SPACES FOR CHANGE | S4C

RESEARCH | POLICY | CITIZEN ACTION

EXECUTIVE SUMMARY

The PROLIFERATION OF DUAL-USE SURVEILLANCE TECHNOLOGIES IN NIGERIA:

Deployment, Risks and Accountability

Supported by:

Spyware Accountability Initiative

Ford Foundation

SEPTEMBER 2024

Summary of Findings

The word “dual-use” is rooted in a distinction between 'benign' versus 'malign', or 'civil' and 'military' uses. Dual-use technologies (DUTs) 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.'[1] 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.[2]

Technology-dependent countries like Nigeria look to other countries to supply them with technological equipment and other digital infrastructure that can enhance its intelligence-gathering, service delivery and security interventions. Companies and tech-exporting countries are obligated to satisfy relevant licensing, entry clearance, export controls and end-user certification requirements for the importation of spyware technologies into Nigeria. Little is known about the licensing conditions and domestic controls for the importation of surveillance technologies, their end-use requirements, and the regulatory architecture for the enforcement of these requirements. Their dual-use characteristics, compounded by inadequate importation controls for dual-use goods, have not only made regulation difficult but also exacerbated their potential for exploitation, repurposing and outright misuse.

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

To what extent can watchdogs leverage the export-controls of supplier countries to demand accountability for the surveillance-linked human rights abuses as well as the reform of spyware trade? Here are our main findings:

1. Nigeria grapples with numerous security challenges and has procured technologies to help combat criminality: Nigeria grapples with diverse security challenges such as terrorism and violent extremism, banditry, farmer-herder conflicts, secessionist agitations, kidnapping, and road robbery. To tackle these security challenges, the government has massively procured an array of technological equipment over the years to help combat criminality and increase national capacities in intelligence operations, information gathering, monitoring and tracking of criminal elements, etc.[3]

2. Walking in America's footsteps: America's 'securitization' of the response to the 9/11 attacks on the Twin Towers created the foundations for the massive expansion of anti-terrorism frameworks (including surveillance initiatives) over the following 20 years. 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,[4] 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.

3. Surveillance is enabled by law and other multiple drivers: Apart from national security, there are several drivers of surveillance ranging from inherent colonial policing systems, military rule hangover, profitable spyware trade, population explosion, and increasing authoritarianism etc. Most importantly, surveillance is legally-permissible under numerous statutes that permit the derogation of certain human rights, including the right to privacy, under certain circumstances such as (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. 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.[5]

3. 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/
4. Britannica: "Edward Snowden", https://www.britannica.com/biography/Edward-Snowden, retrieved 8 July 2024
5. 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/

4. Despite legal safeguards for privacy rights, interceptions, data breaches and privacy intrusions persist: Certain legal safeguards have been inserted to preserve the right to privacy of residence and correspondence protected under Section 37 of Nigeria's 1999 Constitution. These safeguards are contained in numerous legal provisions inserted into the Data Protection Act 2023 (NDPA), Consumer Code of Practice Regulations 2007 (NCC Regulations), Child Rights Act 2003, Freedom of Information Act, 2011 (FOI Act), Cybercrimes (Prohibition, Prevention Etc.) Act 2015 (as amended), National Identity Management Commission (NIMC) Act 2007, etc. 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 empowers law enforcement to bring all sorts of misdemeanors under the purview of each law.

5. An array of dual-use technologies is imported regularly into Nigeria by state actors: 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. Surveillance technologies have aided in tackling insecurity such as tracking terrorists, kidnappers, money launderers, drug traffickers, and human traffickers.[6]

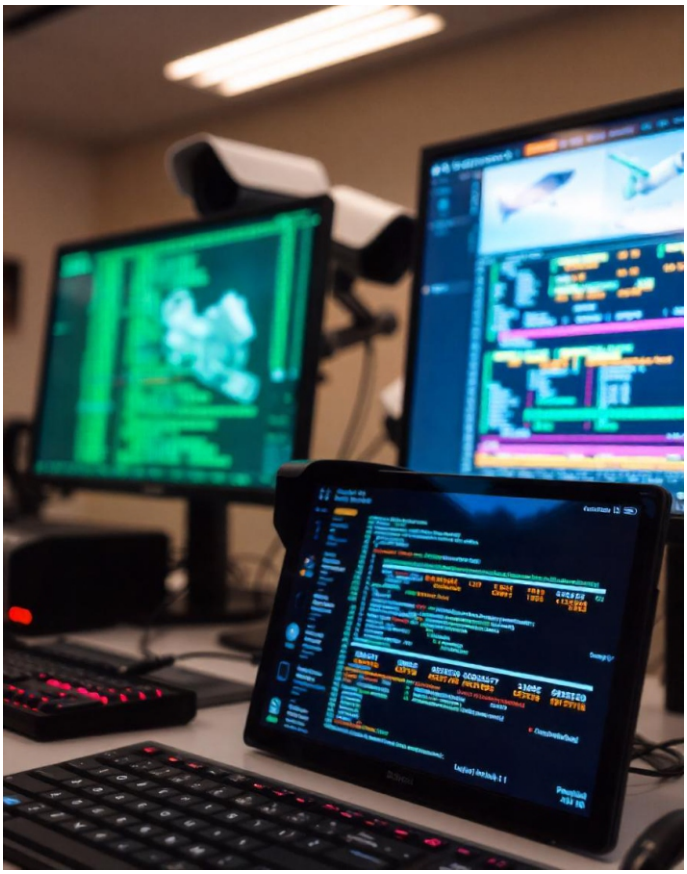
6. The Battle for the Worlds Most Powerful Cyberweapon - The New York Times (nytimes.com)

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. 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.

6. **Repurposing and diversion of spyware (DUTs)**: While these technologies have significantly enhanced the country's security landscape, their potential for repurposing and diversion of security-based technologies is alarmingly high. Surveillance technologies have been used arbitrarily for the following purposes unrelated to security:

- Spying on politicians and regime opponents
- Attack, infect, and monitor target personal computers and smart phones in a stealth way
- Track and intercept private mobile communications
- Intercept the traffic of mobile phones and can track mobile phone users' location data
- Spying on citizens' computers and online communications
- Compulsorily collect biometric and other biological data of citizens on a mass scale
- Track the exact position of a user, even when abroad. This has been used to track the locations of vocal critics, journalists and public commentators for the purpose of arrest and detention
- Social media monitoring
- Compromise most operating systems, except iOS, encrypted computers and smartphones, even if the target was outside the government's "monitoring domain"
- Surveilling financial records of protesters leading to account blocks and freezes.

7. Technologies popularly used for surveillance include: C4i (Command, Control, Communications, Computers, and Intelligence); Hacking Team and FinFisher; Remote Control System (RCS); GSM Tracking System; Digivox, Distributed Denial of Service (DDoS) using Proxy Internet Protocol (IP) addresses and virtual private networks (VPN); International Mobile Subscriber Identity (IMSI) Catcher; Wise Intelligence Technology (WIT); biometric- and Data Collection Initiatives and so forth.



8. Countries like Israel, China and United States are top suppliers of the technologies imported and often arbitrarily used in Nigeria. 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. Examples of suppliers include Italy's Hacking Team, Netherland's Digivox, US-based Rayo Byte's Proxy Internet Protocol (IP) addresses and virtual private networks (VPN) services, China's IMSI Catcher, Israeli Elbit Systems' Open Source Intelligence (OSINT) solution and Elbit Systems' PC Surveillance Systems (PSS), ADS Aerostar UAV, Circles, C4i, and Wise Intelligence Technology (WiT)), China's CASC CH-3A armed

tactical unmanned aerial vehicle (UAV), Mugin commercial UAV, DJI Phantom and ZTE's Video Surveillance Subsystem (VSS) and biometric ID technologies from Thales (France/Singapore), Dermalog Identification (Germany), BIO-key (USA), and Chongqing Huifan (China).

9. Non-state actors are also involved in spyware abuse: 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. There is evidence that terrorists mostly plan their attacks employing one form of communication or information technology or the other.[7] Boko Haram has begun using drones for surveillance, though authorities fear they will rapidly progress to weaponized platforms.[8] As extremist 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.[9]

10. Nigerian law allows only four categories of importers of controlled items: The regulation of spyware transpires at the import and export points. As an importing country, domestic regulation mainly takes the form of import controls. 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.[10]

EXECUTIVE SUMMARY

7. Ipadeola, Abosede. "Cyberethics, Spyware and the War on Terrorism in an age of Liberal Democracy" Researchgate (2014)

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

9. Cara Anna, ibid

10. 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)

11. Office of the National Security Adviser's (ONSA's) End-User Certificate is the principal import control measure: 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).[11] 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. 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.[12] 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. [13]

12. ONSA maintains a list of 'controlled importation': This list contains surveillance technologies and items typically required by the military. It also contains 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). There are about 262 controlled items and products which requires EUCs for their importation into the country.[14]

13. ONSA List excludes several dual-uses technologies: Many DUTs are excluded from ONSA's control lists, leaving an evident gap in regulation that could be potentially exploited. As such, the requirement for EUC does not apply to the importation of any surveillance technology that is not contained on the list. 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.

14. Excluded dual-use technologies can be exploited in the following ways:

- **By non-security agencies,** including MDAs when they are imported exclusively for civilian purposes, but may be diverted to military and other repressive uses.

11. Office of the National Security Adviser, "Nigeria End-User Certificate Portal" Accessed – May 2024
12. Ibid
13. Ibid
14. NSA, Full HS Codes- End User Certificate: List of Controled Items and Products. Accessed June 5, 2024

- **By private companies:** It is also possible for private companies and individuals to bypass monitoring by ONSA through the importation and surveillance technologies that are not on the ONSA list.

- Evidence shows that states collude with private actors—especially private telecommunication companies — to achieve their surveillance objectives.[15] In certain circumstances, collusion or cooperation to surveil between the state and private companies are imposed by statutes.[16]

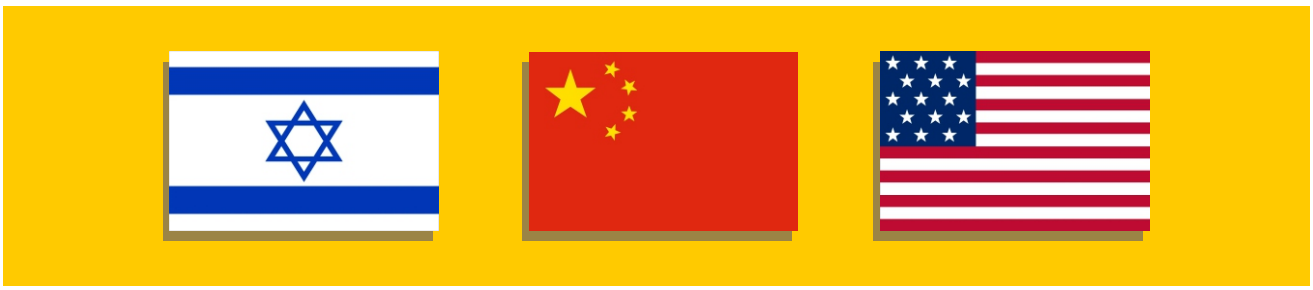
  By non-state armed groups: Reporting suggests that Boko Haram factions in Nigeria have seized contingent-owned equipment (COE) that includes a wide-range of heavy weapon systems. Terror groups have also raided military bases killing soldiers[17] and made off with weapons belonging to peacekeeping missions and militaries.[18] The likelihood of terrorists taking away and diverting surveillance equipment imported for military uses to outright terrorist activities, causing massive harm to civilian populations 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.[19]

15. Regulations governing the importation of DUTs, including surveillance technologies: There are five principal legislations governing the importation of surveillance and other dual use technologies into Nigeria. They are the ONSA's End User Certificate (EUC) regime, the National Office for Technology Acquisition and Promotion (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.

15. Victoria Ibezim-Ohaeri et al, Action Group on Free Civic Space "Security Playbook of Digital Authoritarianism". (2021)
16. See sections 146 – 149 of the Nigerian Communications Act 2003
17. BBC, Nigeria Metele attack: President Buhari speaks of deep shock, November 25, 2018, https://www.bbc.com/news/world-africa-46333126
18. 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
19. James Reinl, IPIS, ibid.

16. 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. Israel entered into a bilateral agreement with India to "promote innovation in startups and MSMEs of both countries for development of dual use technologies."[20] 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.[21] 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.[22]

17. Export control regimes for dual-use technologies in Nigeria's top supplier countries: The export control measures in Nigeria's major supplier countries show that Israel, United States and China have relatively 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 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

20. pib.gov.in/PressReleaseIframePage.aspx?PRID=1770299
21. Ibid.
22. Chinas pursuit of dual-use technologies (iiss.org)

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, inspects, audits and slams 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.

International Export Control Regimes: The USA also leads advocacy for the regulation and enforcement of export controls on DUTs. U.S. control lists are consistent with the lists maintained by the various multinational export control regimes such as 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.[23] 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. Although Israel[24] and China[25] 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. Others include the Missile Technology Control Regime (MTCR), Australia Group (AG), Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC).

23. Home - The Wassenaar Arrangement
24. Privacy Shield Framework, Israel-US Export Control. Accessed June 5, 2024
25. Article 1, ECL

18. As elaborate as export control regimes are, certain limitations inhibit their effectiveness. One such limitation is that human rights considerations lack clarity and consistency. 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.[26] Compare the above stance to the American-supplied weapons which the government of Israel has used to commit serious violations of international humanitarian and human rights law, and in a way that is inconsistent with U.S. law and policy.[27]

Secondly, countries' export control regimes are primarily influenced by national security considerations. 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 Security[28]—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.

Thirdly, African states, including Nigeria are spending over $1bn per year on digital surveillance technologies imported from countries like the U.S., UK, China etc.[29] 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.

Fourth, how contracts for the acquisition of surveillance technologies 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

26. Boko Haram crisis: Nigeria fury over US arms refusal - BBC News
27. Amnesty International, ""U.S.-Made Weapons Used by Government of Israel in Violation of International Law and U.S Law. (2024)
28. Israels Spy-Tech Industry Is a Global Threat to Democracy (jacobin.com)
29. 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

corruption, fraud, and misuse of public funds, weakening domestic financial systems and reducing public confidence in government. A combination of these dysfunctions poses a disadvantage for developing countries like Nigeria procuring surveillance technologies and weakens their agency to negotiate favorable deals.

Fifth, 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. 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.

Sixth, 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.

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

19. How dual-use surveillance technologies impacts human rights and the civic space in Nigeria: Surveillance enables state repression and infringes personal privacy. 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. Outcomes of surveillance could also be used to blackmail civic space actors, such as by threatening to reveal intimate information or images illegally obtained through surveillance. 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. 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, installs apathy. Lastly, Surveillance forces activists to resort to self-censorship and self-exile.

20. Recommendations for addressing misuse of surveillance technologies include

Need for a Comprehensive Legal Framework and Independent Regulator: 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.

Because ONSA is itself an importer of military equipment and DUTs, its role in overseeing the issuance and implementation of import controls is conflicted on account of its multiple roles as a user, importer and regulator, all at once. 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.

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. In other words, 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.[30]

Transparency: To further ensure accountability, regulators should implement transparency requirements. The opacity in the industry is still a source of concern. 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"[31] 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. A similar parliamentary oversight, backed up with periodic reporting cycle, (monthly) in Nigeria would accelerate the country's effort toward attaining transparency in the enforcement of import controls.

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 such as Export Controls and Human Rights Initiative's Code of Conduct 2023,[32] Summit for Democracy 2023's Guiding Principles on Government Use of Surveillance Technologies[33], Summit for Democracy 2024's Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware and the Global Network Initiative's Global Principles on Freedom of Expression and Privacy.[34]

Human Rights by Design: 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.[35] 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.

30. UN Guiding Principles on Business and Human Rights: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
31. Regulation - 2021/821 - EN - EUR-Lex (europa.eu)
32. 230303 Updated ECHRI Code of Conduct - FINAL (state.gov)
33. 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.
34. GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf (globalnetworkinitiative.org)
35. Jonathon Penney, Sarah McKune, Lex Gill and Ronald J. Deibert, ADVANCING HUMAN-RIGHTS-BY-DESIGN IN THE DUAL-USE TECHNOLOGY INDUSTRY, Journal of International Affairs, Vol. 71, No. 2, UNGOVERNED SPACES (SPRING/SUMMER-2018), pp. 103-110 (8 pages)

SPACES FOR CHANGE | S4C

TELEPHONE:

+234 703 620 2074
+234 909 453 9638

EMAIL:

spacesforchange.S4C@gmail.com
Info@spacesforchange.org

@Spaces4Change

@Spaces4Change

@SpacesforChange.S4C.

www.spacesforchange.org