UAVs can be used for unauthorized surveillance, by both state and non-state actors, infringing on individuals' privacy and potentially violating human rights. Cybersecurity tools are equally indispensable for protecting information systems from cyber threats. Used by both the public and private sectors in Nigeria to defend against cyber-attacks and ensure the integrity of critical infrastructure, they can also be repurposed for offensive cyber operations.

Spaces for Change and the Action Group on Free Civic Space (AGFCS)'s 2021 report, [the Security Playbook of Digital Authoritarianism in Nigeria](#), and subsequent report,⁶² presented data regarding the importation and deployment of “dual use technologies” in Nigeria. That report listed the imported technologies in Nigeria, their importers and the countries they were imported from.

The evidence showed that from 2008 to 2021, the federal ministries, departments, and agencies (MDAs) acquired the greatest number of technologies with surveillance capabilities. Notably, telecommunications and information security rank the highest procurement by both states and the federal government. As we shall see below, suppliers may have taken advantage of the weak regulatory and importation controls that characterize developing countries to sell and export their products with little or no scrutiny, increasing citizens' exposure to arbitrary surveillance, including physical harm and other human rights abuses.

62. Spaces for Change (2023) Mapping the Supply of Surveillance Technologies to Africa: Nigeria Country Report, DOI: 10.19088/IDS.2023.027

2.2 ARBITRARY DEPLOYMENT OF DUAL-USE SURVEILLANCE TECHNOLOGIES IN NIGERIA:

The importance of surveillance technologies cannot be overemphasized. For instance, they have aided in tackling insecurity such as tracking terrorists, kidnappers, money launderers, drug traffickers, and human traffickers.⁶³

Likewise, the geographic mapping of terrorists and other targets may not be possible without the employment of spyware and other surveillance technologies, which, in turn, bolsters the effectiveness of coordinated military attacks. While these technologies have significantly enhanced the country's security landscape, their potential for repurposing and diversion of security-based technologies is alarmingly high. The following case studies present some examples:

1. C4i (Command, Control, Communications, Computers, and Intelligence): The C4i was procured by the former Rivers State Governor from an Israeli military firm, to aid in combating crimes in the state. Subsequent events revealed that the technology had been used to facilitate the governor's spying of his major political contenders in the opposition parties.⁶⁴



63. [The Battle for the Worlds Most Powerful Cyberweapon - The New York Times \(nytimes.com\)](https://www.nytimes.com)

64. Premium Times, "[INVESTIGATION: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others. \(2016\)](#)

2. Hacking Team and FinFisher: This intrusion software was used to spy on politicians and regime opponents. Hacking team worked with the governor of Bayelsa State⁶⁵ via contracts, classified as “intelligence”, channeled through an Israeli company, NICE, and then V&V Nigeria, to procure Hacking Teams' most invasive and ruthless intrusion softwares called Remote Control Systems. These softwares can compromise most operating systems, except iOS, encrypted computers and smartphones, even if the target was outside the government's “monitoring domain”⁶⁶ According to reports, the technology could also track the exact position of a user, even when abroad.⁶⁷ Politicians are primarily motivated by elections and political interests to acquire spyware technologies under the guise of combating insecurity in their respective states.⁶⁸

3. Remote Control System (RCS): The RCS is configured to attack, infect, and monitor target personal computers and smartphones in a stealth way. When a target is infected, the RCS allows attackers to access a variety of information, including emails, messages, target positioning, files, screenshots, microphone eavesdropped data, and camera snapshots.⁶⁹ A 2015 report holds that the former Governor of Bayelsa State, acquired the technological tools from Hacking Team, an Italian firm that specializes in developing tools for government agencies to hack their own citizens' information.⁷⁰ Consequently, among other uses, the technology was deployed in hunting down an activist who was incarcerated by the governor, in late 2013, over a Facebook post that was critical of his government.⁷¹

4. GSM Tracking System: Former Nigerian President, Goodluck Jonathan awarded an approximately N6 billion contract to an Israeli security firm, V & V Nigeria Limited, based in Abuja, to acquire a GSM Tracking System for the Nigeria Police Force and upgrade systems at the Department of State Security.⁷² A Dutch company, Digivox, which specialises in “lawful and tactical interception

65. [Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses - Carnegie Endowment for International Peace](#)

66. Ogala Emmanuel, Premium Times, INVESTIGATION: Bayelsa Governor hires world's most ruthless hackers for N100M to hack computers, phones in Nigeria, Accessed via <https://www.premiumtimesng.com/investigationspecial-reports/186391-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-computers-phones-in-nigeriainvestigation-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-c.html>

67. Ogala, E, *ibid.*

68. Ibezim-Oheri et al (2021)

69. Ogala, E, *ibid.*

70. Ogala, E, *ibid.*

71. Ogala, E, *ibid.*

72. Vanguard, [“FG to build multi-billion naira GSM tracking device for police” \(2010\); Premium Times: “EXCLUSIVE: Nigerians beware! Jonathan procures N11billion equipment to tap your phones”. \(2015\)](#)

systems, secure GSM communication, GPS tracking devices and voice logging” has also been linked to Nigeria.⁷³ Law enforcement agencies like the SSS as well as the Nigerian GSM service providers – MTN Nigeria, Globacom, Airtel Nigeria and Etisalat Nigeria – are reportedly using this Digivox technology to intercept electronic communications.

5. Distributed Denial of Service (DDoS): DDoS (distributed denial-of-service) attack is a malicious attempt to disrupt the regular traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. This prevention of regular traffic from arriving at its destination overwhelms the victim's server or network, resulting in a denial-of-service. Proxy Internet Protocol (IP) addresses and virtual private networks (VPN) services are often weaponized to carry out these attacks. For instance, DDoS attacks with IPs sourced from US-based RayoByte has been against four other outlets new media outlets in Nigeria like Peoples Gazette.⁷⁴ Another cyber intelligence system procured by Jonathan's administration in partnership with the National Security Adviser had also been used to launch Distributed Denial of Service (DDoS) attacks on websites critical of the government, especially before the elections.⁷⁵ The National Information Technology Development Agency (NITDA) through its Computer Emergency Readiness and Response Team has also detected the activities of Anonymous Sudan, a hacktivist group—known for its politically and religiously motivated cyber campaigns—targeting national digital infrastructure. Their tactics include targeted attacks on government digital services, using various attack types particularly DDoS attacks.⁷⁶

6. International Mobile Subscriber Identity (IMSI) Catcher: An IMSI catcher is an electronic device that tracks and intercepts mobile phone communications.⁷⁷ It also operates as a phone eavesdropping device designed to intercept the traffic of mobile phones and can track mobile phone users' location data.⁷⁸ An investigation revealed that one G12 IMSI Catcher was supplied to Nigeria's

73. Ogala Emmanuel, *Premium Times*, U.S. spy program reforms spotlight Nigeria's expanding surveillance program, February 10, 2014, <https://www.premiumtimesng.com/news/154931-u-s-spy-program-reforms-spotlight-nigerias-expanding-surveillance-program.html>

74. CPJ, *Premium Times*, Cyberattackers used US company to crash media sites in Nigeria, others, September 8, 2023, <https://www.premiumtimesng.com/news/top-news/623974-cyberattackers-used-us-company-to-crash-media-sites-in-nigeria-others.html?tztc=1>

75. Spaces for Change, Action Group on Free Civic Space "Security Playbook of Digital Authoritarianism", PG 46, (2021); *Premium Times* "INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack unfriendly websites" (2016)

76. iTedgeNew Africa: NITDA alerts on DDOS attack targeting critical national digital infrastructures, August 3, 2023, <https://www.itedgeNews.africa/nitda-alerts-on-ddos-attack-targeting-critical-national-digital-infrastructures/>

77. Zimperium, IMSI Catcher, <https://www.zimperium.com/glossary/imsi-catcher/>

78. SMS Broadcaster, "3 Different Functions of The IMSI Catcher". (2023)

former National Security Adviser, Sambo Dasuki through M.I. Smart Solutions, based in Abuja, a subsidiary of Mi Marathon Resources Limited at the cost of \$329,800, during Jonathan's administration.⁷⁹

7. Wise Intelligence Technology (WIT): There is evidence that Wise Intelligence Network Harvest Analyzer System, Open-Source Internet Monitoring System and Personal Internet Surveillance System is used in Nigeria. An investigative report in 2013 revealed how former Nigerian president, Jonathan despite public outcry and legislative constraints awarded \$40 million to an Israeli firm, Elbit Systems to procure WIT in a bid to spy on citizens' computers and online communications under the pretext of national security and intelligence gathering.⁸⁰

8. Compulsory Biometric- and Data Collection Initiatives: Apart from spyware technologies, other sophisticated methods of surveillance include mobile interception, social media monitoring and compulsory data collection initiatives. Likewise, compulsory data harvesting programs are all hinged on the collection of biometric data or characteristics about the unique behavioral and physical characteristics of individual persons. Multiple biometric collection schemes are currently enforced compulsorily which require citizens to provide fingerprints, facial scans, iris scans, ears and other biological features. The biometric ID systems stored in national databases are linked to citizens' mobile phones, bank accounts, and national ID cards. The main suppliers of biometric ID technologies are Thales (France/Singapore), Dermalog Identification (Germany), BIO-key (USA), and Chongqing Huifan (China). The total value of the contracts exceeds US\$500m.⁸¹

9. Non-state actors are also involved: The abuse of spyware and other dual-use technologies is not limited to state entities like the military or law enforcement formations. Rather, non-state entities, especially terrorist organizations, are also involved. An independent study found that non-state actors are already deploying semi-autonomous drones that are inexpensive relative to the far costlier and more sophisticated weaponry of states.⁸² They can maneuver the drones to circumvent the boundaries of vehicle-borne threats, thereby maximizing the destructiveness and giving the actors an

79. Premium Times, ""[INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack unfriendly websites](#)"" (2016)

80. Premium Times, "[Elbit Systems Officials Arrive; Begin Installation of \\$40 Million Spy Facility for Nigeria](#)". (2013)

81. Victoria Ibezim-Ohaeri et al, 2021

82. Sarah Kreps, Foreign Policy at Brookings, Democratizing Harm: Artificial Intelligence in the Hands of Nonstate Actors, November 2021, https://www.brookings.edu/wp-content/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf

asymmetric advantage. In Nigeria, there is evidence that terrorists mostly plan their attacks employing one form of communication or information technology or the other.⁸³ Boko Haram has begun using drones for surveillance, though authorities fear they will rapidly progress to weaponized platforms.⁸⁴ As extremists organizations quickly adopt the use of drones, analysts says that the greater commercial accessibility to (unmanned aerial vehicle) technology will make UAVs more attractive as a delivery method for terrorist attacks.⁸⁵



83. Ipadeola, Abosede. "[Cyberethics, Spyware And The War On Terrorism in an Age of Liberal Democracy](#)". Researchgate. (2014)

84. Cara Anna, "Nigerian Leader: Islamic Extremists are Now Using Drones," Associated Press, 30 November 2018, <https://apnews.com/>

85. Cara Anna, *ibid.*

CHAPTER

3

Source: Marketforces Africa



**REGULATING THE
IMPORTATION
OF DUAL-USE
TECHNOLOGIES
IN NIGERIA**

The regulation of spyware transpires at the import and export points. Nigeria is a major importer of surveillance and dual-use technologies imported from Israel, China, United States and other countries. As an importing country, domestic regulation mainly takes the form of import controls. Generally, Nigeria does not prohibit the importation of surveillance technologies as no law expressly outlaws such imports. Similarly, the prohibited list of imports maintained by the Nigeria Customs Services⁸⁶ does not exclude surveillance technologies. There are four categories of importers of controlled items:

- (i) ministries, departments and agencies (MDAs) of the federal government. The specific MDAs authorized to import military equipment.
- (ii) military and paramilitary organizations in Nigeria.
- (iii) embassies
- (iv) private corporations and persons.⁸⁷

While it can be safely assumed that items not expressly prohibited can be imported, the Office of the National Security Adviser (ONSA) maintains a list of 'controlled importation'. This list contains surveillance technologies and items typically required by the military as well as some other items that would qualify as DUTs, including surveillance equipment that can be deployed for a wide range of activities such as broadcasting, telecommunications, counter-surveillance, and remotely piloted aircraft (drones). This chapter will examine the regulatory frameworks, licensing conditions and domestic controls for the importation of spywares and other dual-use technologies in Nigeria.

3.1 REGULATING THE IMPORTATION OF DUTs IN NIGERIA:

The principal regulations governing the importation of surveillance and other dual use technologies into Nigeria are the ONSA's End User Certificate (EUC) regime, the National Office for Technology Acquisition and Promotion

86. See [Prohibited Items List During Import - Nigeria Trade Portal](#)

87. –[Embassies, MDAs and Military End-User Certificate Portal \(nsa.gov.ng\)](#). The entities mentioned in (i) to (iii) may either procure the military equipment by directly by themselves or through a private contractor (except for arms and ammunitions which may only be imported by security agencies). In all events, however, the importer is required to obtain EUC in respect of the controlled items. EUC applications by private persons will be routed through the Office of the Commandant General, Nigeria Security and Civil Defence Corps (NSCDC) who would recommend the grant of EUC to ONSA - –[Remotely Piloted Aircraft End-User Certificate Portal \(nsa.gov.ng\)](#)

(NOTAP) Act, Nigeria Customs Service Act, no. 35 of 2023, the Federal Ministry of Industry, Trade and Investment (FMITI) and the Nigeria Communications Commission. This list is not exhaustive as there are other administrative measures, ministerial regulations and executive orders that apply to controlled imports. We detail below how these regulations are enforced in practice.

3.1.1 OFFICE OF THE NATIONAL SECURITY ADVISER'S (ONSA'S) END-USER CERTIFICATE:

Nigeria's Office of the National Security Adviser (ONSA) assists the President in carrying out his function as the chief security officer of the country. This office has oversight over every federal security institution in the country: the Armed Forces, the Nigeria Police, the Nigeria Security and Civil Defence Corps, the Economic and Financial Crimes Commission, the National Security Agencies (which includes the State Security Service),⁸⁸ and others. ONSA is primarily responsible for the issuance of licenses for the importation of surveillance technology or equipment. One of the major conditions for importation is obtaining ONSA's end-user certificate (EUC).

The EUC is an undertaking by a purchaser/importer that any of the controlled items/products covered by the process transferred from the exporting country will be used solely and lawfully within Nigeria and will not be transferred or re-exported to any other entity or country without the consent of the issuing authority, ONSA.⁸⁹ The EUC attests that the purchaser is the intended user of the goods and has no intention to transfer them to another person or entity.⁹⁰ The EUC is issued for the acquisition or use of EUC-controlled items and products within Nigeria. Requests for EUC are subject to the screening of the Department of State Services before approval and is valid for one (1) year from the date of issuance to the importer or purchaser.⁹¹ Below is the list of designated items requiring an EUC.

◆ ONSA Designated Items for an End-User Certificate in Nigeria⁹²

- Arms and ammunition (lethal and non-lethal)
- Parts and accessories for military armaments and hardware like guns, armored tanks, ships and aircraft

88. See Section 1 of the National Security Agencies Act.

89. [Office of the National Security Adviser, "Nigeria End-User Certificate Portal"](#) Accessed – May 2024

90. Ibid.

91. Ibid.

92. Ibid.

- Surveillance and Counter Surveillance Equipment
- Lawful Intercept Equipment
- Accoutrement for security forces, web equipment, and uniforms
- Explosives, fireworks, and pyrotechnics for celebrations, military purposes, and construction work
- All forms of chemicals and materials used for explosives
- All forms of bulletproof materials including vests, ballistics materials, vehicles, and bullion vans as well as Hand and Leg Cuff, Police Baton, Riot Crowd Control Devices, Pepper Sprayer, Explosive Detectors, Metal Detectors, Security Doors, Narcotic Detectors, Bar Light, Mail and Baggage Scanners, Stunner, and Electric Baton, etc
- Other items as could be specifically determined
- Items in which the exporting country requires an End-User-Certificate irrespective of the items listed above

The codes for the importation of the above items are reproduced below:

#	HS CODE	DESCRIPTION	CATEGORY
56	85299090	Antennas/STL Equipment	BROADCAST EQUIPMENT
57	85437099	Satellite Uplinks and Downlinks Equipment	BROADCAST EQUIPMENT
58	8525600000	TRANSMISSION APPARATUS INCORPORATING RECEPTION APPARATUS	BROADCAST EQUIPMENT
172	8806100000	Designed for the carriage of passengers	REMOTELY PILOTED AIRCRAFT/UAVs

#	HS CODE	DESCRIPTION	CATEGORY
173	88806290000	Other-UAVs, DRONES	REMOTELY PILOTED AIRCRAFT/UAVs
174	8806990000	Other-UAVs, DRONES	REMOTELY PILOTED AIRCRAFT/UAVs
175	95049090	UAVs, DRONES	REMOTELY PILOTED AIRCRAFT/UAVs
176	8806220000	With maximum take-off weight more than 250g but not more than 7kg	REMOTELY PILOTED AIRCRAFT/UAVs
177	8806920000	With maximum take-off weight more than 250g but not more than 7kg	REMOTELY PILOTED AIRCRAFT/UAVs
178	8806240000	With maximum take-off weight more than 25kg but not more than 150kg	REMOTELY PILOTED AIRCRAFT/UAVs
179	8806940000	With maximum take-off weight more than 25kg but not more than 150kg	REMOTELY PILOTED AIRCRAFT/UAVs
180	8808230000	With maximum take-off weight more than 7kg but not more than 25kg	REMOTELY PILOTED AIRCRAFT/UAVs

#	HS CODE	DESCRIPTION	CATEGORY
181	8806930000	With maximum take-off weight more than 7kg but not more than 25kg	REMOTELY PILOTED AIRCRAFT/UAVs
182	8806210000	With maximum take-off weight more than 250g	REMOTELY PILOTED AIRCRAFT/UAVs
183	8806910000	With maximum take-off weight more than 250g	REMOTELY PILOTED AIRCRAFT/UAVs
184	8805210000	Air combat simulators and parts	SIMULATION EQUIPMENT
185	8805290000	Other Ground flying trainers and parts thereof not specified	SIMULATION EQUIPMENT
186	85176290	Broadband Detection Receiver	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
187	9031809090	CELLULAR TELEPHONE DETECTOR	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
188	9031809090	GSM DETECTOR	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT

#	HS CODE	DESCRIPTION	CATEGORY
189	8517620000	Machines for reception conversion and transmission...of voice, images or data.	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
190	8521909000	New/Customized NVR for 4G Speed Dome, On Board Recorder	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
191	85437013	Non Linear Junction Detector	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
192	8525800000	SECURITY CLEARANCE FOR RPAs, Portable/Under Vehicle Screen System (Coil Trigger)	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
193	90304000	Spectrum Analyzer	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
194	85258091	Technical Surveillance Counter-measure Tool Kit	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
195	76109090	TELESCOPIC PNEUMATIC MASTS	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT

#	HS CODE	DESCRIPTION	CATEGORY
196	90309090	Telephone and Line Analyzer	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
197	85258090	Thermal Imaging Camera	SURVEILLANCE AND COUNTER-SURVEILLANCE EQUIPMENT
198	85437013	Frequency Jammers Equipment	TELECOMMUNICATION EQUIPMENT
199	85255010	Microwave Equipment	TELECOMMUNICATION EQUIPMENT
200	85291019	Satellite Dishes	TELECOMMUNICATION EQUIPMENT
201	85291099	Satellite Transmitter and Receiver	TELECOMMUNICATION EQUIPMENT
202	85177090	Signal Boosters Equipment	TELECOMMUNICATION EQUIPMENT
202	85177090	SIM Box Equipment - Parts and accessories of measuring or checking instruments, appliances an machines	TELECOMMUNICATION EQUIPMENT

204	8802400000	Aeroplanes and other aircraft of an unladen weight exceeding 15000kg	TREATED VEHICLES
-----	------------	--	------------------

Source: Office of the National Security Adviser.⁹³



There are about 262 controlled items and products which requires EUCs for their importation into the country.⁹⁴ When issued, EUCs are valid for one (1) year from the date of issuance to the importer or purchaser.⁹⁵ Requests by private companies are recommended through the Office of the Commandant General, Nigeria Security and Civil Defence Corps (NSCDC).⁹⁶ The general requirements for the obtaining of an EUC is laid out on the website⁹⁷ managed by ONSA. Spyware has four categories with distinct documentation requirements. The first part, **Surveillance and Counter Surveillance Equipment**, contains twelve (12)⁹⁸ prohibited items. Documentation requirements for obtaining an EUC for this

93. [Full HS Codes End-User Certificate Portal \(nscdc.gov.ng\)](https://nscdc.gov.ng/End-User-Certificate-Portal)

94. NSA, [Full HS Codes- End User Certificate: List of Controlled Items and Products](#). Accessed June 5, 2024

95. Ibid NSA,

96. Please see euc.nscdc.gov.ng/remotely-piloted-aircraft/

97. See euc.nscdc.gov.ng

98. Ibid.

category include particulars of the importer's incorporation certificate, the company's director's profile, particulars of directors' travel documents, introduction letters, proforma invoice/ proof of ownership, Form C07 and tax clearance certificate.

The second part, **Remotely-piloted aircraft (Drones)** contains twelve (12)⁹⁹ prohibited items. The major difference with the surveillance equipment category is the requirement for a formal application made to the Nigeria Civil Aviation Authority (NCAA). The third part, Telecommunication Equipment, requires more documentation than all other categories of spyware. They include an approval certificate or grant from the Nigerian Communications Commission (NCC) and a Letter of Contract Award and Letter of Acceptance (though not mandatory), detailed specification of goods, packing list and the bill of lading. The bill of lading is a shipment document detailing the type, quantity, and destination of the goods being shipped. Another major difference is that the incorporation documents shall be accompanied with the Articles & Memorandum of Incorporation, vendor identification details and a completed Form M obtained from the Central Bank of Nigeria (CBN). The documentation required for the last category, Lawful Intercept Equipment, is similar to the first category.

In practice, the Nigeria Customs Service enforces compliance with the requirements for EUC for all imports involving any item on the ONSA's Control List. The effect of being included on the ONSA list is that the importer will be required to obtain an EUC from ONSA.¹⁰⁰ The essence of EUC is to ensure that the imported military equipment is not diverted to other uses unapproved by the ONSA. It must be presented before the controlled items can be cleared at the port of entry by the Nigeria Customs Service. In May 2024, Nigeria Customs Service confiscated 148 drones at the port of entry because EUC was not obtained for their import.¹⁰¹ The importers eventually abandoned the items. According to the news reports, one of the drones can be in the air for 72 hours consecutively and can be equipped with arms and ammunition.¹⁰²

3.1.2 NATIONAL OFFICE FOR TECHNOLOGY ACQUISITION AND PROMOTION (NOTAP) ACT:

This law requires that all contracts on the transfer of foreign technology to


99. Ibid.

100. [ADRN Surveillance Supply Chain Report Nigeria Country Report.pdf \(ids.ac.uk\)](#)

101. [Customs Hands Over Confiscated Fake US Dollars, 148 Drones To EFCC, Army \(leadership.ng\)](#)

102. Ibid.

Nigerian parties should be registered with NOTAP. The agency is mandated to ensure the acquisition of the best contractual terms and conditions relating to the transfer of foreign technology agreements and register all foreign technology transfer agreements having effect in Nigeria. Its guidelines include some "local content" requirements for software licensing contracts, in addition to other mandatory contract terms.¹⁰³ Technology Transfer Agreements involve the exchange of technology-related assets, knowledge, and skills between entities, usually from developed countries to developing ones like Nigeria.¹⁰⁴ NOTAP, as a coordinating agency in this regard, seeks to supervise and protect the interests of local and foreign entities engaged in technology acquisition.¹⁰⁵



The effect of being included on the ONSA list is that the importer will be required to obtain an EUC from ONSA. The essence of EUC is to ensure that the imported military equipment is not diverted to other uses unapproved by the ONSA. It must be presented before the controlled items can be cleared at the port of entry by the Nigeria Customs Service.

3.1.3 NIGERIA CUSTOMS SERVICE ACT, NO. 35 OF 2023:

The legal authority for management and administration of customs and excise¹⁰⁶ vests on the Nigeria Customs Service (NCS). The NCS acts on behalf of the

¹⁰³. International Comparative Legal Guide, "[Technology Laws and Regulations in Nigeria 2023-2024.](#)" Accessed – May 2024

¹⁰⁴. Bashir, Toyin et al. "[Regulator Spotlight - National Office For Technology Acquisition And Promotion \(NOTAP\)](#)". Banwo and Ighodalo. (2024)

¹⁰⁵. Ibid.

¹⁰⁶. 119.Ibid. Accessed May – 2024

Federal Government to certify the safety and quality standards of goods (technological and non-technological) imported into the country. The Act authorizes the NSC to prohibit the import of goods that can undermine national security and to maintain trade and economic balance in compliance with international agreements. Particularly, Section 30 of the Act requires NCS to examine and verify goods including technological items and their declaration data and the authenticity and existence of their documents; and obtain data from foreign customs administrations and governments, among other responsibilities.

3.1.4 FEDERAL MINISTRY OF INDUSTRY, TRADE AND INVESTMENT (FMITI):

FMTI formulates and implements policies and programs to attract investment, increase trade and exports, develop enterprises, and enhance industrialization. FMTI is mandated to facilitate trade in goods and services and maximize the benefits of foreign trade through bilateral and multilateral relationships with other countries.¹⁰⁷ It can be deduced that FMITI serves as a watchdog ensuring that the Federal Government's interests are safeguarded in foreign trade engagements.

3.1.5 NIGERIA COMMUNICATIONS COMMISSION:

Established in 2003 by the National Communications Commission (NCC) Act, the National Communication Commission (NCC) works to promote access to digital and telecommunication services in Nigeria. NCC licenses and registers telecom operators, selects players, sets price rates, and promotes service accessibility in the telecommunications sector. NCC also licenses the use of digital devices developed for social good and service delivery, and not for warfare.¹⁰⁸ This means that NCC's jurisdiction does not extend to the importation and regulation of surveillance technologies, but rather, the agency grants approval for devices and equipment with internet connectivity and microwave transmission. Devices used in Nigeria must pass electromagnetic compatibility tests.¹⁰⁹ Accordingly, importers of telecommunication equipment that serve dual-use purposes are to obtain an approval certificate or grant from the NCC as a precondition for the issuance of an EUC.

107. Federal Ministry of Trade and Investment, "[About FMITI](#)". Accessed May - 2024

108. Spaces for Change, Dialogue On Private Sector And Civic Space In Nigeria, July 7, 2023, <https://spacesforchange.org/dialogue-on-private-sector-and-civic-space-in-nigeria/>

109. Spaces for Change, *ibid*.

3.2 ARE ITEMS NOT INCLUDED IN ONSA LIST DEEMED TO BE EXCLUDED?:

As the above legal frameworks make clear, agencies and ministries mainly follow ONSA List of Controlled Importation. A cardinal principle of interpretation is that items not included on a list are deemed excluded.¹¹⁰ It therefore means that only the items contained on the ONSA list are controlled for importation. As such, the requirement for EUC does not apply to the importation of any surveillance technology that is not contained on the list. In this regard, three concerns are immediately apparent regarding the ONSA list:

- (i) the list of controlled surveillance equipment is quite lean compared to the massive array of surveillance equipment being offered across the world especially when the ONSA list is compared to other lists such as the Wassenaar Arrangement (which will be discussed later in this report).
- (ii) The focus of the ONSA list is on hardware. It does not contain any reference to computer programs, spyware, and know-how which from recent experience are more harmful to the civic space.
- (iii) As we have seen in Chapter Two, there is evidence of repurposing or diversion of surveillance technologies to violate human rights in Nigeria. Politicians have been accused of forging end-user certificate to acquire sophisticated spyware.¹¹¹ According to a report¹¹² Nigeria has invested extensively in surveillance technologies, and has used such security-grade surveillance technologies in targeting its citizens.¹¹³ These technologies include those used for internet interceptions, mobile interception, social media monitoring, city surveillance, and biometrics.¹¹⁴ As such, most of the harmful surveillance technology, especially those of a dual-use nature, may be freely imported into the country and put to any use, including targeting civic space actors.

110. Typified in the latin maxim: *expressio unius est exclusio alterius*.

111. *ibid*

112. [ADRN Surveillance Supply Chain Report Nigeria Country Report.pdf \(ids.ac.uk\)](#)


113. *Ibid.*

114. *Ibid.*

3.3 TYPOLOGIES OF EXPLOITATION OF EXCLUDED DUAL-USE TECHNOLOGIES:

A. Diversion by Non-security Agencies

The categories of persons and entities authorized to import DUTs, including spyware into the country, is broad, encompassing ministries, departments and agencies (MDAs), military and paramilitary organizations, embassies, private corporations and persons. The only exception is arms and ammunition which may only be imported by security agencies. An independent analysis of the massive budgetary outlay for the procurement of surveillance technologies¹¹⁵ revealed that many surveillance technologies available in the market are imported through MDAs that are not security-focused (for example, the Ministry of Education). More so, the absence of requirement for an EUC for all DUTs means that importation controls are relaxed while diversion, including to security agencies and criminal entities, is highly probable after importation. Diverted technologies can be applied to arbitrarily track and monitor citizens, or cause digital closures and harm to certain targets. Under this scenario, DUTs and other surveillance technologies imported exclusively for civilian purposes may be diverted to military and other repressive uses.



The categories of persons and entities authorized to import DUTs, including spyware into the country, is broad, encompassing ministries, departments and agencies (MDAs), military and paramilitary organizations, embassies, private corporations and persons. The only exception is arms and ammunition which may only be imported by security agencies.

115. Paradigm Initiative: Status of Surveillance in Nigeria: Refocusing the Search Beams, Policy Brief 009: <https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf>

B. Diversion by Private Companies

The principal import control for surveillance technologies in Nigeria is the requirement to procure EUC for items included on the ONSA List. Importers may procure these items by themselves or through a private contractor. Under this arrangement, it is possible for private companies and individuals to divert or transfer surveillance technologies imported for civilian purposes to other sectors for non-civilian use, thereby bypassing public scrutiny. A Carnegie report¹¹⁶ found that globally, private businesses lead the way in the **production and procurement of spy technologies, which they subsequently sell to the government. According to the report, governments purchase these capabilities directly from companies, which provide after-sales support, such as technical upgrades, product updates, trainings, and related customer services. The emergence of the commercial spyware sector has given a wide range of countries the means to acquire advanced surveillance tools they would otherwise struggle to obtain.**¹¹⁷

To demonstrate the likelihood of this scenario, a Premium Times report,¹¹⁸ in May 2014, reported that the CEO of an oil and gas company,¹¹⁹ wrote the CEO of Hacking Team demanding details of their hacking solution, stating that “as a company we will be interested in developing a partnership with your company, this will allow us represent, market, and introduce your stealth spyware solutions to our state intelligence agencies here in Nigeria”. It was later revealed in the chain of emails that company's client in Nigeria was the ONSA.

C. Cooperation Between the Government and Private Companies/Persons

Private persons have been known to participate in public surveillance in two broad ways – (a) as contractors of the government, (b) for own business purposes. The most glaring is Nigeria's US\$470 million CCTV project for the installation of CCTV nationwide by the Chinese company, ZTE.¹²⁰ The project was not operationalized. Almost a decade later, the government of Nigeria concessioned the project to a private company known as MPS Technologies Limited to operate the project and directed the National communications

116. [Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses - Carnegie Endowment for International Peace](#)

117. Ibid

118. [INVESTIGATION: Bayelsa Governor forges End User Certificate to procure N100M hacking tools | Premium Times Nigeria \(premiumtimesng.com\)](#)

119. Tunsmos Petroleum

120. [8 years after failed \\$470m CCTV project: Nigeria pays N40.05bn interest to ZTE - Blueprint Newspapers Limited](#)

Commission to issue the company a Universal Access Service License.¹²¹ According to local news reports, “determined to checkmate security challenges across the country, the Nigerian government has opted to farm out the operations of the \$490 million National Public Security and Communication System to a private company to operate on commercial basis.”¹²² This contract positions MPS Technologies Limited to control large swathes of private information about citizens. The company is in a position to import not only ONSA-controlled security-grade surveillance equipment, but numerous DUTs which are outside the scope of ONSA control.

S4C's report also found evidence showing that states collude with private actors—especially private telecommunication companies—to achieve their surveillance objectives.¹²³ In certain circumstances, collusion or cooperation to surveil between the state and private companies are imposed by statutes.¹²⁴ Fearing sanctions, companies can give subscribers' personal information upon request by law enforcement agencies. Smart phones can easily give off information about the users' location, the routes taken, the length of time spent on a call, logs of received and answered calls etc. Security agencies also exploit these vulnerabilities to aid their monitoring activities. Likewise, Nigerians – corporate or individual – can import uncontrolled surveillance technologies to surveil private citizens either for own purpose or for commercial purposes. These private outfits can bypass monitoring by ONSA through the importation and surveillance technologies that are not on the ONSA list.

D. Terrorists- and Insurgency-Induced Diversions

Nigeria is regarded as the largest importer of military equipment in sub-Saharan Africa, ostensibly in response to the Nigerian government's onslaught with Boko Haram and Islamic State West Africa Province (ISWAP), banditry and militancy.¹²⁵ This explains the dramatic increase in Nigeria's spending on arms “with weapons import climbing by a staggering 418% between 2022 and 2023.”¹²⁶ Nigerian military has lost a considerable amount of these weapons during armed confrontation with non-state armed fighters. Reporting suggests that

121. [Insecurity: FG concedes \\$490 m CCTV Project - Police Affairs Minister \(vanguardngr.com\)](#)

122. Ibid

123. Victoria Ibezim-Ohaeri et al, Action Group on Free Civic Space "Security Playbook of Digital Authoritarianism". (2021).

124. See sections 146 – 149 of the Nigerian Communications Act 2003

125. [Nigeria Military Equipment 2021 - Grey Dynamics Intelligence Series](#)

126. [Nigeria spends 418% more buying foreign weapons in 2023 - Nairametrics](#)

Boko Haram factions in Nigeria have seized contingent-owned equipment (COE) that includes a wide-range of heavy weapon systems, among which are those that originate from EU member states.¹²⁶ Terror groups have also raided military bases killing soldiers¹²⁷ and made off with weapons belonging to peacekeeping missions and militaries,¹²⁸ setting the military back in their fight against the jihadists. Beyond Nigeria, the diversion of contingent-owned equipment (COE)—that is, government-owned materiel—from the four Lake Chad Basin countries participating in and alongside the Multinational Joint Task Force (MNJTF) has occurred on a level unprecedented on the African continent.¹²⁹

According to the United Nations Office of Counterterrorism, the diversion of weaponry is another significant problem in different parts of the world. Access to diverted weapons and ammunition considerably increases the kinetic capacity of terrorists and other armed groups.¹³⁰ Diversion may occur as a result of uncontrolled transfer, unauthorized re-transfer, theft, hand-outs to armed groups, or barter involving natural resources.¹³¹ This situation of military equipment losses represents a shortcoming that equally applies to DUTs imported for non-civilian uses. The danger here is the very high likelihood of terrorists taking away and diverting surveillance equipment imported for military uses to outright terrorist activities, causing massive harm to civilian populations. The likelihood is so high that a terrorist group like Boko Haram has been able to sustain its operations for more than ten years without being resupplied externally, as occurs in most insurgencies.¹³² To make matters worse, this operational shortcoming is not unique to Nigeria where corrupt procurement practices have been documented, but also take place in other MNJTF troop-contributing countries.¹³³

3.4 OTHER WAYS DUAL-USE TECHNOLOGIES CAN BE ABUSED:

1. Weapons Development

DUT can be abused by using it for weapon development, especially by criminal

126. Ibid

127. BBC, Nigeria Metele attack: President Buhari speaks of deep shock, November 25, 2018, <https://www.bbc.com/news/world-africa-46333126>

128. James Reinl, World Post, How stolen weapons keep groups like Boko Haram in business, April 19, 2019, <https://theworld.org/stories/2019/04/19/how-stolen-weapons-keep-groups-boko-haram-business>

129. Council on Foreign Relations, Boko Haram Capture of Military Equipment Fuels Lake Chad Insurgency

130. United Nations Office of Counter Terrorism Centre, "[Preventing Terrorists from Acquiring Weapons](#)". Accessed – June 2024

131. Ibid.

132. James Reinl, IPIS, *ibid.*

133. James Reinl, IPIS, *ibid.*



groups such as terrorist groups. It has been reported that terrorist groups have innovated a new way of carrying out their attacks – weaponized drones. Terrorist groups such as Boko Haram, ISWAP, Al-Qaeda, the Taliban, Houthis, Jaysh Al-Fath, Hezbollah, Hamas, and ISIS are some of the groups that have used and continue to weaponize drones dangerously.¹³⁴ Being easy to buy, easy to modify depending on the purpose for which they are intended to be used, easy to handle and difficult to detect, in the wrong hands, could become feared weapons that threaten people's lives.¹³⁵

2. Biological and Chemical Weapons:

Fertilizers for agricultural use has often been misused by terrorist groups operating in parts of Nigeria to make bombs and other explosives, causing security operatives to place a hold on its distribution.¹³⁶ The use of biotechnology ¹³⁷ intended for medical research, such as “clustered regularly interspaced short palindromic repeats (CRISPR) gene-editing technology, can be misused to create biological weapons. CRISPR is a technology that researchers and scientists use to selectively modify the DNA of living organisms.¹³⁸

134. Mihaiela BUSE, 2019. [“Drones and Terrorism - A New Threat to International Security,” Proceedings of the 11th International Conference on Knowledge Management: Projects, Systems and Technologies, Bucharest, November 7-8, 2019.](#) Accessed June 4, 2024.

135. Ibid

136. Premium Times, [How Boko Haram caused fertiliser scarcity, price increase – Nigerian Govt, December 20, 2016.](#) <https://www.premiumtimesng.com/news/top-news/218530-boko-haram-caused-fertiliser-scarcity-price-increase-nigerian-govt.html?tztc=1>

137. According to the [Norwegian University of Science and Technology](#) (NUST), biotechnology is a technology that utilizes biological systems, living organisms, or parts of them to develop or create different products.

138. [National Human Genome Research Institute, Definition of CRISPR](#) (2024). Accessed June 4, 2024

3. Cyber-attacks and Warfare:

Cybersecurity technologies help protect critical infrastructure, financial systems and personal information from cyber-attacks. However, the same tools can also be repurposed for offensive purposes or adapted for offensive operations. Cyber-attacks on critical infrastructure, like power grids or transportation systems, can have devastating consequences. Hackers can disrupt operations, cause widespread outages, and even endanger lives. Cyber warfare can also involve stealing sensitive data, such as intellectual property, government secrets, or personal information. News reports have disclosed how bank customers and companies lose billions to Nigeria's weak cybersecurity causing unauthorized access to sensitive data, such as passwords, credit card details and personal user information.¹³⁹ Universities across Nigeria have had cyber-attacks like ransomware and data breaches, leading to the unlawful exposure, loss of sensitive information and pornographic displays on their websites.¹⁴⁰

3.5 OPPORTUNITIES FOR INCREASING REGULATORY OVERSIGHT ON THE IMPORTATION OF DUAL-USE TECHNOLOGIES IN NIGERIA:

As seen in the previous chapters, DUTs - like telecommunication equipment - are subjected to greater scrutiny than all other categories of technologies ostensibly because they are applied toward dual-use purposes by a wide range of actors. Despite this extra control measure, many DUTs are excluded from ONSA's control lists, leaving an evident gap in regulation that could be potentially exploited. How can these gaps be closed? There are legal provisions and principles that offer important levers for expanding the application of current ONSA regulation to excluded DUTs in Nigeria:

A. The Catch-All Provision in ONSA List

In addition to items specifically listed on the ONSA list, ONSA will require an importer to obtain an EUC in respect of any item for which an end-user certificate is required by the exporting country.¹⁴¹ For example, China generally requires exporters of DUTs to submit the end-use certificate provided by the end-user, and for exports considered risky. The exporter is required to submit the name of the end-user and end-use certificates verified or issued by the government agencies of the country or region in which the end-user is located. Therefore, the

139. The Punch, Bank customers, companies lose billions to Nigeria's weak cybersecurity, April 2, 2023

140. The Punch, *ibid*.

141. [General Guidelines End-User Certificate Portal \(nsa.gov.ng\)](https://nsa.gov.ng)

catch-all provision in the ONSA list bolsters the scope of the ONSA EUC regime by recognizing the EUC requirements of foreign countries. Thus, to import surveillance technology from China for which the Chinese regulation demands EUC, the importer must approach ONSA for an EUC.

B. Case-by-Case Determinations

Another entry-point is that the power reserved on the ONSA to require EUC for “other items as could be specifically determined.”¹⁴² This suggests that ONSA may determine on a case-by-case basis that the importation of a particular item would require an EUC. At the port of entry, the Nigeria Customs Service may determine that based on the nature of the item being imported, an EUC will be required to clear the item from the port.¹⁴³ This will compel the importer to approach the ONSA for the EUC. It has been the practice by the NCS to demand EUC for items that are not on the ONSA list, and this has frustrated importers.¹⁴⁴ Some importers who resisted the request for EUC incurred higher demurrage bills due to the delays at the port.¹⁴⁵

NCS's practice of demanding for EUC for imports of sensitive nature is reflected in NCS's public statements. In a statement, a high-ranking official of NCS made a blanket declaration that “importers of drones in the country [must] obtain the End-User-Certificate (EUC) before importing them for security reasons.”¹⁴⁶ In other words, drones are not allowed into the country without EUC. This liberal interpretation of the EUC requirement by NCS has resulted in seizures and detention of imports of surveillance technologies, hence increasing the level of oversight over importation of surveillance technologies.

C. The Nigerian Proliferation Financing Regulation

Banks can play an important role in limiting arbitrary importation of DUTs. Nigeria has obligations under international law to counteract proliferation financing to ensure that the Nigerian banking system is not used to finance trade in controlled items. These obligations are reflected in the Terrorism (Prevention and Prohibition) Act, 2022 and guidelines issued by the Central Bank of Nigeria,¹⁴⁷ and the inherent risk assessment conducted by the Nigerian Financial Intelligence Unit.¹⁴⁸

142. Ibid.

143. [Customs Intercepts Combat-Ready Drone, Military Hardware At MMIA \(leadership.ng\)](#)

144. [Manufacturers, Importers Groan over Customs End User Certificate Abuse - THISDAYLIVE](#)

145. Ibid.

146. [Drones not allowed without End-User-Certificate MMIA Customs boss PortNews](#)

147. [AML CIRCULAR AND REGULATIONS MERGED.pdf \(cbn.gov.ng\)](#)

148. [DownloadFile \(nfiu.gov.ng\)](#)



The Central Bank of Nigeria defines PF as “the act of raising funds, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of Proliferation of Weapons of Mass Destruction (WMD), including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods used for non-legitimate purposes)”.¹⁴⁹ This means that PF is concerned with the trade in the following:

- (i) weapons of mass destruction,
- (ii) materials required for the delivery of weapons of mass destruction, and
- (iii) dual-use technologies and dual-use goods used for non-legitimate purposes.

Although the ONSA list contains items that qualify as DUTs, it does not use the term “dual use” to describe them. It means that there is no deliberate directory of items listing DUTs in use in Nigeria. The absence of a clear definition and list of DUTs not only presents a compliance challenge, but also vests broad discretionary powers on both customs and law enforcement agencies. While such broad discretion may be prone to abuse, it still creates an additional layer

149. [TFS PROLIFERATION FINANCING.pdf \(cbn.gov.ng\)](#)

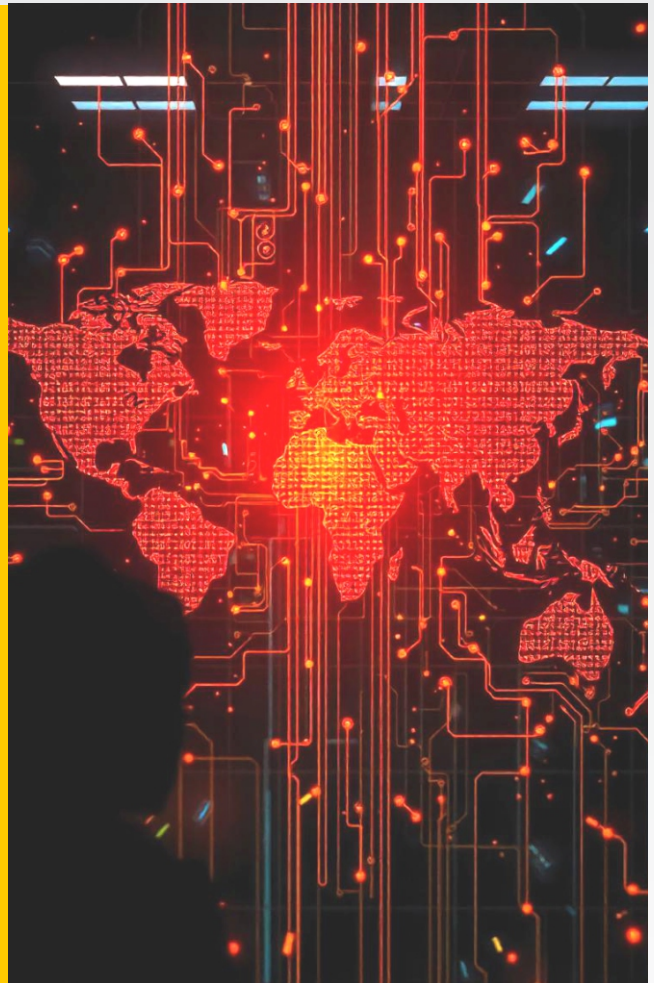


of oversight, especially for independent entities like banks to undertake stringent due diligence regarding payments for the importation of DUTs.¹⁵⁰ This includes filing reports to regulatory bodies responsible for enforcing anti-money laundering, countering financing of terrorism and combating weapon proliferation regimes in the country. However, the extension of anti-terrorism financing regulations to DUTs must take humanitarian exemptions into account, thereby making special exceptions or considerations for importation by humanitarian aid and development groups who legitimately use drones in their charitable operations.

150. See Central Bank of Nigeria (Customer Due Diligence) Regulations, 2023. This Regulation defines “Proliferation Financing (PF)” as the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations, etc.

CHAPTER

4




**EXPORT CONTROL
REGIMES FOR
DUAL-USE
TECHNOLOGIES**

The preceding chapter shed light on the import controls for dual-use technologies (DUTs), especially those with surveillance capabilities in Nigeria, highlighting the strengths and the gaps in regulation, and the opportunities for reform. So, how do suppliers of surveillance technologies regulate their products for export? In the fight against the proliferation of surveillance technologies in Nigeria, engaging with suppliers and their host countries might be a potent weapon. This chapter will examine the export control regimes in the Nigeria's three major supplier countries, the existing common control lists in the international arena, the export control system of dual-use products, and how it affects Nigeria in the global digital surveillance market. The analysis will mainly focus on Nigeria's major suppliers—China, Israel and the United States—to deepen understanding of the export control regimes applicable to the spywares and dual-use technologies, particularly analyzing these three countries' export authorizations, quantitative limitations and end-use requirements.

Export controls have been established over the past decades in the context of regimes and treaties in order to prevent or, decelerate the diffusion of items (i.e., materials, technologies, components, equipment, but also software) that could be misused in nuclear, chemical, biological, and cyber-driven weapons. The core objective is to detect and preempt accidental or purposeful illicit procurement or trafficking of such items, by assessing the risk of misuse, assessing the track record of the importer, and by interfering in the link between exporter and importer.¹⁵¹ Along this line, export controls in the European Union take into account the “EU and its Member States' international obligations, including UN Security Council Resolution 1540; the Nuclear Non-Proliferation Treaty; the Chemical Weapons Convention; and the Biological Weapons Convention.”¹⁵² These regimes exist to complement the United Nations Resolutions for arms control. For example, UN Resolution 1540 “calls upon all States to take and enforce effective measures to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including related materials, equipment, and technology covered by relevant multilateral treaties and arrangements.” It prohibits nations from supplying weapons to non-state actors, especially terrorist organizations.

151. German Council on Foreign Relations: [Anticipatory governance of emerging and disruptive technologies with dual-use potential | DGAP](#)

152. [Exporting dual-use items - European Commission \(europa.eu\)](#)



Export controls have been established over the past decades in the context of regimes and treaties in order to prevent or, decelerate the diffusion of items (i.e., materials, technologies, components, equipment, but also software) that could be misused in nuclear, chemical, biological, and cyber-driven weapons. The core objective is to detect and preempt accidental or purposeful illicit procurement or trafficking of such items, by assessing the risk of misuse, assessing the track record of the importer, and by interfering in the link between exporter and importer.




4.1 DUT PRODUCTION TRENDS IN MAJOR SUPPLY COUNTRIES:

Trends in technologically-advanced countries indicate a conscious drive toward growing their national DUT capabilities and inventories ultimately for military uses in the long-term. From a military strategic standpoint, DUTs require a short lead time to be converted into military technologies. They are half-done military or security hardware and software. Revealing this trend, Israel's defence ministry has recognized "the need to support smaller startup companies, especially those making dual-use technology that can be used for civil or defense applications."¹⁵³ As an official confirmed, "Israel Defense Forces need quick answers to their problems, so time-to-market must be fast. We are in huge competition with commercial market because start-ups look to civilian market.

153. [How Israel's military is prioritizing dual-use start-ups to accelerate defense tech - Breaking Defense](#)

So, we want to transform commercial capabilities to defense R&D.”¹⁵⁴

Israel also entered into a bilateral agreement with India to “promote innovation in startups and MSMEs of both countries for development of dual use technologies.”¹⁵⁵ Under the agreement, both countries will work together to bring out next generation technologies and products in the areas such as Drones, Robotics, Artificial Intelligence, Quantum technology, Photonics, Biosensing, Brain-Machine Interface, Energy Storage, Wearable Devices, and Natural Language Processing.¹⁵⁶ Like Israel, China has also been reported to be purposefully pursuing advanced DUTs in its quest to be, not only a global 'science and tech superpower', but also to build a strong military that can fight and win wars.¹⁵⁷ Therefore, you can expect exponential developments in DUTs, except that the key driver might be the non-civilian use of such technologies. The table below shows how technology production is increasingly becoming an instrument of economic and industrial dominance among major powers.

COUNTRY	USA 	ISRAEL 	CHINA 
Dominant Surveillance tech export	Social media surveillance and political marketing	Malware	Public space surveillance
Notable companies	Facebook, Google, Twitter	NSO Group, Cellebrite, Cytox, and Candiru	Huawei, ZTE, C.E.I.E.C., Hikvision

154. Ibid.

155. pib.gov.in/PressReleaseFramePage.aspx?PRID=1770299

156. Ibid.

157. [Chinas pursuit of dual-use technologies \(iiss.org\)](http://Chinas%20pursuit%20of%20dual-use%20technologies%20(iiss.org))

COUNTRY	USA 	ISRAEL 	CHINA 
Export Control regulator	The U.S. Department of Commerce's Bureau of Industry and Security (BIS)	The Export Control Agency of the Ministry of Economy and Industry	The Ministry of Commerce (MOFCOM), the Chinese Customs Bureau and the State Council and Central Military Commission
Export Control Rules	Export Administration Regulations, Commercial Control List, Wassenaar Arrangement's List of Dual Use Goods and Technologies	Wassenaar Arrangement's List of Dual Use Goods and Technologies, The Defense Export Controls Act	Export Control Law 2020, Dual Use Items List, Regulations for the Administration of the Import and Export of Technology, Administrative List of Export of Military Products
Regulatory priority	National security, foreign policy, economic objectives	Export driven, national security, foreign policy	Protectionist, state interest

COUNTRY	USA 	ISRAEL 	CHINA 
Control	Export licence	Export licence	Export licence, end-use and end-user certificates
Responsiveness to public outcry	Fairly responsive	Not responsive	Not responsive

African states, including Nigeria are spending over \$1bn per year on digital surveillance technologies imported from countries like the U.S., Britain, China etc.¹⁵⁸ While the USA and the UK dominate the provision of social media surveillance and 'political marketing' consultancy to manipulate voter beliefs and behaviour, other countries like Germany, Italy, and Israel are the major exporters of mobile phone hacking malware. Chinese companies dominate public space surveillance via safe city surveillance systems.”¹⁵⁹

4.2 EXPORT CONTROL REGIMES FOR DUAL-USE TECHNOLOGIES IN NIGERIA'S MAJOR SUPPLIER COUNTRIES:

The governments of Israel, China, and the United States, adhere to specific export regimes with distinct obligations for suppliers and importers. Below is an overview of the regimes applicable to these countries and their related obligations:

4.2.1 ISRAEL'S EXPORT CONTROL REGIME:

Israel maintains a robust export control system for dual-use technology, aiming

158. Roberts, T. et al. (2023) Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2023.027
 159. [African nations spending \\$1bn a year on harmful surveillance - Institute of Development Studies \(ids.ac.uk\)](https://ids.ac.uk)

to prevent the proliferation of sensitive items while fostering legitimate trade. Israel has two main export control regimes, a civilian regime administered by the Israeli Ministry of Economy and Industry (MOE) and a defense regime administered by the country's Ministry of Defense,¹⁶⁰ specifically the Defense Export Controls Agency (DECA). The Export Control Agency of the Ministry of Economy and Industry administers and enforces controls over dual use, nuclear, chemical, and biological exports aiming to promote the national security of the State of Israel as well as regional and international stability.¹⁶¹ On the other hand, DECA, under the **Ministry of Defense (MoD)** is responsible for exports of defense equipment and dual-use items designed for military purposes or military end-users.

Israel's Defense Export Control Law (DECL) 2007 lays the foundation for Israel's export control system, specifically focusing on defense-related products, services, equipment, information and dual-use items with potential military applications.¹⁶² DECL Law regulates export of defense equipment, the transfer of defense know-how and the provision of defense services, for reasons of national security considerations, foreign relations considerations, international obligations and other vital interests of the State.¹⁶³ It defines specific categories of items subject to export controls, including dual-use goods that could be used for both civilian and military purposes. All defense exports require licenses from DECA, with several types of licenses depending on the nature of the export, such as marketing, export, and transit licenses.¹⁶⁴ The MOD evaluates applications based on criteria such as national security, foreign policy, international obligations, and human rights considerations.

Israel's Dual-Use Technology Export Control Procedures:

a. Licensing Requirements: Companies exporting dual-use technology must obtain licenses from the appropriate authority (MOE or MoD) depending on the intended use and end-user. Exporters must submit detailed applications, including information about the items, end-users, and end-use.¹⁶⁵

b. End-User and End-Use Verification: Rigorous verification procedures are in place to ensure the legitimacy of the recipient and the intended civilian use of the technology. This might involve documentation, site visits, and cooperation with

160. Herzog Fox & Neeman, "Israel's Civilian Dual-Use Export Control List for 2021". Lexology. (2021).

161. Dual Use Export Control, [The Export Control Agency of the Ministry of Economy and Industry](#) (2023)

162. [Defense Export Control Law \(2007\) of Israel](#). Accessed June 6, 2024

163. Section 1 of the [Defense Export Control Law \(2007\) of Israel](#).

164. Chapter D, Sections 16 - 22, of the [Defense Export Control Law \(2007\) of Israel](#).

165. Section 6(b)(1), the [Defense Export Control Law \(2007\) of Israel](#).

foreign customs authorities. Exporters must provide certifications that verify the end-use and end-user of the exported items to ensure that they are not diverted to unauthorized users or for unauthorized uses,¹⁶⁶

c. Post-Shipment Verification: In some cases, there might be requirements for verifying that the technology has reached the declared end-user,¹⁶⁷ including maintaining a detailed records (for a minimum of ten years) of their transactions and make them available for inspection.¹⁶⁸ This includes information on the nature of the items, the quantity, the value, the identity of the buyers, and the delivery dates.¹⁶⁹

d. Periodic Reporting: Suppliers are required to submit periodic reports to the DECA which details their export activities. These reports ensure that the DECA has up-to-date information on the flow of dual-use technologies and can monitor compliance effectively.¹⁷⁰

e. Availability for Inspection: Suppliers must make their records available for inspection by DECA officials. This ensures that the authorities can verify compliance with export control regulations and investigate any potential violations.

f. Compliance Audits: DECA conducts compliance audits to ensure that suppliers adhere to the reporting requirements and other provisions of the law. Failure to comply with these requirements can result in severe penalties, including fines, imprisonment, and revocation of export licenses.

g. Record Keeping: An export license holder is mandated under the DECL to keep a record concerning any defense export transactions that he/she has conducted. The record shall include the following details:

- (i) the licensed defense equipment;
- (ii) the defense know-how or defense service;
- (iii) the interim users and the end user;
- (iv) the end-use of the licensed defense equipment;
- (v) the dates when the defense export was carried out and additional details as shall be set forth in the regulations.

166. Ibid


167. Ibid

168. Ibid

169. Section 36 of the [Defense Export Control Law \(2007\) of Israel](#).

170. Section 28 of the [Defense Export Control Law \(2007\) of Israel](#).

The most significant difference between Nigeria's EUC certification and Israel's licensing regime is the requirement of reporting deployment and actual usage of the technology. Suppliers of dual-use technology under the Israel Defense Export Control Law (2007) must adhere to rigorous reporting requirements, including detailed applications, end-use and end-user certifications, maintaining transaction records, periodic reporting, making records available for inspection, and compliance audits. These measures are designed to ensure that dual-use technologies are exported responsibly and do not compromise national or international security.



Suppliers of dual-use technology under the Israel Defense Export Control Law (2007) must adhere to rigorous reporting requirements, including detailed applications, end-use and end-user certifications, maintaining transaction records, periodic reporting, making records available for inspection, and compliance audits. These measures are designed to ensure that dual-use technologies are exported responsibly and do not compromise national or international security.

4.2.2 EXPORT CONTROL REGIME IN THE PEOPLE'S REPUBLIC OF CHINA:

China has established a comprehensive export control system to regulate dual-use technologies for the purpose of building an export control system that is commensurate with its international standing and aligned with its national security and interests. As mentioned in its white paper on dual use technology control, China, a major player in the international export and manufacturing of

DUTs, has put in place rules, policies, and practices, including signing several international agreements and treaties to control the export and limit the potential abuse of dual use technologies.¹⁷¹

The primary legislation on dual-use technology in China is the Export Control Law (2020). Enacted in December 2020, China's Export Control Law (ECL) is the first of its export control framework governing dual-use items, military products, nuclear materials, and other goods, technologies, and services related to national security. Divided into five (5) chapters and 49 articles, the ECL makes explicit provisions regarding international cooperation, systems, and measures related to dual-use technology export controls. It also establishes a basic institutional framework and unified rules for export control policies, including a control list, temporary controls, a restricted name list, and supervision.¹⁷² The ECL was developed with changing circumstances in mind, as noted in its white paper, published in 2021 (a year after the enactment of the ECL), incorporating standard international practices as well as China's own export control experience. It establishes a comprehensive framework for China's export control system, strengthens the country's export laws, and covers all relevant aspects of export control, including requirements, conditions, and penalties for export licensing of controlled items especially dual-use technologies. It is noteworthy that the ECL does not explicitly repeal other existing laws and regulations on dual use items such as the 2007 Regulation on nuclear dual-use items. Rather, the ECL ensures that all aspects of export control, including those specific to nuclear dual-use technologies, are managed under a unified, stringent, and internationally aligned system.¹⁷³

Licensing Procedure and Obligation of Exporters Under China's Export Control Law:

1. Export Control Authorities: The departments of the State Council and the Central Military Commission undertake export control functions (also known as the state export control authorities.¹⁷⁴ The state export control authorities are responsible for formulating and implementing unified rules for export control, formulating control lists, schedules, and catalogs (hereinafter collectively referred to as "the control list"), and practicing export licensing, among others,¹⁷⁵ and developing policies¹⁷⁶ for items which export licenses will be

171. [China's Export Controls \(2021\)](#). Accessed June 12, 2024

172. [China's Export Controls \(2021\)](#). Accessed June 12, 2024

173. [China's Export Controls \(2021\)](#). Accessed June 12, 2024

174. Article 5 ECL

175. Article 4 ECL

176. Article 8 ECL

required. The enforcement authorities can designate items that are not on the list of controlled items as a "temporarily controlled item" for two years, which can be lifted or extended at the end of the two years.¹⁷⁷

From the above, dual-use items (goods) in China are administered and regulated by either the State Council or the Central Military Commission (CMC) departments, depending on the category they fall into. The ECL also requires state export control authorities to review an exporter's application for exporting a controlled item to decide whether or not to grant an approval, by taking into full consideration the following factors:¹⁷⁸

- (a) National security and interest;
- (b) International obligations and commitments;
- (c) The type of export;
- (d) The sensitivity of the controlled item;
- (e) Destination country or region of the export;
- (f) The end user and end use of the exported item;
- (g) The relevant credit records of the applicant exporter; and
- (h) Other factors set forth by laws and administrative regulations.

2. End-User and End-Use Verification: End-User and End-Use Verification: The Chinese authorities require exporters to verify the end-use and end-users of dual-use items. As a check against abuse and diversion of dual use technologies, exporters are required to submit to the state export control authorities information about the end-user and end-use, which shall be issued by the end-user or the relevant government agency of the country or region where the end-user is located.¹⁷⁹ Furthermore, exporters are mandated to undertake not to change the end-use of the relevant controlled item or transfer it to any third party without consent of the state export control authorities, notifying the state export control authorities about any change in the end-use or end-user of the item without delay.¹⁸⁰

177. Article 9 (2) ECL

178. Article 13 ECL

179. Article 15 of ECL

180. Article 16 ECL



The Chinese authorities require exporters to verify the end-use and end-users of dual-use items. As a check against abuse and diversion of dual use technologies, exporters are required to submit to the state export control authorities information about the end-user and end-use, which shall be issued by the end-user or the relevant government agency of the country or region where the end-user is located.

3. Application for Dual Use Export: Article 21 of the ECL provides for the exportation of dual use items and such application are subject to the provision of applicable laws and administrative regulations, e.g. Regulations of the People's Republic of China on the Control of Nuclear Dual-use Items and Related Technologies Export, etc., The state's export control authorities are responsible for the reception, approval or disapproval of applications for the export of dual-use items, within the statutory time period after reviewing the applications either independently or in conjunction with the relevant departments in accordance with this Law and other relevant laws and administrative regulations.¹⁸¹

181. Article 22 of ECL

4. Embargo on Export of DUTs: The ECL contains provisions that prohibit the export of any relevant controlled items to any specified country, region, organization, or individual. ^{182&183} The state export control authorities conduct risk assessments of countries and regions to identify the risk and apply corresponding control measures.¹⁸⁴ They also maintain the list of importers and end-users who fall under any of the following circumstances – violating the end-user and end-use management requirements; may threaten or endanger national security or interest; or using any controlled item for terrorism.¹⁸⁵ Furthermore, the ECL prohibits exporters from trading with any importer or end user on the control list.¹⁸⁶

5. Inspections and Audits: Chinese authorities conduct inspections and audits to ensure compliance with export control regulations.¹⁸⁷ Exporters must cooperate with these inspections and provide necessary documentation.

6. Penalties: The ECL makes provisions for penalties for contravention of its provisions which are captured in Chapter IV (Articles 33-44) of the ECL, also known as legal penalties. Penalties range from fines, imprisonment, revocation of export license, etc. For instance, exporting controlled items without a license or beyond the scope of the license, the ECL imposes fines ranging from five to ten times the value of the illegal business. ^{188 189} Fines are also imposed for refusing or obstructing inspections.¹⁹⁰



¹⁸². Bingna Guo and James Hsiao, [White and Case, China Enacts Export Control Law Following Its Announcement of the Unreliable Entities List](#) (January 15, 2021)

¹⁸³. Article 8 ECL

¹⁸⁴. Ibid; Bingna Guo and James Hsiao (2021)

¹⁸⁵. Article 18

¹⁸⁶. Article 18 (2) ECL

¹⁸⁷. Article 17 ECL

¹⁸⁸. Article 33 of the ECL

¹⁸⁹. Bingna Guo and James Hsiao, *ibid* (2021)

¹⁹⁰. *Ibid*.

Other Laws and Regulations on Export Control in China:

Since the 1990s, China has promulgated six administrative regulations on dual-use goods (technologies), they are:

- (a) Regulations of the People's Republic of China on the Administration of the Controlled Chemicals
- (b) Regulations of the People's Republic of China on the Control of Nuclear Export
- (c) Regulations of the People's Republic of China on Administration of Arms Export,
- (d) Regulations of the People's Republic of China on the Control of Nuclear Dual-use Items and Related Technologies Export
- (e) Regulations of the People's Republic of China on Export Control of Missiles and Missile-related Items and Technologies, and
- (f) Regulations of the People's Republic of China on Export Control of Dual-use Biological Agents and Related Equipment and Technologies.

Each of these regulations seeks to ensure effective controls for the exportation of items on the controlled list, especially dual-use items, including spyware.¹⁹¹ The Ministry of Commerce (MOFCOM) plays a central role in the export control of dual-use technologies, but it operates within a broader framework of state export control authorities.¹⁹² These authorities collectively ensure comprehensive oversight and compliance with national and international export control regulations. While MOFCOM serves as the primary licensing authority for dual-use technologies, it works in close collaboration with other state export control authorities as highlighted in the table above. MOFCOM handles the overall licensing process, policy formulation, and enforcement, while specialized state authorities provide technical assessments, regulatory oversight, and support within their respective domains. This coordinated approach ensures a comprehensive and effective export control system for dual-use technologies in China.

191. Ibid.

192. Mission, [Ministry of Commerce People's Republic of China \(MOFCOM\)](#), Accessed June 16, 2024

4.2.3 EXPORT CONTROL REGIMES IN THE UNITED STATES OF AMERICA (USA):

The U.S. Bureau of Industry and Security (BIS) under the Department of Commerce is charged with developing, implementing, and interpreting the country's export control policy for dual-use commodities, software, and technology.¹⁹³ Dual-use products under BIS regulatory jurisdiction have predominantly commercial uses and may have military applications.¹⁹⁴ The accurate, consistent, and prompt review and processing of licenses for proposed exports and reexports of products and technology from the United States is one of BIS's main goals.¹⁹⁵ The goal of BIS is to safeguard American economic, foreign policy, and national security interests without placing unnecessary regulatory barriers on lawful international trade.¹⁹⁶

U.S. control lists are consistent with the lists maintained by the various multinational export control regimes. They are, however, augmented by unilateral controls when necessary to ensure national security and foreign policy imperatives.¹⁹⁷ The three major lists of export-controlled items are the Commerce Control List (CCL), the United States Munitions List (USML), and the Nuclear Regulatory Commission Controls (NRCC).

The U.S. Munitions List regulates defense-related articles and services. A service or article may be classified as defense-related if it has been produced, configured, altered, or modified especially for military use and hasn't been primarily used for civil purposes, or lacks performance that is comparable to that of a good or service used in civil applications ... and requires control due to its substantial military or intelligence applicability.¹⁹⁸



Source: Govima Media

193. Bureau of Industry and Security, ["Policy Guidance"](#). (2024)

194. Ibid.

195. Bureau of Industry and Security, ["Licensing"](#). (2024)

196. Ibid.

197. State Government, ["Overview of US Export Control System"](#). Accessed June - 2024

198. Ibid.

The U.S. government controls the export of sensitive equipment, software, and technology as a means to promote its national security interests and foreign policy objectives.¹⁹⁹ Through its export control system, the U.S. government can effectively provide for national security by limiting access to the most sensitive U.S. technology and weapons; promoting regional stability; taking into account human rights considerations; preventing proliferation of weapons and technologies, including weapons of mass destruction to problem end-users and supporters of international terrorism; and complying with international commitments, i.e. non-proliferation regimes, UN Security Council sanctions and UNSC resolution 1540.²⁰⁰

The USA leads advocacy for the regulation and enforcement of export controls on DUTs. The United States is also a member of several export control regimes in force globally and played a pioneering role in developing some global security initiatives relating to counter-terrorism, non-proliferation, and proportionate deployment of military accessories and dual-use products. Some of these regimes are examined below:

4.3 INTERNATIONAL EXPORT CONTROL ARRANGEMENTS FOR DUAL-USE TECHNOLOGIES:

It is important to acknowledge that it is impossible to provide an exhaustive list of dual-use technologies because technology is in perpetual evolution. Consequently, it is the responsibility of governments to develop a list of technologies qualifying as DUTs. The implication is that what constitutes DUTs will vary from country to country. National human rights, national security and strategic policies may also contract or expand the list of recognized DUTs. However, there have been efforts among countries to cooperate in harmonizing DUT designations and categorizations. Here are some examples below:

A. Wassenaar Arrangement

The most popular global endeavor to harmonize export control is the “Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies” of 1995 which has been updated several times with the most recent iteration being in 2023.²⁰¹ The Wassenaar Arrangement is established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of

199. [Overview of U.S. Export Control System, Strategic Trade Management and Export Controls 2009-2017](#) (2011)

200. Ibid.

201. [Home - The Wassenaar Arrangement](#)

conventional arms and dual-use goods and technologies, thereby preventing destabilizing accumulations, which also aim to prevent the acquisition of these items by terrorists.²⁰²

There are 42 participants in the Wassenaar Arrangement including France, Russia, the United Kingdom, and the United States, but excluding other notable technological and military powers such as China and Israel. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.²⁰³ Although Israel²⁰⁴ and China²⁰⁵ are not members of the Wassenaar Arrangement (WA), their export control policies are aligned with the principles of the Wassenaar Arrangement by adopting the WA list of dual-use items subject to control.

B. Missile Technology Control Regime (MTCR)

Israel is not a formal member but voluntarily adheres to the regime's guidelines, controlling the export of missile and unmanned aerial vehicle (UAV) technology capable of delivering Chemical, Biological and Nuclear (CBN) weapons, and establishes controls on exports of dual-use missile technologies.²⁰⁶ The MTCR is an informal political understanding among states that seek to limit the proliferation of missiles and missile technology,²⁰⁷ formed in 1987 by the G-7 industrialized countries (Canada, France, Germany, Italy, Japan, the UK, and the United States) following secret negotiations from 1983.²⁰⁸ The MTCR was initiated by like-minded countries to address the increasing proliferation of nuclear weapons by addressing the most destabilizing delivery system for such weapons.²⁰⁹ In 1992, the MTCR's original focus on missiles for nuclear weapons delivery was extended to a focus on the proliferation of missiles for the delivery of all types of weapons of mass destruction (WMD), i.e., nuclear, chemical and biological weapons. Such proliferation has been identified as a threat to international peace and security.²¹⁰ China is not a member of the Missile Technology Control Regime (MTCR), but has applied for membership and pledged

202. [the Wassenaar Arrangement](#)

203. Ibid.

204. Privacy Shield Framework, [Israel-US Export Control](#). Accessed June 5, 2024

205. Article 1, ECL

206. kolja Brockmann et al, [the Missile Technology Control Regime at a Crossroads. \(2022\); Bureau of Industry and Security. Israel-US Export Control. \(2024\)](#). Accessed June 5, 2024

207. Ibid.

208. kolja Brockmann et al, [the Missile Technology Control Regime at a Crossroads. \(2022\)](#)

209. Ibid.

210. Ibid.

to abide by its main control mechanisms.²¹¹ China has expressed its support for the objectives of the MTCR and has committed to controlling the export of missile-related technology and equipment to prevent their proliferation.²¹²

C. Nuclear Suppliers Group (NSG)

Founded in 1974, the Nuclear Suppliers Group (NSG) comprises 48 nuclear supplier countries that seek to contribute to the non-proliferation of nuclear weapons through the implementation of two sets of guidelines for nuclear exports and nuclear-related exports.²¹³ The NSG Guidelines also contain the so-called “Non-Proliferation Principle,” adopted in 1994, whereby a supplier, notwithstanding other provisions in the NSG Guidelines, authorises a transfer only when satisfied that the transfer would not contribute to the proliferation of nuclear weapons.²¹⁴ China was admitted into the NSG 30 years after its creation, 2004. It is interesting to note that even though Israel does not participate in all of these arrangements, they implement controls in line with these regimes.²¹⁵ China, on its part, maintains own DUT list in its national Export Control Law but references its non-proliferation obligations under international law when formulating its list.²¹⁶



211. Ibid.

212. Ibid.

213. [About the Nuclear Supplier Group \(NSG\)](#). Accessed June 19, 2024

214. Ibid.

215. [Israel Export Control Information \(doc.gov\)](#)

216. [环球律师事务所 \(glo.com.cn\)](#)

D. The Australia Group (AG)

The AG is an informal alliance established to reduce the possibility that exporting or transshipping nations may contribute to the proliferation of chemical and biological weapons (CBWs).²¹⁷ The Group convenes annually to explore strategies for enhancing the efficacy of participating nations' national export licensing policies to deter potential proliferators from acquiring materials for CBW initiatives. Participants in the Australia Group do not undertake any legally binding obligations. As such, the effectiveness of their cooperation depends solely on a shared commitment to CBW non-proliferation goals and the strength of their respective national measures.²¹⁸

CONCLUDING OBSERVATIONS:

The analysis of the export control measures in Nigeria's major supplier countries show that Israel, United States and China have comparatively rigorous export control requirements. Overall, China's export control regime for dual-use technology is governed by both local laws and international commitments. Likewise, the United States is a member of the Wassenaar Arrangement (WA), Nuclear Suppliers Group (NSG), Australia Group (AG), and Missile Technology Control Regime (MTCRG). Aside from being a member of the four multilateral export control regimes, the U.S. supports a multiplicity of treaties and UN-rooted norms on technological and arms control.


While the US subscribes to the four export controls regimes—WA, MTCR, AG, and NSG—China is a member of the NSG, but Israel is a party to none. Nevertheless, Israel's civilian export control regime currently encompasses the WA's List of Dual-Use Goods and Technologies, as well as a chemical, biological, and nuclear-related items list, which, is a collation of certain control lists under the aegis of the AG, NSG, and Chemical Weapons Convention.²¹⁹ Israel's Ministry of Defense can issue additional orders that define other dual-use items requiring export controls beyond the WA list, particularly those relevant to Israel's national security interests.²²⁰

217. The Australia Group, ["Introduction"](#). Accessed June 2024

218. Ibid.

219. Ibid.


220. Ibid.



While end-use certification is popular across export and import countries, Nigeria's EUC certification procedures are less rigorous when compared to the supplier countries. Israel's export control regimes include heightened methods of scrutiny such as post-shipment verification, periodic reporting, inspections and audits. It also incorporates record-keeping of up to ten-years of particulars of shipments in terms of the quantity, the value, the identity of the buyers, and the delivery dates, accompanied by an elaborate compliance mechanism for ensuring adherence to policies and maintaining up-to-date information on the flow of dual-use technologies.

While end-use certification is popular across export and import countries, Nigeria's EUC certification procedures are less rigorous when compared to the supplier countries. Israel's export control regimes include heightened methods of scrutiny such as post-shipment verification, periodic reporting, inspections and audits. It also incorporates record-keeping of up to ten-years of particulars of shipments in terms of the quantity, the value, the identity of the buyers, and the delivery dates, accompanied by an elaborate compliance mechanism for ensuring adherence to policies and maintaining up-to-date information on the flow of dual-use technologies.

China's end-use verification systems contain explicit prohibitions against diversion. Accordingly, exporters cannot change the end-use of the relevant controlled item or transfer it to any third party without consent of the state export control authorities, including notifying the state export control authorities about any change in the end-use or end-user of the item. In addition, China's export control authorities conduct risk assessments of countries and regions to identify importers and end-users violating the end-user and end-use management requirements; or endangering national security or interest; or using any controlled items for terrorism purposes. Just like Israel, China conducts inspections, audits and slaps penalties on violators.



These robust layers of scrutiny found in suppliers' export control regimes are for the most part, absent in Nigeria's EUC certification procedures even though custom authorities often use their discretion—at the port of entry—to apply administrative measures that achieve similar outcomes.

These robust layers of scrutiny found in suppliers' export control regimes are for the most part, absent in Nigeria's EUC certification procedures even though custom authorities often use their discretion—at the port of entry—to apply administrative measures that achieve similar outcomes. The lack of stringent importation controls at the national level and corresponding mechanisms for enforcing export trade control measures at the international level have made developing countries like Nigeria to become a haven for the unbridled importation of various kinds of technologies. The thin layers of scrutiny, compounded by porous borders, make the abuse and diversion of imported DUTs almost inevitable. Activists, journalists, campaigners, opposition politicians, dissenters and organized groups demanding accountability continue to bear the brunt of the exploitation and misuse of dual-use surveillance technologies. The activities of insurgent groups and non-state armed fighters further increase the propensity of arms and ammunition crossing borders. Weak border restrictions and inadequate security measures increase the chances of terrorists securing dual-use weapons to perpetuate these criminal activities.



CHAPTER

5



**THE LIMITATIONS OF
EXPORT CONTROL
REGIMES AND THE
IMPLICATIONS FOR
IMPORTING COUNTRIES**

As we saw in the last chapter, the export controls of major supplier countries are mainly predicated on considerations premised on national security, foreign relations, international obligations and other vital interests of the State. Similarly, trends in technologically advanced countries indicate a conscious drive toward growing their national DUT capabilities and inventories ultimately for military uses in the long-term. To put this in proper context, it means that supplier countries will put their own national security, interests, diplomatic influence and foreign policy first, before that of the importer. Some countries may introduce additional controls based on public security or human rights considerations. As we shall see, this is also subjective, and conditioned on the interests and foreign policy alignments of the supplier country.

The ultimate outcome is the emergence of global power asymmetry, enabled by technology, which confers power on one group to exert dominance on other less-developed countries. Very scant literary attention has been devoted to exploring and exposing the dangers of this technological dependency on the digital sovereignty of developing countries and the inherent potential for exploitation, domination and conquest. This chapter interrogates the effectiveness of emerging global tradition of technology governance, the implications for the political sovereignty of importing countries and the extent to which watchdogs can rely on the export control regimes of supply countries to increase accountability for responsible spyware trade and use.

5.1 HUMAN RIGHTS CONSIDERATIONS LACK CLARITY AND CONSISTENCY:

The consideration of human rights is increasingly becoming a central component of export control regimes and measures. This means that export countries will consider the human rights temperature in the locales where their products will be used. The supply, sale, transfer, and procurement of dual-use technologies and spyware continue to raise significant human rights, global stability, and security concerns across the world, despite the existence of these export control treaties and regimes. A major aggravating factor is the duplicitous differential in countries' application and compliance with the different regimes that regulate, control, and curb the abuse of dual-use products. A glaring example is the United States position on arms sale to Nigeria and Israel on the ground of human rights considerations. In 2014, the United States refused to sell weapons to Nigeria for its fight against Boko Haram on the grounds of alleged poor human rights records.²²¹ In 2021, the United States tightened its

221. [Boko Haram crisis: Nigeria fury over US arms refusal - BBC News](#)

export controls on “items used in surveillance of private citizens and other malicious cyber activities” and requires special licenses to export such technologies to countries where they can be used to abuse human rights.²²²

Compare the above stance to the numerous criticisms targeted against the US in relation to the Israel-Gaza crisis. According to Amnesty International USA, American-supplied weapons provided to the government of Israel have been used in serious violations of international humanitarian and human rights law, and in a way that is inconsistent with U.S. law and policy.²²³ Reciprocatively, amidst what many called Israeli-caused “genocide” in Gaza, the U.S. says “it has not found Israel to violate international humanitarian law in its conduct of the war in Gaza or the provision of humanitarian assistance.”²²⁴ The differential in the US position on Nigeria and Gaza reveals significant uncertainty regarding U.S. full compliance with export control regimes on dual-use products and international laws that seek to protect human rights from abuse, particularly in the dimension of arms trade and dual-use transfers.²²⁵

5.2 NATIONAL INTEREST AND NATIONAL SECURITY CONSIDERATIONS:

Countries' export control regimes are primarily influenced by national security considerations. They will restrict exports to countries if they perceive a risk that the end-user country could weaponize the technologies against them.²²⁶ It is instructive to highlight that supplier with vested interests in Nigeria's significant market may exert influence on the state's security policies and programs. Power and information asymmetries characterizing technology supply deals provide proxy ground for external powers to manipulate fragile institutions, exercise their own interests, and flex their muscles. For instance, Nigeria's lawmakers have given the go-ahead to a joint committee of police, public procurement, debt management and IT officials to investigate China's ZTE over a \$470 million contract for the Nation Communication Security System.²²⁷ The project also consists of the installation of close circuit television (CCTV) cameras in many strategic parts of the Federal Capital Territory (FCT). The investigation aimed to

222. [Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and other Malicious Cyber Activities | U.S. Department of Commerce](#)

223. Amnesty International, [“U.S.-Made Weapons Used by Government of Israel in Violation of International Law and U.S. Law”](#). (2024)

224. Americas, Middle East [“US says Israel not violating international humanitarian law in its use of US-supplied weapons”](#). (2024)

225. Ibid.

226. Ibid.

227. Michael Malakata, Nigeria Investigates ZTE Cybersecurity Contract, <https://www.csoonline.com/article/533926/data-protection-nigeria-investigates-zte-cybersecurity-contract.html>

determine whether the award of the project to ZTE conformed to due-process guidelines for government contracts and ascertain the quality of materials supplied.

This investigation was triggered by the suspicion that the real benefits of surveillance programs financed by Chinese loans flowed back to China. In other words, Nigeria paid out 15 percent (\$70.5 million) in advance payment for the project and signed a sovereign guarantee to the tune of \$399 million to enable China's ZTE to source loans from Chinese government for the project payable with interests. While China gains from both financing the surveillance projects, they make further gains by also supplying the same surveillance equipment. This translates to double profits from both the loans and the contract supplies which were allegedly substandard. There are also allegations of lack of transparency in the contract as well as the use of sub-standard materials. As a commentator aptly captured: "The money always ends up going back to China."²²⁸

The stringency of export controls also depends on how much national interest is invested in the industry. For a country like Israel, known as a hub for surveillance technology and home to the dominant NSO Group—Circle and Mer Security²²⁹—export control (or the enforcement of existing controls) may not be as stringent in other countries (like the EU) where the industry is not as significant. Through its licensing responsibilities in relation to defense equipment, know-how, and counter-proliferation, as well as preventing harm to Israel's international relations and national strategic interests, DECA has worked to protect Israel's national security and defense interests since its inception.²³⁰ It has been reported that NSO Group is a critical [bargaining] tool in Israeli diplomacy and foreign policy²³¹ and New York Times has described NSO Group as a "de facto arm of the [Israeli] State."²³² Israel has repeatedly licensed the export of Pegasus to authoritarian regimes²³³ and has failed to take any notable action against NSO Group following the Pegasus scandal. In addition to continuing to license Pegasus for export despite ongoing litigation against NSO Group, Israeli courts have ruled against revoking the export license of Pegasus software notwithstanding allegations that it has been used to target human rights activists and political dissidents around the globe.²³⁴

228. [Paul Mozur, Jonah M. Kessel](#) and Melissa Chan, New York Times, *ibid*.

229. [Israels Spy-Tech Industry Is a Global Threat to Democracy \(jacobin.com\)](#)

230. Israeli Ministry of Defense, "[Defence Control Agency \(DECA\)](#)". Accessed - June 2024

231. [How Israel used the NSO Group to further its diplomacy \(trtworld.com\)](#)

232. [Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker - The New York Times \(nytimes.com\)](#)

233. [The Battle for the Worlds Most Powerful Cyberweapon - The New York Times \(nytimes.com\)](#)

234. [SHANNON VAVRA](#), CYBERSCOOP, Israeli court rejects request to revoke NSO Group's export license, JULY 13, 2020, <https://cyberscoop.com/nso-group-amnesty-international-israel-export/>

Export control may also be used by a country to maintain political or strategic advantage over its competitors. For example, Israel's export of dual-use technologies, particularly cyber-surveillance tools have increased over the years. In 2022, Israel approved the sale of drones to 145 different countries, with a 25% increase in the number of countries to which intelligence and cyber systems were sold.²³⁵ China is known to highly discourage the export of technologies to countries with poor diplomatic relations with China.²³⁶

5.3 DEPENDENCY ON FOREIGN TECHNOLOGY AND EXPERTISE:

African states, including Nigeria are spending over \$1bn per year on digital surveillance technologies imported from countries like the U.S., UK, China etc.²³⁷ This translates into billions of dollars' worth of capital flows from developing economies to the advanced economies even though the former is globally described as "poor". Importing countries with such high importation budgets rarely allocate resources for developing their own national technological capabilities. What the procuring states don't probably know is that this dependency on foreign technological imports has several implications for their domestic political, economic, and security systems. Perhaps, a few countries are aware of these risks to their sovereign agency and sidestepping the predations of countries and companies supplying these technologies. For instance, out of the five countries studied in a recent report, Malawi is the only one to have rejected the safe city surveillance package offered by Chinese companies.²³⁸



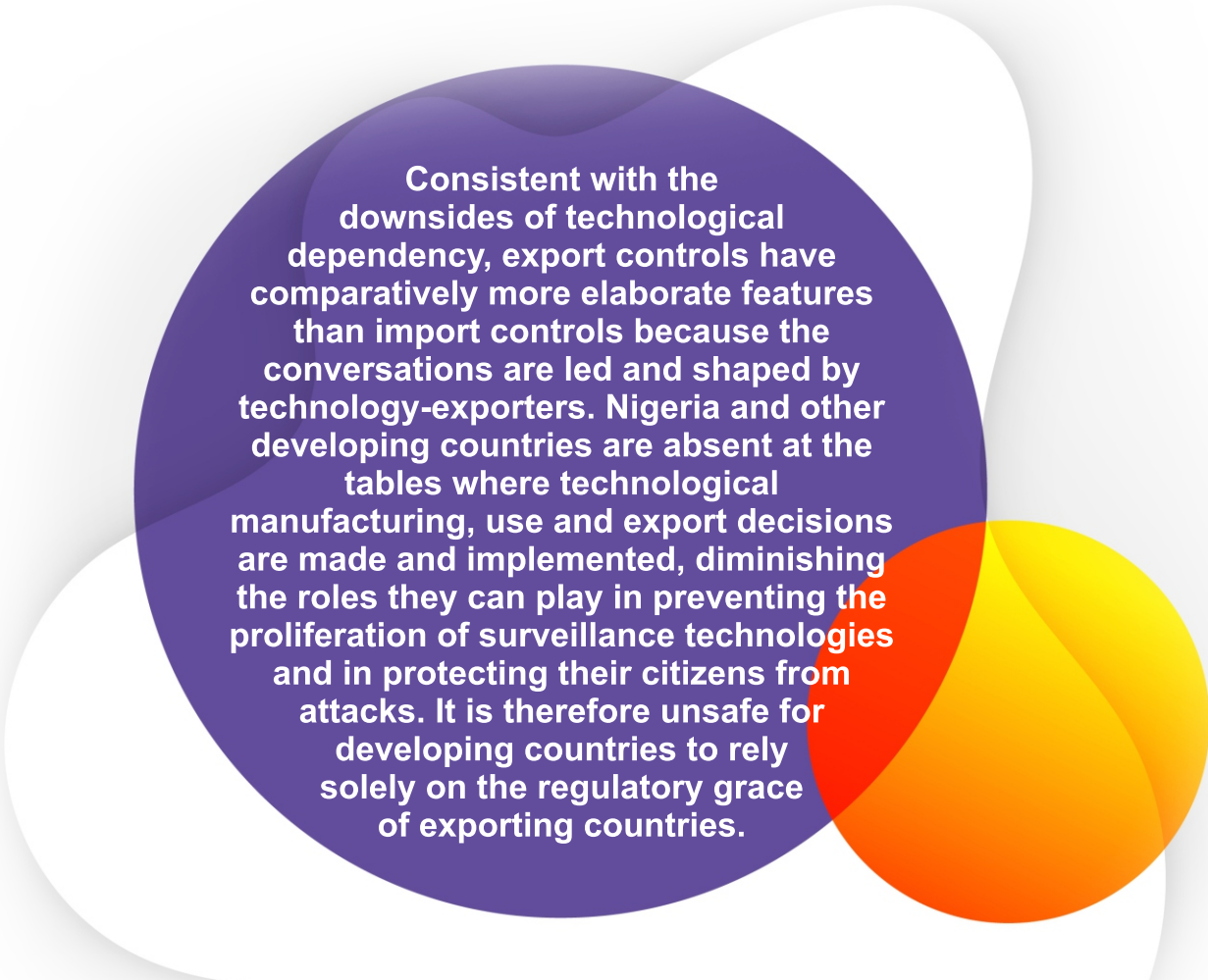
African states, including Nigeria are spending over \$1bn per year on digital surveillance technologies imported from countries like the U.S., UK, China etc.

235. Yaron, Oded, "[Record-breaking Spike in Countries Buying Israeli Arms and Cyber](#)". *Haaretz*. (2023)

236. [China to tighten export controls on dual-use technology - Nikkei Asia](#)

237. Roberts, T. et al. (2023) Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2023.027

238. Roberts, T. et al. (2023), *ibid*.



Consistent with the downsides of technological dependency, export controls have comparatively more elaborate features than import controls because the conversations are led and shaped by technology-exporters. Nigeria and other developing countries are absent at the tables where technological manufacturing, use and export decisions are made and implemented, diminishing the roles they can play in preventing the proliferation of surveillance technologies and in protecting their citizens from attacks. It is therefore unsafe for developing countries to rely solely on the regulatory grace of exporting countries.

Consistent with the downsides of technological dependency, export controls have comparatively more elaborate features than import controls because the conversations are led and shaped by technology-exporters. Nigeria and other developing countries are absent at the tables where technological manufacturing, use and export decisions are made and implemented, diminishing the roles they can play in preventing the proliferation of surveillance technologies and in protecting their citizens from attacks. It is therefore unsafe for developing countries to rely solely on the regulatory grace of exporting countries.

5.4 ECONOMIC SABOTAGE, CORRUPTION AND ILLICIT TRANSFER FLOWS:

The Nigerian state heavily relies on foreign suppliers, primarily from the USA, China, Europe, and Israel, for its surveillance technologies.²³⁹ Exactly how these

239. Victoria Ibezim-Ohaeri et al, Security Playbook of Digital Authoritarianism in Nigeria, *ibid*.

acquisitions are negotiated and supplied are shrouded in secrecy. These transactions are often classified as national security, and therefore, withheld from public scrutiny. The lack of transparency in the procurement processes raises concerns about corruption, fraud, and misuse of public funds, weakening domestic financial systems and reducing public confidence in government. This weakening effect not only stems from the presence of bribery and corruption, but from weak import controls, insufficient regulations governing dual use technologies and inefficient government institutions. A combination of these dysfunctions poses a disadvantage for developing countries like Nigeria procuring surveillance technologies and weakens their agency to negotiate favorable deals.

Additionally, surveillance technologies are often procured in foreign currency. Explaining why terrorism persists despite huge budgetary allocations to military procurements, a Nigeria military chief lamented:²⁴⁰

“In the past, you heard large sums of money approved for the military but the question is, how much do we get? That is very important. Also, we don't manufacture any of the items we use; we buy them in dollars. If you look at the amount released and you convert to dollars, how much is it?”

State agency to contract is further weakened by the precipitous decline of the national currency compared to the currency of the supplying country. Because the cost of surveillance technologies is unilaterally fixed by the supplier, this results in procuring countries being shortchanged or getting little value for their procurements.

5.5 ESPIONAGE CONCERNS:

Without watertight controls and safeguards, African states will remain the major victims of their own technological acquisitions and inadvertently expose their countries to unrestrained espionage activities. An independent investigation revealed how a China-financed and China-built computer network at the African Union (AU), allegedly [inserted a backdoor](#) that allowed it to transfer data.

²⁴⁰. News Express: Why terrorism continues despite huge budgetary allocations — Defence Chief, <https://newsexpressngr.com/news/211022/why-terrorism-continues-despite-huge-budgetary-allocations-defence-chief>

The hack wasn't detected until January 2017 when technicians noticed that between midnight and 2.00am every night, there was a peak in data usage even though the building was empty. After investigating, it was found that the continental organization's confidential data was being copied on to servers in Shanghai.²⁴¹ Since the discovery of the hack, the AU has allegedly acquired its own servers and refused Chinese offers to reconfigure them. Lessons learned from this episode underscore why strong import regimes and restrictions are necessary to reduce illicit activity of foreign actors in domestic markets that threaten state sovereignty and agency. Foreign cyber espionage on a country's public infrastructure, territory, and information technology systems may harm civilians' data and digital safety, and breach privacy rights.

5.6 DATA PRIVACY BREACHES:

The most concerning dimension is how the procurement of surveillance technologies from countries with scant regard for human rights values renders citizens more vulnerable to external harms and brazen privacy intrusions. Nearly all dual-use technologies and applications with surveillance capabilities—including smart phones, smart electronics, spywares, military equipment, social networking sites, etc. used in Nigeria—are externally produced and controlled.

Citizens' data in the hands of foreign nation-states that produce and supply these technologies could vest enormous influence over political or economic affairs of one foreign nation over Nigeria. In this regard, the Cambridge Analytica²⁴² scandal easily comes to mind where Facebook had allowed someone to extract vast amounts of private information about vast numbers of people from its system, and that entity had passed the data along to someone else, who had used it for political ends. This kind of data exposure—to foreign and commercial interests—may produce disparate physical and psychological outcomes for people and groups that already face discrimination and marginalization, such as women and children, the LGBTQ+ community, ethnic minorities etc., which could potentially translate into serious physical violence.²⁴³

241. Abdi Latif Dahir, Quartz, China “gifted” the African Union a headquarters building and then allegedly bugged it for state secrets, January 30, 2018, <https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years>


242. Julia Carrie Wong, The Guardian, The Cambridge Analytica scandal changed the world – but it didn't change Facebook, <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>

243. Western Balkans Cybersecurity Research Network, ONLINE ACTIONS, OFFLINE HARMS: Case studies on Gender and Cybersecurity in the Western Balkans, Geneva Center for Security Governance (October 2023); https://www.dcaf.ch/sites/default/files/publications/documents/Online-actions-offline-harms_EN-2nov2023.pdf

5.7 DUAL-USE SURVEILLANCE TECHNOLOGIES, AND THE CIVIC SPACE IN NIGERIA:

As we can see, the import controls at the national level as well as the export control regimes, at the international level, are significant for curtailing the supply, sale, transfer, and procurement of dual-use technologies. Yet, evidence shows that they do not assure fool-proof protection against infringements on human rights and constraints on the civic space.

The subsequent sections demonstrate how mass or targeted surveillance operations violate protected rights, especially when conducted unlawfully, without judicial warrants, independent oversight, or public consent. Of specific significance are the rights to privacy, freedom of expression, and association, which are guaranteed by the Nigerian 1999 Constitution and international human rights law.



As we can see, the import controls at the national level as well as the export control regimes, at the international level, are significant for curtailing the supply, sale, transfer, and procurement of dual-use technologies. Yet, evidence shows that they do not assure fool-proof protection against infringements on human rights and constraints on the civic space.

Surveillance Enables State Repression: The greatest concern around surveillance technologies is their potential misuse for political repression and human rights abuses. Surveillance practices also undermine the citizens' dignity, autonomy, and security, translating to significant reductions in citizens'

agency. Agency reductions are magnified by the state's power to punish dissent. This creates a chilling effect as citizens self-censor or avoid public engagement for fear of being surveilled or punished. The citizens have little agency to challenge or resist the state's surveillance because of low digital literacy, poverty and broader limitations in access to justice.

While all citizens are subjected to the adverse impacts of arbitrary surveillance, evidence shows that certain groups of civic actors are disproportionately affected. According to a recent finding by Spaces for Change, journalists are disproportionately targeted and impacted by state repression more than other civic actors.²⁴⁴ According to the Closing Spaces Database which the recent report was premised upon:

Journalists covering environmental justice issues, the mismanagement of natural resources and extractive activities are more likely to get into trouble or experience brutality by security operatives in Nigeria while long prison terms and huge fines are popular silencing techniques used on journalists and media outlets...Press coverage for classified operations of the police and the military comes at a great cost in Nigeria and other West African countries where the accused persons are often slammed with criminal investigations or criminal charges bordering on "qualified disobedience,"²⁴⁵ "violating defense secrecy"²⁴⁶ and acts 'inimical to state and national security"²⁴⁷ respectively.

Apart from journalists, other groups primarily targeted by repressive surveillance operations include protesters, activists, opposition politicians and civil society organizations. Beyond surveilling the finances and movements of #EndSARS protesters, their bank accounts were frozen, and they were slammed with terrorism financing criminal charges which attracts up to life imprisonment.²⁴⁸ Not only that, police operatives mount surveillance at strategic

244. Spaces for Change, Civic Space in West Africa: Trends, Threats and Futures (2023)

<https://spacesforchange.org/civic-space-in-west-africa-trends-threats-and-futures/>

245. [Authorities Investigate 3 Cape Verde Journalists After Reporting On Police Killing](#)

246. [Senegalese Journalists Arrested over Military Coverage](#)

247. Committee to Protect Journalists, [Nigerian journalist jailed for refusing to reveal source](#)

248. Victoria Ibezim-Ohaeri, AGFCS et al, #ENDSARS: Police Brutality, Protests and Shrinking Civic Space in Nigeria, (2020) <https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/>

such as by threatening to reveal intimate information or images illegally obtained through surveillance. The apparent widespread use of Pegasus spy software to illegally undermine the rights of those under surveillance, including journalists and politicians, was "extremely alarming" and confirmed "some of the worst fears" about the potential misuse of such technology.²⁵⁵ Following the deployment of Pegasus spyware to target one of its staff in 2021, Human Rights Watch asked governments to ban the sale, transfer, and export of surveillance technologies until human rights safeguards are in place.²⁵⁶ In Nigeria, how surveillance has been deployed against civic space activities is being widely documented:



Aminu Adamu Muhammed posted on Twitter that the wife of President Buhari had put on a lot of weight suggesting that she was benefiting from wealth plundered by the President. He was tracked by the State Security Service to his school and arrested over 5 months after making the post.²⁵⁷



Emeka Richmond Ngornadi, a Lagos-based Igbo businessman, was tracked for 2 years and eventually arrested while he was on the way to visit his wife in Anambra State for a post he made allegedly in support of the Indigenous People of Biafra (IPOB). He was detained in inhumane conditions and was put under pressure to admit that he was a member of IPOB.²⁵⁸



Chido Onuma, a journalist and author, was arrested by the State Security Service upon his arrival at the airport in Abuja from Spain in September 2019. He was flagged allegedly for wearing a shirt supporting Biafra, even though the inscription on his shirt was the title of his book.²⁵⁹

255. United Nations News, "[Pegasus: Human rights-compliant laws needed to regulate Spyware](#)". (2021)

256. Human Rights Watch, "[Human Rights Watch Among Pegasus Spyware Targets](#)". (2022)

257. [Aminu said he was arrested, beaten on Aishas order Uncle \(punchng.com\)](#)

258. [DSS Arrest and Detained Businessman for Expressing Support for IPOB Online - Closing Spaces](#)

259. [Why I was arrested - Chido Onumah | Premium Times Nigeria \(premiumtimesng.com\)](#)

Surveillance Can Thwart Civic Action: Surveillance can be used by the government as counterintelligence against civil society. Although security operatives use counterintelligence as a tactic for gathering information necessary to prevent security breaches. This tactic has been deployed to counteract planned campaigns or organized protests by civil society. COINTELPRO is the most infamous demonstration of how intelligence gathered through surveillance can be used clandestinely to disrupt civic movements. According to the FBI, “The FBI began COINTELPRO — short for Counter intelligence Program — in 1956 to disrupt the activities of the Communist Party of the United States.²⁶⁰ In the 1960s, it was expanded to include a number of other domestic groups.”²⁶¹

Similarly, Nigerian authorities cracked down on “EndSARs” protesters, charged prominent supporters of financing terrorism and suspended the bank accounts of twenty individuals and entities that supported the protests. Targeted groups either raised or received money in support of the protests that erupted across Nigeria in 2020, against recurring acts of police brutality by men of a unit of the Nigeria Police Force known as the Special Anti-Robbery Squad (SARS). The monies were used to provide medical and legal aid for injured and arrested demonstrators, grants for journalists to cover police and army abuses at the protests, and help to families of those killed during the demonstrations.²⁶² Surveilling customers' financial transactions during the protests aided in tracking the bank accounts of #EndSARs supporters as bank staff revealed that the directive to block accounts was related to transaction records that included references to EndSARS.²⁶³ The constant feeling of being watched or their financial transactions being monitored can discourage people from expressing critical opinions, supporting or participating in protests. This stifles free speech and creates a climate of fear.²⁶⁴ It can also strangle public discourse and prevent the formation of opposition movements especially in countries with weak rule of law systems and limited oversight.

Surveillance Breeds Distrust Between the Government and Civil Society: Surveillance drives a wedge between civil society and the government. This distrust impacts the morale of civic space actors and in the place of vibrancy,

260. This is a self-admission by FBI

261. [FBI Records: The Vault COINTELPRO](#)

262. The Guardian <https://www.theguardian.com/world/2020/nov/13/nigeria-cracks-down-on-end-sars-protesters-alleging-terrorism>

263. Human Rights Watch, Nigeria: Punitive Financial Moves Against Protesters, November 13, 2020 via <https://www.hrw.org/news/2020/11/13/nigeria-punitive-financial-moves-against-protesters>

264. Ibid.

installs apathy. A deflated civic space may be seen as a political victory by authoritarian governments. Nothing fuels this deflation more than the way surveillance fuels paranoia and self-censorship. The knowledge, or even the perception, that one is being surveilled elicits fear and paranoia which have chilling effects on civic actors. According to a study,²⁶⁵ the prompting and fueling of “paranoia” is a tactic with a longstanding precedent used by intelligence agencies in both Western democracies and authoritarian countries to mount pressure on activists and journalists.²⁶⁶ For example, the revelation that the FBI had for years been running a covert domestic counter-intelligence operation dubbed COINTELPRO gave rise to paranoia that led journalists to believe there was “an FBI agent behind every mailbox”.²⁶⁷

Surveillance Forces Activists to Resort to Self-Censorship and Self-Exile: Paranoia often leads to self-censorship, or self-exile, knowing that one is being observed by a person who has the power and wherewithal to take action against him. Feeling watched has been described as a powerful tool for social control.²⁶⁸ According to security expert Bruce Schneier, “the fact that you won't do things [that you would ordinarily do, and the fact] that you will self-censor, are the worst effects of pervasive surveillance.”²⁶⁹ According to a United States Office of the High Commissioner on Human Right (OHCHR) report;

Increasing numbers of journalists and media workers are forced to flee abroad to escape political persecution and legal and other restrictions in their own country. In exile, they are not always safe or able to exercise their profession freely. Physical and online threats and attacks, surveillance from home or host countries, language barriers, lack of legal status and restrictions on their freedom of movement, and retaliation against family members in their home country are constant concerns.²⁷⁰

265. [Now You See Me Now You Don't: Journalists Experiences With Surveillance \(tandfonline.com\)](https://www.tandfonline.com)

266. Ibid, page 4

267. Ibid. See also Pew Research Center study of 2015 showing the perception by journalist of being under government surveillance - [Investigative Journalists and Digital Security | Pew Research Center](https://www.pewresearch.org)

268. [How Fear of Government Surveillance Influences Our Behavior | Literary Hub \(lithub.com\)](https://www.lithub.com)

269. Ibid.

270. [OHCHR | Report on Journalists in Exile](https://www.ohchr.org)

Self-exile is one of the dangerous consequences of arbitrary surveillance as was seen in the case of Eti-Inyene Akpan, a freelance photojournalist.²⁷¹ Fearing for his safety after taking and uploading photos of protesters' killings during the #EndSARS protests in October 2020, Akpan fled the country. He reported receiving several calls from unknown persons asking him to pull down his posts. His bank account was frozen while personnel of the State Security Service visited his office to look for him.²⁷² Fleeing the country on self-exile may not even guarantee the freedom he seeks.



CONCLUSION

Indeed, legitimate grounds necessitating massive surveillance procurements exist, ranging from easing crime detection, combating terrorism, transforming governance through automated systems and processes or improving service delivery. Festering security challenges in different parts of the country also provides powerful alibi for the authorities to procure surveillance and crime-fighting technologies. Despite these justifications, overwhelming evidence shows²⁷³ that these acquisitions have for the most part, served state interests and entrenched power imbalances between the rulers and the ruled. The imbalances do not only provoke a fierce clash between state power and citizens' rights but also raise fundamental questions about privacy protection, information integrity and the effectiveness of domestic import control regimes.

271. [How Digital Surveillance Threatens Press Freedom In West Africa - HumAngle \(humanglemedia.com\)](https://humanglemedia.com)

272. Ibid.

273. Victoria Ibezim-Ohaeri et al, Action Group on Free Civic Space, Security Playbook of Digital Authoritarianism in Nigeria (December 2021): <https://closingspaces.org/the-security-playbook-of-digital-authoritarianism-in-nigeria/>

CHAPTER

6



**OPPORTUNITIES
FOR LEGAL
REFORM AND
CIVIC ACTION**

Evidently, poorly regulated importation and use of dual-use surveillance technologies precipitate norm shifts in the direction of autocracy. In response to this trend, individuals, groups, civic actors and lawmakers are exercising their agency in diverse ways to resist repression and the power imbalances associated with digital surveillance. Advancements in digital technology have widened the umbrella of activism, allowing new entrants like bloggers, media influencers, freelance writers, including ordinary citizens to have greater access to online and offline spaces for civic action. Consequently, the internet and social media easily handed citizens a limitless tool for expression and democratic participation, expanding the civic space beyond the traditional media outlets, the streets and town halls. In this chapter, we examine opportunities for civic actors to push for the reform of import controls for dual-use surveillance technologies and safely navigate the new paradigm of digital ecosystems for protecting specific communities. Below, we proffer next steps campaigners can take to either refine or demand reform of spyware imports into Nigeria.

A. Reforming Regulatory Frameworks for Import Controls: Nigeria needs to develop a robust legal framework for regulating the importation of dual-use technologies. As research evidence shows, ONSA's EUC is an inadequate control measure. Not only that, ONSA's EUC certification protocol, though enforced by the Nigeria Custom Service (NCS), is not yet backed by statute. As such, the EUC is widely perceived as an adhoc measure requiring statutory foundation. A new legal framework, with inputs from civil society, will not only set the terms and conditions for the importing DUTs, including surveillance technologies, but also draw from the robust legal arrangements in the export control sphere—not limited to explicit prohibitions against diversion, pre- and post-shipment verification procedures, periodic reporting, inspections, audits, record-keeping, law enforcement institutions and penalties for breach. To improve transparency, it is imperative for the compliance systems for ensuring adherence to import controls to publish information on authorizations, denials and prohibitions as well as the jurisdictions DUTs are imported from. As an importing country, it is imperative for Nigeria to prescribe stringent import controls because the country bears ultimate responsibility for protecting its citizens from the rapacious economic pursuits of exporting countries.

B. Independent and Efficient Regulator: Because ONSA is itself an importer of military equipment and DUTs, its role in overseeing the issuance and implementation of import controls is conflicted. ONSA's multiple roles as a user, importer and regulator, all at once, raises questions as to its ability to impartially balance the entity's vested interests versus the discharge of their regulatory responsibilities to the public. A separate regulator that is not involved in the surveillance supply chain is better suited to play this regulatory role such as the

Ministry of Trade and Investment. This is the approach taken by technology-exporting countries Like Israel, China and the US.

Israel's Export Control Agency of the Ministry of Economy and Industry regulates the export of dual-use technologies designed for civilian and commercial purposes while the DECA, under the Ministry of Defense is responsible for exports of defense equipment and dual-use items designed for military purposes or military end-users. China also adopts a two-tiered regulatory approach, with the dual-use Items (goods) administered and regulated by either the State Council or the Central Military Commission (CMC) departments, depending on the category they fall into. The United States' regulatory approach is somewhat similar. The U.S. Bureau of Industry and Security (BIS) under the Department of Commerce regulates the country's export of dual-use commodities, software, and technology. Adopting this model of an independent regulatory is accordingly, relevant for the Nigerian context in order to enhance law enforcement and compliance with extant regulations relating technology. The independent regulator must be equipped to tackle the complexities of DUTs and constituted in such a way as to assure the protection of citizens' rights.

C. Due Diligence: For export and import controls to be effective, due diligence is indispensable. Control regimes must demand two levels of due diligence – (a) due diligence by the authorities, and (b) due diligence by the exporters and importers. The obligation of state authorities to conduct due diligence forms part of their obligations under international human rights law. The UN Human Rights Committee, in reference to states' obligations under the International Covenant on Civil and Political Rights noted that states may violate their obligations under the covenant by “permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm” that private persons or entities cause.²⁷⁴

The obligation to conduct due diligence does not rest on the authorities alone. As responsible business persons, exporters must bear some responsibility toward ensuring that DUTs do not fall into the wrong hands.²⁷⁵ As expected, the business community has pushed back against legally-binding due diligence obligations,

274. Human Rights Committee: 'General Comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant', UN Doc CCPR/C/21/Rev.1/Add.13 (29 March 2004) para 8.

275. See [fourth edition of PI's Guide to International Law and Surveillance](#). Article 39 of the **Report of the United Nations High Commissioner for Human Rights, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests, UN Doc A/HRC/44/24 (24 June 2020)** provides: All business enterprises, including those that develop new technologies that are used to monitor the activities of civil society actors, have a responsibility to respect human rights.

which they consider as additional bottlenecks in doing business.²⁷⁶ They argue that it is not their responsibility to determine standards of human rights and as such, cannot be expected to conduct checks except as prescribed by law.²⁷⁷ However, there are international human rights principles which suggests that the due diligence obligations of business persons are not optional. Principle 13 of the UN Guiding Principles on Business and Human Rights provides that:

The responsibility to respect human rights requires that business enterprises: (A) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; (B) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

More specifically, Principle 17 provides that:

In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Human rights due diligence: (a) Should cover adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships; 18 (b) Will vary in complexity with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations; (c) Should be ongoing, recognizing that the human rights risks may change over time as the business enterprise's operations and operating context evolve.

²⁷⁶. Trans-European Policy Studies Association (2022) Parties to the Covenant', UN Doc CCPR/C/21/Rev.1/Add.13 (29 March 2004) paragraph 8.

²⁷⁷. Machiko Kanetake (2019)

The above provisions place a corresponding obligation on technology-exporting countries like China, US and Israel to go beyond box-ticking to conducting real impact analysis of the use of the product in the destination country in terms of risks to security and human rights. Due diligence requirements have also been incorporated as part and parcel of DUT regulations, including import and export controls in some jurisdictions. For instance, the EU's regulations require exporters to notify the authorities if they become 'aware' that non-listed dual-use items are intended for the commission of serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression.²⁷⁸ Also, the French Duty of Vigilance Law sets out the obligation of large corporates to implement a vigilance plan aimed at preventing serious violations of human rights, health and safety, and damage to the environment as a result of the activities of the corporate as well as subcontractors and suppliers down the value chain.²⁷⁹

D. Transparency: To further ensure accountability, regulators should implement transparency requirements. The opacity in the industry is still a source of concern. An example is the difficulty in accessing information regarding the licensing for the NSO Group whose spyware has enabled the invasion of privacy of journalists and other civil space actors at a phenomenal scale.²⁸⁰ A watchdog coalition²⁸¹ has advocated that “neither the companies nor states concerned should be allowed to withhold critical information under the pretext of commercial confidentiality or national security concerns”²⁸²

In 2021, the European Union issued a modified regulation setting up a “Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items”²⁸³ The regulation dedicates a section to transparency provisions, obligating the European Commission to submit an annual report to the European Parliament and the Council on the implementation of the regulation and on the activities, examinations and consultations of the Dual-Use Coordination Group. That annual report shall be public and shall include information on authorizations (in particular, the number, value, types of items and destinations at Union and Member State levels), denials and prohibitions under the regulation. A similar parliamentary oversight, backed up

278. Article 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821).

279. Linklaters (2023): French Duty of Vigilance Law: first decision on the merits rendered by a French Court, <https://sustainablefutures.linklaters.com/post/102iuhu/french-duty-of-vigilance-law-first-decision-on-the-merits-rendered-by-a-french-c>, retrieved 8 July 2024.

280. [EU: Robustly Implement New Export Rules for Surveillance Tech | Human Rights Watch \(hrw.org\)](#)

281. which includes Human Rights Watch, Amnesty International, RSF, CPJ and Access Now,

282. Ibid.

283. [Regulation - 2021/821 - EN - EUR-Lex \(europa.eu\)](#)

with periodic reporting cycle, (monthly) in Nigeria would accelerate the country's effort toward attaining transparency in the enforcement of import controls.



E. Voluntary Best Practice Initiatives: States and companies keen on developing a responsible business culture are taking voluntary steps to curb the abusive tendencies of DUTs, including surveillance technologies. Best practices of voluntary compliance take the form of accession to rights-based codes of conduct and joining networks of like-minded peers. Nigeria may require suppliers and importers of DUTs into Nigeria to subscribe to any of the initiatives below:

GROUP / INITIATIVE	NOTABLE MEMBERS	GUIDING PRINCIPLES AND COMMITMENT
Export Controls and Human Rights Initiative	Australia, Denmark, Norway, the United States. Israel did not endorse the code of conduct on dual-use technology exports. ²⁸⁴	Code of Conduct 2023 ²⁸⁵ Ensure that domestic legal, regulatory, policy and enforcement tools are appropriate and updated to control the export

284. Georgetown Journal of International Affairs, *Cyber Mercenaries: Limiting Government Use of Commercial Spyware*, September 4, 2024, <https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/>

285. [230303 Updated ECHRI Code of Conduct - FINAL \(state.gov\)](https://www.state.gov/230303/Updated-ECHRI-Code-of-Conduct-FINAL)

GROUP / INITIATIVE	NOTABLE MEMBERS	GUIDING PRINCIPLES AND COMMITMENT
		control the export of dual-use goods or technologies to end-users that could misuse them for the purposes of serious violations or abuses of human rights
Summit for Democracy 2023	Canada, France, Germany, Ghana, Kenya, Tunisia, the UK and the US	<p>Guiding Principles on Government Use of Surveillance Technologies²⁸⁶</p> <p>Governments should not use surveillance technologies to unjustifiably interfere with freedom of expression; discourage the exercise of human rights and fundamental freedoms; perpetrate technology-facilitated gender-based violence or discrimination online and offline; perpetuate harmful or discriminatory norms and stereotypes; or limit bodily autonomy through any means, including but not limited to unlawful collection or misuse of personal health data, including reproductive and sexual data, or distribution of intimate images.</p>
Summit for Democracy 2024	Australia, Canada, Costa Rica, Denmark, France, Finland, Germany, Japan, New Zealand, Norway, Poland,	<p>Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware</p> <p>Establish robust guardrails and procedures to ensure that any</p>

286. [FOC FINAL - Surveillance Principles \(03092023\) \(state.gov\)](#). Three main areas of concern identified are: (1) the use of internet controls to suppress human rights by limiting access to information, (2) the use of AI to continuously monitor people without legal basis, and (3) use of analytic tools to support the discriminatory enforcement of laws against vulnerable groups, dissidents, and the like.

GROUP / INITIATIVE	NOTABLE MEMBERS	GUIDING PRINCIPLES AND COMMITMENT
	Ireland, Republic of Korea, Sweden, Switzerland, the United Kingdom, and the United States	<p>commercial spyware use by our governments is consistent with human rights.</p> <p>Preventing the export of software, technology, and equipment to end-users who are likely to use them for malicious cyber activity.</p> <p>Robust information sharing on commercial spyware proliferation and misuse, including to better identify and track these tools.</p>
Global Network Initiative	Google, Meta, Yahoo, Zoom, MTN, Microsoft, Human Rights Watch	<p>Global Principles on Freedom of Expression and Privacy²⁸⁷</p> <p>ICT companies have the responsibility to respect and promote the freedom of expression and privacy rights of their users. ICT has the potential to enable the exchange of ideas and access to information in a way that supports economic opportunity, advances knowledge and improves quality of life. By implementing these Principles, ICT companies can also work to protect, promote and support human rights, including through improved responsible decision-making, shared learning and multi-stakeholder collaboration.</p>

287. [GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf \(globalnetworkinitiative.org\)](https://www.globalnetworkinitiative.org/wp-content/uploads/2015/02/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf)

GROUP / INITIATIVE	NOTABLE MEMBERS	GUIDING PRINCIPLES AND COMMITMENT
Global Network Initiative	Google, Meta, Yahoo, Zoom, MTN, Microsoft, Human Rights Watch	<p>Implementation Guidelines for The Principles on Freedom of Expression and Privacy²⁸⁸</p> <p>Consistent with the UN Guiding Principles on Business and Human rights, and considering international human rights standards, participating companies will carry out human rights due diligence to identify, prevent, evaluate, mitigate and account for risks to the freedom of expression and privacy rights that are implicated by the company's products, services, activities and operations.</p>

E. Human Rights by Design: Technology can still fall into the wrong hands in spite of all due diligence and precautions. This is why “human rights by design” has been proposed as a key tool for the protection of human rights in the age of technology. The principle posits that instead of grappling with reining in the human rights abuses orchestrated using new technologies, the producers should commit to designing technologies that respect human rights by default instead of enabling features that can give rise to human rights abuses.²⁸⁹ For DUTs such as surveillance technologies, the designers of the tools will already preempt the human rights impact of the tool and incorporate safeguards at the design stage.

For example, the potential of artificial intelligence to be used as a tool of human rights abuse has been widely discussed.²⁹⁰ Algorithms have been created to censor speech, discriminate against a demography, and target a group of people for attack.²⁹¹ So, why create them in the first place? At the moment, this is still an

288. [Implementation-Guidelines-for-the-GNI-Principles.pdf \(globalnetworkinitiative.org\)](https://www.globalnetworkinitiative.org/implementation-guidelines-for-the-gni-principles.pdf)

289. Jonathon Penney Sarah McKune Lex Gill Ronald J. Deibert (2018)

290. Volker Türk (2024): Human rights must be at the core of generative AI technologies, says Türk, <https://www.ohchr.org/en/statements-and-speeches/2024/02/human-rights-must-be-core-generative-ai-technologies-says-turk>, retrieved 8 July 2024

291. Ibid.

ethical question but it is fast gaining recognition both among states and corporates who seek to advance human rights. At the corporate level, big organizations like Google are taking steps to incorporate this philosophy in the development of their products. For example, Google engaged experts to conduct a human rights assessment at the development stage of its new celebrity recognition application program interface (API) for use in the media and entertainment industry.²⁹² Corporates can also introduce features that restrict some functionalities of technologies which may be abused. For example, tracking software can require an additional level of authorization from the designers or regulators to be able to deploy the software beyond a particular number of targets.

MOBILIZING RESISTANCE TO SURVEILLANCE INITIATIVES IN NIGERIA

Civic actors have responded to arbitrary surveillance during four major situations: (1) research enquiries, (2) halting repressive legislations, (3) challenging secrecy and (4) spearheading accountability campaigns for specific injustices. On the first part, there is scant homegrown literature undertaking indepth examinations into the security of cyberspaces, the scale of online and offline surveillance and the range of technology-facilitated threats in domestic systems. Research consortiums are however emerging across the country, with mainly independent researchers and non-governmental organizations populating these consortiums. Examples include the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Action Group on Free Civic Space (AGFCS), Africa Digital Rights Network (ADRN) etc.

CIPESA's network of collaborators in Africa and globally, share the vision of advancing an open, safe and free internet and work to promote effective and inclusive ICT policy and practice for improved governance, livelihoods, and human rights in Africa.²⁹³ AGFCS members leverage diversity and expertise within the network to undertake joint action research projects. The group has been investigating the Security Playbook aimed at identifying and analyzing incidents of the misuse of the security architecture and digital technologies to crack down on civic actors in Nigeria. Likewise, Nigerian organizations are members of the Africa Digital Rights Network (ADRN), composed of activists, academics and analysts who carry out research on digital rights in Africa.²⁹⁴

292. Jonathon Penney Sarah McKune Lex Gill Ronald J. Deibert (2018)

293. About CIPESA: <https://cipesa.org/about-us/about-cipesa/>

294. See ADRN website <https://www.africandigitalrightsnetwork.org/>

They carry out novel studies, produce unique reports, and are publishing a groundbreaking series of collected edition books.

The homegrown research initiatives build a body of evidence to steer policy reform and for civic actors working to challenge rising levels of digital authoritarianism. An example is how AGFCS members are leveraging the findings of the three Security Playbook reports to take action to reform relevant norms and laws via policy and regulatory advocacy. They are also addressing downstream harms of the security and counterterrorism architecture through engagement with security and law enforcement agencies as well as initiating advocacy to improve data protection and reform of the surveillance ecosystem through a cross-cutting dimension exploring gendered and intersectional impacts.²⁹⁵

On the second part, the introduction of draft statutes containing repressive provisions present opportunities for civic groups to rally round an issue of common interest. AGFCS members have collectively [responded to legislative proposals](#) that hold enormous potential to shrink the civic space. From the Social Media Bill to the NGO Bill to the Infectious Diseases Bill, the group has intervened together as the need arises to help solve specific legal and non-legal problems presented on a rolling basis. These bills conferred significant surveillance and policing powers to law enforcement agencies. The Infectious Diseases Bill (IDB 2020) introduced during the COVID-19 pandemic sought to enlarge governmental powers to reduce infection spread through strict enforcement of public health protocols, contact tracing, ramping up testing, increasing genomic surveillance of the virus to identify circulating variants. Resistance to the draft statute particularly stemmed from Section 24 of the now rested IDB 2020 which granted overreaching powers to law enforcement officers or the police to surveil, trace and apprehend persons suffering from infectious diseases. The successful outcomes and cumulative impact of these joint interventions inspired the coalition to adopt collaborative problem-solving as an indispensable strategy for delivering its civic space advocacy objectives.

On the third part, challenging secrecy and encouraging transparency is the primary motivation for most interventions initiated by active citizens and advocacy groups in Nigeria. Both civil society organizations, the media, active citizens, professional bodies, policy makers, among others, deploy varying strategies such as research, advocacy, litigation, and public campaigns to

295. See Action Group on Free Civic Space, <https://closingspaces.org/group-activities/>

challenge unregulated surveillance and advocate for digital rights and accountability. To dismantle the secrecy characterizing security and surveillance contracts, groups have utilized public interest litigation as a strategy for demanding contract transparency. In one of the lawsuits, a Federal High Court in Abuja issued an order requiring Nigeria's former President Buhari and his regime to answer for how a \$460 million Chinese loan was used to fund the failed Abuja Closed-Circuit Television (CCTV) project.²⁹⁶ The lawsuit particularly challenged the government's failure to "disclose information and specific documents on the total amount of money paid to contractors from the \$460 million loan obtained in 2010 from China to fund the apparently failed Abuja Closed-Circuit Television (CCTV) project, and failure to name the contractors involved and explain why the government has continued to re-pay the loan."²⁹⁷

It is not only civic groups that are pushing to dismantle the structures of secrecy surrounding surveillance contracts. Federal lawmakers and the media have notably complemented the advocacy pursuits of civil society groups. In November 2023, the Nigerian Senate, exercising their legislative oversight functions, ordered a probe into the implementation of the \$500 million contract for the installation of Closed-Circuit Television (CCTV) cameras in the Federal Capital Territory. The project was awarded to a Chinese firm, ZTE Communications in 2010, for the installation of five components, including the video surveillance system and comprehensive, reliable, modern and robust public security communication technology.²⁹⁸ In the same vein, journalists play a crucial role in reporting about the procurement and use of surveillance technologies, contributing to public debate, and pressuring the government and companies to be more transparent and accountable.

Also, the courts play a major role in reviewing security decisions and initiatives. Interpreting Section 45 of the Nigerian Constitution which permits human rights derogations in certain circumstances, the Federal High Court ruled in the context of right to peaceful assembly and association that for a circumstance which will justify derogations from constitutionally guaranteed rights to arise, there must be a properly declared state of emergency.²⁹⁹ The implication is that there ought to be an extraordinary situation before the derogation of one's rights can be

296. SERAP website: SERAP sues FG over failed Chinese \$460m Abuja CCTV project, <https://serap-nigeria.org/2019/12/01/serap-sues-fg-over-failed-chinese-460m-abuja-cctv-project/>

297. SERAP website, *ibid.*

298. [Godsgift Onyedinefu](#), Business Day, Senate demands probe into \$500m spent on CCTV cameras for FCT November 23, 2023, <https://businessday.ng/news/article/senate-demands-probe-into-500m-spent-on-cctv-cameras-for-ct/>

299. All Nigeria Peoples Party v Inspector General of Police (2006) CHR 181

justified. Notwithstanding these safeguards and oversight mechanisms, it is safe to conclude that the interception of personal communications poses a serious threat to the constitutionally-protected right to privacy³⁰⁰ and undermines personal data protection. Because the specific circumstances where authorized interception can take place are very wide and unpredictable, implementing these laws without adequate checks and balances potentially increases citizens' exposure to unrestrained surveillance and privacy intrusions that are usually justified by reference to national security.

Lastly, accountability campaigns by civic actors take various forms. It encompasses online and offline campaigns demanding the release of arrested activists and protesters under government's watchlists;³⁰¹ push for legal reforms;³⁰² lawsuits seeking justice;³⁰³ digital literacy and security trainings to empower citizens on how to protect their online privacy and security. Spaces for Change (S4C), as well as Paradigm Initiative, a social enterprise that builds an ICT-enabled support system, run Digital Security Clinics and Digital Rights and Inclusion Media Fellowships to promote digital rights in Africa³⁰⁴ etc. Sustaining accountability campaigns often involves building relationships and alliances between civil society, local communities, state actors and the private sector so as to co-create innovative ideas, improve results, increase capacity and maximize impact. This has allowed for the complementarity of skills, and for deepening the bonds of solidarity among local stakeholders as they maximize the use of existing spaces to organise and collectively respond to threats.³⁰⁵

CONCLUSION

In conclusion, the intended purposes for acquiring surveillance technologies vary. However, an examination of digital surveillance in Nigeria reveals a

300. Section 37 of the Constitution of the Federal Republic of Nigeria

301. Premium Times, Police detain EndSARS activist Eromosele Adene for days without charge — Lawyer, November 10, 2020, <https://www.premiumtimesng.com/news/headlines/425447-police-detain-endsars-activist-eromosele-adene-for-days-without-charge-lawyer.html?tztc=1>

302. FIJ, Data and Digital Rights Coalition Addresses Data Censorship and Surveillance in Nigeria, <https://fij.ng/article/data-and-digital-rights-coalition-addresses-data-censorship-and-surveillance-in-nigeria/> in Nigeria

303. CHANNELS TV, ECOWAS Court Declares FG's Twitter Ban Unlawful, <https://www.channelstv.com/2022/07/14/ecowas-court-declares-fgs-twitter-ban-unlawful/>

304. Spaces for Change, Pushing Back Against Digital Risks and Threats in Abia State, <https://spacesforchange.org/pushing-back-against-digital-risks-and-threats-in-abia-state/>

305. Victoria Ibezim-Ohaeri, GALVANIZING COLLECTIVE ACTION TO PROTECT THE CIVIC SPACE IN NIGERIA, Shehu Musa Yar Adua Foundation, <https://www.yaraduafoundation.org/files/Galvanizing%20Collective%20Action.pdf>

complex landscape defined by power dynamics, rights infringements, and the agency of various actors. The Nigerian government's substantial investment in surveillance technologies raises questions about the underlying motivations and the impact on citizens' fundamental rights.

The historical context of surveillance in Nigeria, dating back to the pre-colonial era, highlights the persistence of state control mechanisms. Since the establishment of the former NSO to the current metamorphosis into the Department of State Services (DSS), the way the agency conducts its covert and surveillance operations have evolved over time. While the government's evolving approach also reflects an adaptation to contemporary challenges, the analysis of power dynamics underscores the asymmetry between the state and citizens, as well as the influence of foreign suppliers. The state's extensive use of surveillance technologies, justified under the guise of countering threats and promoting national security, has led to the violation of privacy rights and curtailed freedom of expression.

The analysis in this paper reveals the disproportionate impact on specific groups, including peaceful activists, opposition politicians, and journalists. The rights to privacy, freedom of expression, and association are consistently undermined, creating a chilling effect on democratic participation. Despite facing these formidable challenges, civil society, media, policymakers, and individuals have shown varying degrees of agency in resisting and challenging the overreach of digital surveillance. In the face of these dynamics, proposals for a comprehensive surveillance law reform, independent oversight, transparency in procurement, and strategic litigation aim to address the shortcomings in the current system, have been proposed. The evolving landscape of digital surveillance in Nigeria necessitates continuous scrutiny, advocacy, and adaptation of legal and policy frameworks.



The state's extensive use of surveillance technologies, justified under the guise of countering threats and promoting national security, has led to the violation of privacy rights and curtailed freedom of expression.

BIBLIOGRAPHY

- ◆ **Action Group on Free Civic Space:** Shrinking Civic Space in the Name of Security, (2022) <https://closingspaces.org/7965-2/>
- ◆ **Amnesty International:** "U.S.-Made Weapons Used by Government of Israel in Violation of International Law and U.S. Law." 2024
- ◆ **Amnesty International:** Vavra, Shannon. "Israeli Court Rejects Request to Revoke NSO Group's Export License." Cyberscoop, July 13, 2020, <https://cyberscoop.com/nso-group-amnesty-international-israel-export/>
- ◆ **Andrew Walker:** United States Institute of Peace, Special Report: What Is Boko Haram? Special Report 308 ~ June 2012, <https://www.usip.org/sites/default/files/SR308.pdf>
- ◆ **AP News:** Anna, Cara. "Nigerian Leader: Islamic Extremists are Now Using Drones." Associated Press, 30 Nov. 2018, <https://apnews.com/>
- ◆ **Australia Group:** "Introduction." The Australia Group. Accessed June 2024
- ◆ **Awka, Titus Eleweke:** "Obiano Inaugurates CCTV Surveillance Cameras in Anambra." 2019. Accessed 27 May 2024, [Obiano Inaugurates CCTV Surveillance Cameras in Anambra. 2019](#)
- ◆ **BBC News:** Abuja attack: Car bomb hits Nigeria UN building, Published 27 August 2011, <https://www.bbc.com/news/world-africa-14677957>
- ◆ **BBC News:** "Boko Haram Crisis: Nigeria Fury Over US Arms Refusal." November 11, 2014 <https://www.bbc.com/news/world-africa-30006066>
- ◆ **BBC:** Nigeria Metele Attack: President Buhari Speaks of Deep Shock." BBC, November 25, 2018, <https://www.bbc.com/news/world-africa-46333126>

- ◆ **Britannica:** "Edward Snowden", retrieved 8 July 2024, <https://www.britannica.com/biography/Edward-Snowden>
- ◆ **Brookings:** Kreps, Sarah. Democratizing Harm: Artificial Intelligence in the Hands of Nonstate Actors. Brookings, Nov. 2021, https://www.brookings.edu/wp-content/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf
- ◆ **BSR:** "Google's Human Rights by Design." November 2019. <https://www.bsr.org/en/blog/google-human-rights-impact-assessment-celebrity-recognition>
- ◆ **Business Day:** Godsgift Onyedinefu. "Senate Demands Probe into \$500m Spent on CCTV Cameras for FCT." November 23, 2023, <https://businessday.ng/news/article/senate-demands-probe-into-500m-spent-on-cctv-cameras-for-fct/>
- ◆ **Business Hilights:** "Can el-Rufai Right FCT, Lagos Wrongs on Spending N2.55Bn on CCTV, Drones?" Business Hilights, 2016. Accessed 27 May 2024.
- ◆ **Carnegie Endowment for International Peace:** "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." 14 Mar. 2023 [Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses - Carnegie Endowment for International Peace](https://www.carnegieendowment.org/policy-analysis/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses)
- ◆ **CBN:** AML Circular and Regulations." Central Bank of Nigeria, cbn.gov.ng
- ◆ **Channels TV:** "ECOWAS Court Declares FG's Twitter Ban Unlawful." CHANNELS TV, July 14, 2022. <https://www.channelstv.com/2022/07/14/ecowas-court-declares-fgs-twitter-ban-unlawful/>
- ◆ **CIA:** "Nigeria - The World Factbook." The World Factbook, 29 Aug. 2024, <https://www.cia.gov/the-world-factbook/countries/nigeria/>
- ◆ **China's Export Controls (2021).** Accessed June 12, 2024
- ◆ **Closing Space:** Space in West Africa: Trends, Threats and Futures (2023); <https://closingspaces.org/civic-space-in-west-africa-trends-threats-and-futures/>

- ◆ **Closing Space: DSS Arrest and Detained Businessman for Expressing Support for IPOB Online - DSS Arrest and Detained Businessman for Expressing Support for IPOB Online**
- ◆ **Committee to Protect Journalists:** August 16, 2018, Nigerian journalist jailed for refusing to reveal source, <https://cpj.org/2018/08/nigerian-journalist-jailed-for-refusing-to-reveal/>
- ◆ **Danish Institute for International Studies:** Rasmussen, Niels Aadal. Chinese Missile Technology: Control – Regime or No Regime? 2007. Accessed June 19, 2024, https://www.files.ethz.ch/isn/29608/nra_chinese_missile_technology_control.pdf
- ◆ **Defence and Security Quarterly:** Unknown gunmen and insecurity in Nigeria: Dancing on the brink of state fragility, Security and Defence Quarterly 2023;42(2):16-34, <https://securityanddefence.pl/Unknown-gunmen-and-insecurity-in-Nigeria-Dancing-on-the-brink-of-state-fragility,163462,0,2.html>
- ◆ **Dennis Broeders:** The Secret in the Information Society, Springer Link, Published:14 April 2016, <https://link.springer.com/article/10.1007/s13347-016-0217-3>
- ◆ **European Commission:** Exporting dual-use items, July 8, 2024 <https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items>
- ◆ **Federal Ministry of Trade and Investment:** “About FMTI.” Accessed May 2024, <https://fmt.gov.ng/about>
- ◆ **Foundation for Investigative Journalism:** "Data and Digital Rights Coalition Addresses Data Censorship and Surveillance in Nigeria." <https://fij.ng/article/data-and-digital-rights-coalition-addresses-data-censorship-and-surveillance-in-nigeria/>
- ◆ **German Council on Foreign Relations (DGAP):** Dr. Georgios Kolliarakis “Anticipatory Governance of Emerging and Disruptive Technologies with Dual-Use Potential.” <https://dgap.org/en/research/publications/anticipatory-governance-emerging-and-disruptive-technologies-dual-use>

- ◆ **Grey Dynamics:** Nigeria Military Equipment 2021. Grey Dynamics Intelligence Series, <https://greydynamics.com/>
- ◆ **Guardian Newspaper:** Emmanuel Akinwotu, Nigeria cracks down on 'end Sars' protesters, alleging terrorism
November 13, 2020
<https://www.theguardian.com/world/2020/nov/13/nigeria-cracks-down-on-end-sars-protesters-alleging-terrorism>
- ◆ **History Class:** Cheta Nwanze A History of Nigeria's Police Service, published in Africa is a Country; Accessed via
<https://Africasacountry.Com/2014/04/Historyclass-Nigerias-Police>
- ◆ **HumAngle:** "How Digital Surveillance Threatens Press Freedom in West Africa." February 24, 2023, <https://humanglemedia.com/how-digital-surveillance-threatens-press-freedom-in-west-africa/>
- ◆ **Human Rights Watch:** "Human Rights Watch Among Pegasus Spyware Targets." 2022, "[Human Rights Watch Among Pegasus Spyware Targets](#)"
- ◆ **Human Rights Watch:** Nigeria" The Dawn of a New Dark " Human Rights Abuses Rampant as Nigerian Military Declares Absolute Power
- ◆ **Human Rights Act 1998**
- ◆ **Human Rights Watch:** "Nigeria: Punitive Financial Moves Against Protesters." November 13, 2020.
<https://www.hrw.org/news/2020/11/13/nigeria-punitive-financial-moves-against-protesters>
- ◆ **International Comparative Legal Guide:** Technology Laws and Regulations in Nigeria 2023-2024. n.d., <https://iclg.com/>
- ◆ **Institute of Development Studies:** ADRN Surveillance Supply Chain Report: Nigeria Country Report. IDS, n.d.,
[ADRN_Surveillance_Supply_Chain_Report_Nigeria_Country_Report.pdf \(ids.ac.uk\)](#)
- ◆ **Institute of Development Studies:** Roberts, T., et al. Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia., 2023, DOI: 10.19088/IDS.2023.027

- ◆ **IPIS Research:** Berman, Eric G. The Management of Lethal Materiel in Conflict Settings: Existing Challenges and Opportunities for the European Peace Facility. IPIS, September 8, 2021, <https://ipisresearch.be/publication/the-management-of-lethal-materiel-in-conflict-settings-existing-challenges-and-opportunities-for-the-european-peace-facility/>
- ◆ **Isaac Olawale Albert:** Terror as a political weapon: reflections on the bomb explosions in Abacha's Nigeria, IFRA Special Research Issue VOL. 1, p. 37-56
- ◆ **ITEdgeNews:** "NITDA Alerts on DDoS Attack Targeting Critical National Digital Infrastructures." 3 Aug. 2023, <https://www.itedgenews.africa/nitda-alerts-on-ddos-attack-targeting-critical-national-digital-infrastructures/>
- ◆ **Latest Nigeria News:** [Businessman arrested by DSS over alleged IPOB comments on social media, lawyer alleges](https://www.latestnigeriannews.com/p/841212/businessman-arrested-by-dss-over-alleged-ipob-comments-on-social-media-lawyer-alleges), accessed on Jul 13, 2023, <https://www.latestnigeriannews.com/p/841212/businessman-arrested-by-dss-over-alleged-ipob-comments-on-social-media-lawyer-al.html>
- ◆ **Leadership Newspaper:** Customs Hands Over Confiscated Fake US Dollars, 148 Drones to EFCC, Army." Leadership, n.d., <https://leadership.ng/>
- ◆ **Leadership Nigeria:** Customs Intercepts Combat-Ready Drone, Military Hardware at MMIA." Leadership, <https://leadership.ng/customs-intercepts-combat-ready-drone/>
- ◆ **Linklaters:** "French Duty of Vigilance Law: First Decision on the Merits Rendered by a French Court." 2023. <https://sustainablefutures.linklaters.com/post/102iuhu/french-duty-of-vigilance-law-first-decision-on-the-merits-rendered-by-a-french-c>
- ◆ **Los Angeles Times:** Allam M. Jalon, A break-in to end all break-ins, March 8, 2006, <https://www.latimes.com/archives/la-xpm-2006-mar-08-oe-jalon8-story.html>
- ◆ **Mojeed, Musikilu:** "Jonathan Procures N11 Billion Equipment to Tap Your Phones." Premium Times, 2015. Accessed 27 May 2024 [Can el-Rufai right FCT, Lagos wrongs on spending N2.55Bn on CCTV, drones?](https://www.premiumtimesng.com/news/local-news/2015/05/27/can-el-rufai-right-fct-lagos-wrongs-on-spending-n2.55bn-on-cctv-drones/)

- ◆ **Michael P. Seng and Gary T. Hunt:** The Press and Politics in Nigeria: A Case Study of Developmental Journalism, p.95, <https://lira.bc.edu/files/pdf?fileid=cad4a6b4-7fad-400f-a514-9309ecd62e4c>
- ◆ **Nairametrics:** Nigeria Spends 418% More Buying Foreign Weapons in 2023." Nairametrics, 2023, <https://nairametrics.com/nigeria-foreign-weapons-spending-2023/>
- ◆ **National Communication Commission:** Guidelines for the provision of internet service. <https://www.ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file>
- ◆ **National Office for Technology Acquisition and Promotion:** "Mandate." Accessed May 2024, <https://notap.gov.ng/>
- ◆ **National Office for Technology Acquisition and Promotion (NOTAP):** Bashir, Toyin, et al. "Regulator Spotlight -" Banwo and Ighodalo, 2024, '[Regulator Spotlight - National Office For Technology Acquisition And Promotion \(NOTAP\)](#)
- ◆ **News Express:** Why terrorism continues despite huge budgetary allocations – Defence Chief <https://newsexpressngr.com/news/211022/why-terrorism-continues-despite-huge-budgetary-allocations-defence-chief>
- ◆ **New York Times Magazine:** What an Uncensored Letter to M.L.K. Reveals, 2014, <https://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html>
- ◆ **Nigeria Customs Service:** "Nigeria Customs Service Act, 2023." Accessed May 2024, <https://nigeriacustoms.gov.ng/>
- ◆ **Nigeria Security and Civil Defence Corps:** Embassies, MDAs and Military – End-User Certificate Portal." Nigeria Security and Civil Defence Corps, n.d., EUC applications by private persons will be routed through the Office of the Commandant General, Nigeria Security and Civil Defence Corps (NSCDC) who would recommend the grant of EUC to ONSA– [Remotely Piloted Aircraft End-User Certificate Portal \(nsa.gov.ng\)](#)

- ◆ **NSO Group:** retrieved 8 July 2024, <https://www.nsogroup.com>
- ◆ **Office of the National Security Adviser:** "Nigeria End-User Certificate Portal." Accessed May 2024, <https://nsa.gov.ng/>
- ◆ **Ogala, Emmanuel:** "Investigation: Bayelsa Governor Hires World's Most Ruthless Hackers for N100M to Hack Computers, Phones in Nigeria." Premium Times, May 27, 2024 accessed via <https://www.premiumtimesng.com/investigationspecial-reports/186391-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-computers-phones-in-nigeria-investigation-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-c.html>. Accessed 27 May 2024.
- ◆ **Orji, Igbeaku:** "Abia to Improve Security, Install CCTV." 2024. Accessed 27 May 2024, Abia to Improve Security, Install CCTV
- ◆ **Paradigm Initiative:** Status of Surveillance in Nigeria: Refocusing the Search Beams. Policy Brief 009, <https://paradigmhq.org/wp-content/uploads/2021/04/Policy-Brief-009-Status-of-Surveillance-in-Nigeria.pdf>
- ◆ **Peter Dauvergne:** Facial recognition technology for policing and surveillance in the Global South: a call for bans. *Third World Quarterly*, 43, 1-11, 2022 10.1080/01436597.2022.2080654
- ◆ **Petersen, Julie K:** Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications. Taylor & Francis Group, LLC, 2000, pp. 1-17. [Dual-Use Technologies and National Security | International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings | The National Academies Press](#) State Government, [Guiding Principles on Government Use of Surveillance Technologies \(state.gov\)](#)
- ◆ **Port News:** Drones Not Allowed Without End-User Certificate – MMIA Customs Boss." PortNews, n.d., <https://portnews.com.ng/drones-end-user-certificate/>

- ◆ **Premium Times:** "Cyberattackers Used US Company to Crash Media Sites in Nigeria, Others." Premium Times, 8 Sept. 2023, <https://www.premiumtimesng.com/news/top-news/623974-cyberattackers-used-us-company-to-crash-media-sites-in-nigeria-others.html?tztc=1>.
- ◆ **Premium Times:** "Elbit Systems Officials Arrive; Begin Installation of \$40 Million Spy Facility for Nigeria." 2013, Elbit Systems Officials Arrive; Begin Installation of \$40 Million Spy Facility for Nigeria
- ◆ **Premium Times:** Emmanuel Ogala, Investigation: Bayelsa Governor forges End User Certificate to procure N100M hacking tools, July 15, 2015 [INVESTIGATION: Bayelsa Governor forges End User Certificate to procure N100M hacking tools | Premium Times Nigeria \(premiumtimesng.com\)](https://www.premiumtimesng.com/news/top-news/218530-boko-haram-caused-fertiliser-scarcity-price-increase-nigerian-govt.html?tztc=1)
- ◆ **Premium Times:** "Exclusive: Nigerians Beware! Jonathan Procures N11 Billion Equipment to Tap Your Phones." 2015.
- ◆ **Premium Times:** "Investigation: How Jonathan Govt. Paid Companies Linked to Doyin Okupe to Hack 'Unfriendly' Websites." 2016, ["INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack unfriendly websites](https://www.premiumtimesng.com/news/top-news/218530-boko-haram-caused-fertiliser-scarcity-price-increase-nigerian-govt.html?tztc=1)
- ◆ **Premium Times:** Mihaiela Buse. "Drones and Terrorism - A New Threat to International Security." Proceedings of the 11th International Conference on Knowledge Management: Projects, Systems and Technologies, Bucharest, November 7-8, 2019. Accessed June 4, 2024.
- ◆ **Premium Times:** "How Boko Haram Caused Fertiliser Scarcity, Price Increase – Nigerian Govt." December 20, 2016. <https://www.premiumtimesng.com/news/top-news/218530-boko-haram-caused-fertiliser-scarcity-price-increase-nigerian-govt.html?tztc=1>
- ◆ **Premium Times:** Ogala, Emmanuel, "U.S. Spy Program Reforms Spotlight Nigeria's Expanding Surveillance Program." Premium Times, 10 Feb. 2014, <https://www.premiumtimesng.com/news/154931-u-s-spy-program-reforms-spotlight-nigerias-expanding-surveillance-program.html>

- ◆ **Premium Times:** "Police Detain EndSARS Activist Eromosele Adene for Days Without Charge – Lawyer." November 10, 2020. , <https://www.premiumtimesng.com/news/headlines/425447-police-detain-endsars-activist-eromosele-adene-for-days-without-charge-lawyer.html?tztc=1>
- ◆ **Premium Times:** Why I was arrested - Chido Onumah | September 29, 2019, <https://www.premiumtimesng.com/news/top-news/355098-why-i-was-arrested-chido-onumah.html>
- ◆ **Press Release:** "Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and Other Malicious Cyber Activities." U.S. Department of Commerce, <https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private>
- ◆ **Punch Newspaper:** Aminu said he was arrested, beaten on Aisha's order – Uncle, November 29, 2022, <https://punchng.com/aminu-said-he-was-arrested-beaten-on-aishas-order-uncle/>
- ◆ **The Punch:** "Bank Customers, Companies Lose Billions to Nigeria's Weak Cybersecurity." April 2, 2023, <https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/>
- ◆ **Punch Newspaper:** [Eniola Akinkuotu, CBN accuses #EndSARS campaigners of terrorism](https://punchng.com/cbn-accuses-endsars-campaigners-of-terrorism/), 11 November 2020 <https://punchng.com/cbn-accuses-endsars-campaigners-of-terrorism/>
- ◆ **Punch Newspaper:** Ojoye, Taiwo. Court affirms IPOB's proscription, designation as terrorist group. January 19, 2018. Accessible at https://punchng.com/court-affirms-ipobs-proscription-designation-as-terrorist-group/#google_vignette
- ◆ **Punch Newspapers:** Sunday Aborishade, NIA gets N4.87bn budget to track, intercept calls, messages, July 12, 2021, <https://punchng.com/nia-gets-n4-87bn-budget-to-track-intercept-calls-messages/>
- ◆ **Quartz:** Abdi Latif Dahir, Quartz, China "gifted" the African Union a headquarters building and then allegedly bugged it for state secrets, January 30, 2018, <https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years>

- ◆ **Researchgate:** Ipadeola, Abosedo. "Cyberethics, Spyware and the War on Terrorism in an Age of Liberal Democracy." ResearchGate, 2014, ['Cyberethics, Spyware And The War On Terrorism in an Age of Liberal Democracy'](#)
- ◆ **Socio-Economic Rights and Accountability Project (SERAP):** "SERAP Sues FG Over Failed Chinese \$460m Abuja CCTV Project." December 1, 2019, <https://serap-nigeria.org/2019/12/01/serap-sues-fg-over-failed-chinese-460m-abuja-cctv-project/>
- ◆ **SMS Broadcaster.** "3 Different Functions of The IMSI Catcher." 2023, 3 Different Functions of The IMSI Catche
- ◆ **Spaces for Change:** "Dialogue on Private Sector and Civic Space in Nigeria." 7 July 2023, <https://spacesforchange.org/dialogue-on-private-sector-and-civic-space-in-nigeria/>
- ◆ **Spaces for Change:** "Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia." Institute of Development Studies, 2023, <https://www.ids.ac.uk/publications/mapping-the-supply-of-surveillance-technologies-to-africa-case-studies-from-nigeria-ghana-morocco-malawi-and-zambia/>
- ◆ **Spaces for Change:** "Pushing Back Against Digital Risks and Threats in Abia State." , <https://spacesforchange.org/pushing-back-against-digital-risks-and-threats-in-abia-state/>
- ◆ **Spaces for Change:** Security Playbook of Digital Authoritarianism, p. 46. 2021, <https://spacesforchange.org/coming-december-8-security-playbook-of-digital-authoritarianism-in-nigeria/>
- ◆ **Spaces for Change:** Policy Brief: Analysis Of The Terrorism (Prevention & Prohibition) Act 2022 (2023), <https://spacesforchange.org/policy-brief-analysis-of-the-terrorism-prevention-prohibition-act-2022/>
- ◆ **Stockholm International Peace Research Institute:** Brockmann, Kolja, et al. The Missile Technology Control Regime at a Crossroads. 2022, https://www.sipri.org/sites/default/files/2022-12/2212_mtc_r_final_report.pdf

- ◆ **The Cable:** Obi-Oyedepo Leaked Audio: A Dangerous Slope, April 3, 2023
<https://www.thecable.ng/obi-oyedepo-leaked-audio-a-dangerous-slope>
- ◆ **The Guardian:** Julia Carrie Wong, The Cambridge Analytica scandal changed the world – but it didn't change Facebook,
<https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>
- ◆ **The New York Times:** “Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker.”
<https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html>
- ◆ **The Nigerian Press:** Michèle Maringues, Current state, Travails and Prospects, contained in Nigeria During the Abacha Years (1993-1998) | 'Kunle Amuwo, Daniel C. Bach, Yann Lebeau at pp p. 185-218,
<https://books.openedition.org/ifra/640?lang=en>
- ◆ **The Open University:** Resource 4: The Aba Women's Riot,
<https://www.open.edu/openlearncreate/mod/oucontent/view.php?id=160512§ion=2.7>
- ◆ **The Pegasus Project:** "Forbidden Stories" Accessed 8 July 2024,
https://forbiddenstories.org/projects_posts/pegasus-project/
- ◆ **The Washington Post:** The Jean Seberg Story -
<https://www.washingtonpost.com/archive/politics/1980/09/05/the-jean-seberg-story/11049a35-bbdb-4aef-ab67-22d06a9e98e5/>
- ◆ **The World:** Reinl, James. “How Stolen Weapons Keep Groups Like Boko Haram in Business.” April 19, 2019,
<https://theworld.org/stories/2019/04/19/how-stolen-weapons-keep-groups-boko-haram-business>
- ◆ **Third World Legal Studies:** The State Security Service and Human Rights in Nigeria -1996-97, <https://core.ac.uk/download/pdf/303859358.pdf>
- ◆ **Thisday Live:** Manufacturers, Importers Groan over Customs' End User Certificate Abuse.” n.d., <https://thisdaylive.com/customs-end-user-certificate-abuse/>

- ◆ **United Nations:** Dr. Fatima Akilu Director, Office of the National Security Adviser Federal Republic of Nigeria at the Sixty-Seventh Session of the UNGA on Measures to Eliminate International Terrorism (AGENDA ITEM 105),
https://www.un.org/en/ga/sixth/67/pdfs/statements/int_terrorism/nigeria.pdf
- ◆ **Vanguard Newspaper:** "FG to Build Multi-Billion Naira GSM Tracking Device for Police." 2010
- ◆ **Vanguard Newspaper:** October 20, 2022, #EndSARS Anniversary: Police mount surveillance at strategic points in Osun,
<https://www.vanguardngr.com/2022/10/endsars-anniversary-police-mount-surveillance-at-strategic-points-in-osun/>
- ◆ **Vanguard Newspaper:** "Insecurity: FG Concessions \$490m CCTV Project - Police Affairs Minister 2022" https://www.vanguardngr.com/2022/12/insecurity-fg-concessions-490-m-cctv-project-police-affairs-minister/#google_vignette
- ◆ **Victoria Ibezim-Ohaeri:** Action Group on Free Civic Space "Security Playbook of Digital Authoritarianism". (2021).
<https://spacesforchange.org/coming-december-8-security-playbook-of-digital-authoritarianism-in-nigeria/>
- ◆ **Victoria Ibezim-Ohaeri:** #ENDSARS: Police Brutality, Protests and Shrinking Civic Space in Nigeria, (2020) <https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/>
- ◆ **Victoria Ibezim-Ohaeri:** "Galvanizing Collective Action to Protect the Civic Space in Nigeria." Shehu Musa Yar Adua Foundation.
<https://www.yaraduafoundation.org/files/Galvanizing%20Collective%20Action.pdf>
- ◆ **Victoria Ibezim Ohaeri:** "Security Playbook of Digital Authoritarianism." Action Group on Free Civic Space, 2021. spacesforchange.org/coming-december-8-security-playbook-of-digital-authoritarianism-in-nigeria/

- ◆ **United Nations Office on Drugs and Crimes (UNODC):** User's Guide to the Terrorism (Prevention) Act, 2011 (TPA) as amended by the Terrorism (Prevention) (Amendment) Act, 2013 (TPAA) Published 2021:
https://www.unodc.org/conig/uploads/documents/UNODC_Users_Guide_to_Terrorism.pdf
- ◆ **United Nations:** "Pegasus: Human rights-compliant laws needed to regulate spyware." 2021, <https://operationalsupport.un.org/en/pegasus-human-rights-compliant-laws-needed-to-regulate-spyware>
- ◆ **United Nations:** "Preventing Terrorists from Acquiring Weapons." Accessed June 2024, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf
- ◆ **University of Cambridge:** "Dual-Use Goods, Technology and Software." Import Export Hub, <https://www.importexport.admin.cam.ac.uk/controlled-goods-licences-and-sanctions/dual-use-goods-technology-and-software>
- ◆ **U.S Department of State:** "Missile Technology Control Regime." NTI, Accessed June 2024, <https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/missile-technology-control-regime-mtcr-frequently-asked-questions/>
- ◆ **U.S. Department of State:** "Nigeria Country Report on Human Rights Practices for 1996." Released by the Bureau of Democracy, Human Rights, and Labor, 30 Jan. 1997
- ◆ **Western Balkans Cybersecurity Research Network:** Online Actions, Offline Harms: Case studies on Gender and Cybersecurity in the Western Balkans, Geneva Center for Security Governance (October 2023), https://www.dcaf.ch/sites/default/files/publications/documents/Online-actions-offline-harms_EN-2nov2023.pdf
- ◆ **Zimperium:** "IMSI Catcher." Zimperium, <https://www.zimperium.com/glossary/imsi-catcher/>

SPACES FOR CHANGE | S4C



TELEPHONE:

+234 703 620 2074

+234 909 453 9638

EMAIL:

Info@spacesforchange.org

spacesforchange.S4C@gmail.com

 **@Spaces4Change**

 **@Spaces4Change**

 **@SpacesforChange.S4C.**

www.spacesforchange.org