Issue #4

INTEL WATCH

August 2025

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

DO YOU KNOW WHO'S WATCHING YOU? WE'RE HERE TO HELP YOU FIND OUT

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH MANUAL

BUILDING DIGITAL RESILIENCE MANUAL

EXECUTIVE SUMMARY

Electoral disinformation has sown disorder across Sub-Saharan Africa, damaging electoral integrity, social cohesion, and public trust in democratic norms and institutions. This guide offers a practical and context-specific roadmap to understanding and combating electoral disinformation in the region. While grounded in regional and international best practice, it dismantles the often "Global North"-lensed assumptions about information disorders. And instead, foregrounds the lived realities, vulnerabilities, and technological patterns specific to the region and its countries.

Part One of the guide unravels the **WHAT, WHO, WHY, AND HOW** of electoral disinformation:

- **WHAT:** The Conceptual Frameworks of Disinformation: What is disinformation? What are the different types of disinformation? What are its theoretical frameworks? Guidance is provided to aid in distinguishing disinformation from other information disorders, as well as from political propaganda.

- **HOW and WHY:** Cultural and Social Drivers: How do local contexts and specific social, political, and cultural contexts of individual countries shape susceptibility to disinformation?

- **HOW and WHY:** Psychological Drivers: Why does disinformation resonate so deeply and undermine trust in institutions, media, and truth?

- **HOW and WHY:** Technical Drivers: How are social media platforms and recommender algorithms and other design choices exploited by malign actors to amplify falsehoods at scale?

- **WHO: Actors and Tactics:** Who is spreading disinformation, and what strategies, both covert and overt, are they using to sway public opinion or disrupt democratic processes?

Part Two outlines the **HOW TO**, a practical roadmap for countering electoral disinformation. It includes:

- Establishing Electoral Disinformation Response Teams: Practical guidance on the essential roles and skills needed to monitor and combat disinformation, along with advice on building partnerships with organisations already working in the information integrity space in Sub-Saharan Africa.

- Digital Ecosystem Statistics: Guidelines for mapping national-level vulnerabilities, including gaps in digital access, weaknesses in the media landscape, and disinformation risks. Guidance is also provided on how to factor in the unique social and cultural conditions of each country as part of this process.

- Using Social Media Analytics (SMA) to Monitor Misinformation: A proactive and reactive strategy that covers (1) collecting and analysing social media data, (2) a recommended SMA workplan covering the lead-up, during, and after an election is held.

- A **substantial annex** is included to reinforce the guide's key learnings. It features:

- A comprehensive glossary of terms commonly used in the counter-disinformation field. In addition, the footnotes were specifically chosen to include text that explains the various concepts and issues extensively for those requiring deeper explanation

- Case studies of electoral disinformation monitoring projects from various African countries.

- Recommended books and articles offering deeper insights into the theoretical and technical foundations of disinformation and associated topics.

- A curated selection of similar electoral disinformation guides developed by international organisations.

RECRUITMENT: RESEARCH AND JOURNALISM DIRECTOR, INTELWATCH

Intelwatch is a recently launched non-profit organisation based in South Africa and working internationally. We aim to promote democratic oversight of state and private intelligence agencies. We do this by monitoring and reporting on surveillance activities, raising awareness of the risks of undemocratic intelligence and surveillance activities, and advocating for progressive laws and policies that safeguard fundamental rights.

Intelwatch seeks to appoint a Research and Journalism Director to undertake this work. This is a one year long remote position with the possibility of renewal depending on performance in the role and if funds permit. Despite this being a remote role, applicants must have permission to work in South Africa or via consultancy.

JOB DESCRIPTION

- The Research and Journalism Director is responsible for, inter alia, leading the development of strategic research and journalism projects, managing journalism and research projects and conducting research and journalism, ensuring strategic communication, ensuring popular education and mobilisation materials are developed and maintained, and supporting national strategic partnerships.

RESPONSIBILITIES

- The responsibilities of this role include, amongst others:
- Maintaining a knowledge of key environmental trends and developments impacting on Intelwatch and commissioning and conducting research on those issues.
- Identifying strategic research and journalism projects to support advocacy interventions.
- Identifying exploratory journalism and research interventions that fall within Intelwatch's mandate.
- Identifying strategic research and journalism projects and implement them, either through managing commissioned researchers and journalists, or conducting research or journalism.
- Ensuring that clear messages are developed based on the research and journalism and consistently communicated in appropriate forms to appropriate audiences.

- Ensuring that Intelwatch's research and journalism finds a wide audience, including audiences that are strategically important to changing policy and laws.
- Spearheading the development and use of a wide range of communication channels to publicise the findings of research and journalism.
- Ensuring that the research and journalism work of Intelwatch is well documented.
- Ensuring that Intelwatch responds timeously to developments impacting thematic areas.
- Developing popular education and mobilisation materials with relevant stakeholders, based on the research and journalism and ensuring that these are used in Intelwatch's work.
- Maintaining a knowledge of and relationships with critical organisations whose work impacts on the research and journalism aspects of Intelwatch.
- Exploring and developing cooperation with relevant stakeholders.

QUALIFICATIONS AND REQUIREMENTS

The ideal candidate will have the following:

- At least five years' experience in senior positions in the non-profit field.
- A relevant degree (preferably post-graduate)
- A commitment to the principles underpinning Intelwatch's work, including freedom of expression, democratic participation, and accountable governance.
- A strong track record in research, journalism, advocacy, coordination and capacity-building.
- Experience in stakeholder engagements.
- Experience in popular education
- Experience in developing, implementing and overseeing strategic research, journalism and advocacy campaigns and processes.
- Strong organisational management skills.
- Strong Strategic Communication skills
- Excellent communication skills.

TO APPLY

To apply, please send a CV and covering letter to apply@intelwatch.org.za by 30 September 2025.

If you have not been contacted within two weeks of the closing date, please consider your application as having been unsuccessful.

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

GOOGLE CONFIRMS IT HAS BEEN HACKED — WHAT USER DATA HAS BEEN STOLEN?

IMAGE SOURCE: FORBES

Google has confirmed that hackers linked to the ShinyHunters/UNC6040 group breached one of its corporate Salesforce databases in June 2025, successfully stealing customer contact details and sales notes related to small and medium business prospects. The attack was conducted via sophisticated voice phishing (vishing), tricking employees into authorizing access for a malicious version of Salesforce's Data Loader application. While Google states that no sensitive payment, Google Account credentials, or personal advertising data were compromised, the stolen records—business names, phone numbers, and sales-related information—could enable follow-up social engineering attacks. Google quickly terminated access, performed impact assessments, implemented additional security measures, and completed notifications to affected parties by August 8, 2025. The incident underscores growing risks from social engineering, especially targeting cloud platforms, and highlights the commercial value of even allegedly "basic" CRM data when misused - Forbes

SOPHISTICATED DEVILSTONGUE WINDOWS SPYWARE TRACKING USERS GLOBALLY

IMAGE SOURCE: CYBER SECURITY NEWS

DevilsTongue is a highly sophisticated Windows-based spyware developed by the Israeli firm Candiru, also known as Sourgum, which has been active since at least 2019. It exploits zero-day vulnerabilities in Windows and browsers such as Chrome and Internet Explorer to gain stealthy, kernel-level access to infected devices. The spyware uses advanced persistence techniques like COM hijacking and a signed third-party driver to run covertly in memory, evade detection, and maintain system stability. Once deployed, DevilsTongue can exfiltrate sensitive data including files, credentials, encrypted messages from apps like Signal, and browser cookies, enabling attackers to impersonate victims online. It is primarily used by government clients to target high-value individuals such as politicians, activists, and journalists across multiple countries worldwide. Its deployment infrastructure spans several active clusters linked to countries including Saudi Arabia, Hungary, and Indonesia, demonstrating ongoing operations despite international sanctions against Candiru. The malware's complexity and targeted use underline its significant threat to privacy and national security - Cyber Security News

INTEL WATCH

Watching the watchers. Guarding the guardians.

ANDROID SPYWARE POSING AS ANTIVIRUS: FAKE SECURITY APP TRICKS USERS AND STEALS DEVICE DATA

IMAGE SOURCE: DIGWATCH

Android spyware posing as antivirus apps is a growing cybersecurity threat in 2025, where malicious actors distribute fake security applications to trick users into installing spyware on their devices. These fake antivirus apps appear legitimate and lure users by promising protection but instead gain unauthorized access to sensitive data, monitor activities, and sometimes install additional malware. The spyware often arrives through phishing campaigns, malicious websites, or third-party app stores outside Google Play. Despite Android's built-in security and Google Play's strict app vetting, users remain vulnerable, especially when sideloading apps. Independent security tests highlight the importance of using certified and reputable antivirus software to ensure genuine protection, while users are advised to maintain vigilance, avoid suspicious downloads, and update devices promptly to minimize risks.Android spyware disguised as antivirus apps is an increasing threat in 2025, where malicious apps trick users into installing spyware that steals sensitive data and monitors device activities. These fake antivirus apps are distributed via phishing, malicious sites, or third-party stores and can evade detection by appearing legitimate. Despite Android's built-in protections and Google Play's app vetting, users remain vulnerable when sideloading apps. Experts stress using certified security apps and advise users to avoid suspicious downloads and keep devices updated to reduce risks. - DigWatch

---

JOURNALISTS GET NEW SPYWARE PROTECTIONS IN LANDMARK EU MEDIA LAW

IMAGE SOURCE: CYBER SECURITY NEWS

The European Union has enacted the landmark European Media Freedom Act (EMFA), which provides unprecedented legal protections for journalists across all 27 member states, including stringent safeguards against government spyware and surveillance. The law explicitly prohibits authorities from compelling journalists to reveal their sources and severely restricts the deployment of surveillance technologies against media workers, enhancing press freedom and media independence amid growing concerns over political interference and attacks on journalists. EMFA also mandates increased transparency in media ownership and state advertising, and requires digital platforms to avoid arbitrary censorship of independent media content. Despite broad support within the EU Parliament, successful implementation depends on member states fully adopting the law and effectively enforcing its provisions, as many countries face challenges in aligning national legislation. The creation of the European Board for Media Services will oversee enforcement, aiming to uphold democratic values by protecting media pluralism and safeguarding journalists from digital threats in an increasingly hostile environment - Courthouse News service

AI CHATBOTS AND FACIAL RECOGNITION: PRIVACY IN PERIL

IMAGE SOURCE: OPEN TOOLS

The integration of AI chatbots and expanded use of facial recognition technology by law enforcement have intensified concerns over privacy, surveillance, and data security. AI chatbots such as ChatGPT and Meta's bots employ emotional tactics that exploit user trust to gather extensive personal data, often without users fully understanding the risks or consenting to data collection. Facial recognition technologies raise profound privacy issues due to their ability to track individuals continuously and the potential for misidentification, bias, and chilling effects on free expression. Corporate policies, exemplified by companies like Meta, often lack transparency and have been criticized for inadequate privacy safeguards, leading to calls for stronger regulation and clearer user controls. The erosion of digital privacy is seen as part of a broader trend where AI-enabled surveillance tools increasingly threaten fundamental rights, necessitating urgent legal and policy responses to safeguard personal data in this evolving technological landscape - Open Tools

JOURNALISTS GET NEW SPYWARE PROTECTIONS IN LANDMARK EU MEDIA LAW

IMAGE SOURCE: BAR & BENCH

The rapid integration of AI-driven policing technologies in India, including predictive policing algorithms, facial recognition systems, and social media monitoring tools, poses serious threats to civil liberties, procedural fairness, and democratic governance. These technologies operate with minimal transparency, oversight, or legal safeguards, leading to widespread surveillance without consent, algorithmic bias that disproportionately affects marginalized communities, and violations of privacy and due process. Facial recognition error rates vary widely across demographics, raising concerns about wrongful targeting. The current legal framework is inadequate, as existing laws and guidelines fail to regulate AI's use in law enforcement effectively. Supreme Court rulings emphasize the right to privacy and due process, but AI tools often circumvent these protections. The article calls for a moratorium on AI policing until robust judicial oversight, algorithmic transparency, and anti-bias measures are established to prevent AI-driven erosion of democracy and human rights in India - Bar & Bench

REPRESSION MONITOR

SPYWARE INSTALLED ON KENYAN FILMMAKERS' PHONES IN POLICE CUSTODY

IMAGE SOURCE: COMMITTEE TO PROTECT JOURNALISTS

Two Kenyan filmmakers had spyware, specifically commercially available FlexiSPY, installed on their phones while the devices were in police custody following their arrest in May 2025 on allegations related to publishing false information. Forensic analysis by Citizen Lab confirmed the installation occurred around May 21, while police held the devices. The filmmakers and two others were released without charge, but their electronic devices were withheld for over two months. The spyware enables covert monitoring of messages, calls, location, and other private data, raising serious concerns about press freedom and the safety of journalists' devices under Kenyan law enforcement. Police accused the filmmakers of involvement in a BBC documentary criticizing Kenyan security forces, though the BBC denied their involvement. The case remains under investigation with courts granting multiple extensions. Authorities have yet to respond to calls for transparency regarding the spyware installation - Committee to Protect Journalists

FRESH CONCERNS OVER IMPACT OF UGANDA'S EXPANDING DIGITAL SURVEILLANCE

IMAGE SOURCE: BIOMETRIC UPDATE

Uganda's expanding digital surveillance apparatus is raising fresh concerns over its impact on journalists, civil society, and human rights defenders, as documented in recent reports. Incidents like the targeted phone confiscations and spyware attacks against journalist Canary Mugume illustrate a broader pattern of government-led surveillance that threatens privacy, free expression, and safety. The government has invested heavily in technologies such as the Huawei Safe City facial recognition system, biometric SIM card registration linked to national IDs, real-time vehicle tracking via digital number plates, and extensive social media monitoring. These tools give security agencies unprecedented power to monitor, identify, and target critics, often without adequate legal oversight, contributing to fear, self-censorship, and disruptions in civil society activities. Digital rights advocates call for urgent legal reforms, stronger independent oversight, and transparency from technology providers to protect digital rights and prevent abuses amid Uganda's shifting political landscape ahead of the 2026 elections - Biometric Update

INTEL WATCH

Watching the watchers. Guarding the guardians.

NEW REPORT DETAILS SURVEILLANCE AND SPYWARE NETWORK THAT IS ENDANGERING JOURNALISTS AND HUMAN RIGHTS ACTIVISTS

IMAGE SOURCE: BHRRC

A recent report by Unwanted Witness exposes a widespread surveillance and spyware network in Uganda targeting journalists, human rights defenders, activists, and opposition politicians, severely endangering their safety and freedom of expression. The report highlights attacks like physical assaults and phone confiscations aimed at stealing sensitive data, often linked to government-backed spyware programs. It documents extensive use of surveillance technologies—including the Huawei Safe City project with facial recognition cameras, mandatory biometric SIM registration linked to national IDs, and social media monitoring—that facilitate real-time tracking, harassment, self-censorship, and intimidation. This unchecked surveillance environment has led to media closures, journalist arrests, and pervasive fear that hampers civil society activities, as security agencies wield expanded powers without sufficient oversight. The report calls for urgent reforms to protect digital rights, uphold privacy, and safeguard the democratic space ahead of Uganda's 2026 elections - BHRRC

REPORT: JORDANIAN HUMAN RIGHTS DEFENDERS AND JOURNALISTS HACKED WITH PEGASUS SPYWARE

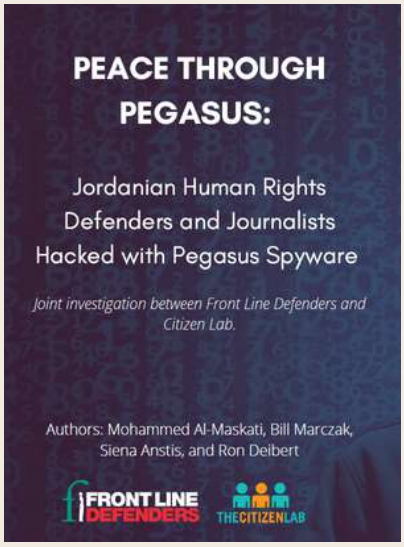

IMAGE SOURCE: FRONT LINE DEFENDERS

A digital forensic investigation by Front Line Defenders and Citizen Lab uncovered Pegasus spyware on the phones of four Jordanian human rights defenders, including a woman activist, lawyer, and journalist, with two Pegasus operators linked to the Jordanian government identified. The spyware facilitated intrusive surveillance of activists working against corruption in Jordan, underscoring the hostile environment for human rights defenders facing government repression. The findings revealed ongoing Pegasus hacking on Apple devices despite legal actions against NSO Group, highlighting the persistent threat posed by such spyware. The report calls on Jordanian authorities to cease digital harassment, urges Apple and hosting company Dreamhost to improve spyware detection and prevention, and demands a global moratorium on surveillance technology sales until enforceable human rights standards and accountability mechanisms are established - Front Line Defenders

INTEL WATCH

Watching the watchers. Guarding the guardians.

NEW REPORT EXPOSES AFRICAN 'SMART CITIES' AS HUBS FOR DIGITAL SURVEILLANCE.

IMAGE SOURCE: THE OBSERVER

Ethiopian Prime Minister Abiy Ahmed's government has been weaponizing digital tools to silence critics and control public discourse by heavily investing in advanced digital monitoring and sentiment analysis technologies. These tools enable proactive surveillance of online communication, social media, and digital platforms to detect dissent, monitor opposition, and suppress critical voices, thus restricting freedom of expression and political opposition. This strategy is embedded within the broader "Digital Ethiopia 2025" initiative, which seeks widespread digital transformation but also raises significant concerns about surveillance, political repression, and the erosion of civil liberties in the country - Borkena

INDIA'S DATA PROTECTION ACT: A SHIELD FOR PRIVACY OR A TOOL FOR STATE SURVEILLANCE?

IMAGE SOURCE: TECH POLICY

India's Digital Personal Data Protection Act, enacted in 2023, aims to safeguard citizens' personal data by defining the rights of individuals (data principals) and obligations of entities handling data (data fiduciaries). It mandates verifiable consent for data processing, especially for children and persons with disabilities, and requires data fiduciaries to implement security safeguards, ensure data accuracy, notify breaches, and erase data when no longer needed. The act also establishes a Data Protection Board to enforce compliance and handle grievances. However, it includes broad exemptions for government agencies and activities related to national security, public order, and law enforcement, allowing significant scope for state surveillance. These exemptions, along with the government's power to exempt certain data fiduciaries temporarily or indefinitely, have raised concerns about the act potentially serving as a tool for state surveillance rather than fully protecting privacy rights. The law balances privacy with legitimate state interests but has been criticized for lacking stringent oversight mechanisms to prevent misuse - Tech Policy

INTEL WATCH

Watching the watchers. Guarding the guardians.

KREMLIN USES LOCAL PROVIDERS TO INSTALL SPYWARE

IMAGE SOURCE: INNOVATION ORIGINS

The Kremlin-linked cyber espionage group Turla, part of Russia's Federal Security Service (FSB), is exploiting its control over local Russian internet service providers (ISPs) to install spyware on the computers of diplomats and other targets in Moscow. This tactic involves manipulating internet traffic to disable encryption and make communications vulnerable to surveillance, marking the first confirmed instance of cyber espionage conducted at the ISP level by Turla. The group, known also as Secret Blizzard, has been active for nearly 20 years targeting governments, journalists, and institutions. By using this method, Turla can implant malware backdoors to steal data and maintain persistent access, posing a significant risk to foreign embassies and sensitive organizations operating within Moscow's digital infrastructure - Innovation Origins

SURVEILLANCE BY AL GOVT: SPENDING SPIKED BEFORE LAST THREE ELECTIONS

IMAGE SOURCE: THE DAILY STAR

In the lead-up to Bangladesh's last three national elections (2014, 2018, and 2023), state spending on surveillance technologies surged significantly, playing a key role in the Awami League's consecutive electoral victories amidst credible allegations of widespread irregularities. Surveillance efforts targeted opposition parties such as BNP and Jamaat-e-Islami, as well as dissidents, students, and activists, subjecting them to invasive monitoring, arbitrary arrests, enforced disappearances, and extrajudicial killings. Spending shifted from geolocation trackers before 2018 to more advanced spyware by 2023, capable of bypassing end-to-end encryption on platforms like Messenger, Telegram, WhatsApp, and Viber. The National Telecommunication Monitoring Centre (NTMC) led spending, with a record $88.3 million in 2022 under new leadership, boosting its evolution into a sophisticated intelligence agency. Over the past decade, Bangladesh imported or deployed at least 160 surveillance and spyware systems at an estimated $184.5 million, with about 30 percent sourced from Israeli-linked firms via intermediaries circumventing trade restrictions. These technologies included Pegasus, Cellebrite, AI-powered facial recognition systems, IMSI catchers, and signal jammers. Surveillance activities remain largely unchecked due to broad legal powers granted to law enforcement, intelligence, and regulatory agencies, weak oversight, and exemptions from information disclosure laws, facilitating democratic backsliding through repression of political opponents and activists - The Daily Star

JESUIT HUMAN RIGHTS CENTER WARN OF GROWING STATE SURVEILLANCE IN MEXICO

IMAGE SOURCE: BORKENA

Ethiopian Prime Minister Abiy Ahmed's government uses advanced digital monitoring and sentiment analysis technologies to surveil online communications and social media, targeting dissent and political opposition to restrict freedom of expression. This surveillance strategy is part of the broader "Digital Ethiopia 2025" initiative aimed at digital transformation, but it has raised significant concerns about increasing political repression, erosion of civil liberties, and the use of digital infrastructure to consolidate authoritarian control under the guise of modernization - Borkena

POLICE FACIAL RECOGNITION VANS 'FEEL TOTALITARIAN'

IMAGE SOURCE: BBC

Police facial recognition vans in the UK have sparked concerns among young people who describe their presence as "totalitarian" and intrusive. The Home Office is rolling out 10 new Live Facial Recognition (LFR) vans across seven police forces to aid in locating suspects involved in serious crimes such as sexual offenses, violent assaults, and organized crime. These vans scan faces of passersby and compare them against police watchlists, with trained officers verifying matches. While officials cite the technology's success in catching dangerous criminals and maintaining public safety, civil liberties groups warn that the expansion represents a significant growth of the surveillance state, treating everyone as a potential suspect and raising issues related to privacy, the absence of a legal framework, and potential biases. The government is conducting consultations to establish safeguards and oversight prior to wider deployment, amidst ongoing legal challenges and public debate about the balance between security and civil rights - BBC

INTELLIGENCE AGENCIES

ZAMBIA'S UPDATED CYBER LAWS PROMPT SURVEILLANCE WARNINGS

IMAGE SOURCE: DARK READING

Zambia's updated Cyber Security and Cyber Crimes Acts of 2025, enacted in April, have sparked serious concerns over expanded state surveillance powers that threaten citizens' privacy, freedom of expression, and democratic rights. The laws grant law enforcement broad authority to intercept electronic communications without warrants based on vague criteria, permit intrusive audits of critical information infrastructure, and require data localization for "critical sectors," which broadly include public services and social media platforms. The Cyber Security Agency's placement under direct presidential control raises fears of political interference and weak oversight. Rights groups and legal bodies warn that these vague provisions can be weaponized to suppress dissent, restrict the press, and target activists, especially ahead of the 2026 elections, while harsh penalties ranging from fines to long prison sentences reinforce these risks. The laws passed with minimal public consultation, leading to widespread criticism that they prioritize state control over genuine cybersecurity, potentially enabling authoritarian abuses and undermining Zambia's democratic framework - Dark Reading

SHEIKH HASINA REGIME SPENT MILLIONS ON SPY TECH FOR SURVEILLANCE, CROWD CONTROL; ISRAEL AMONG TOP SUPPLIERS

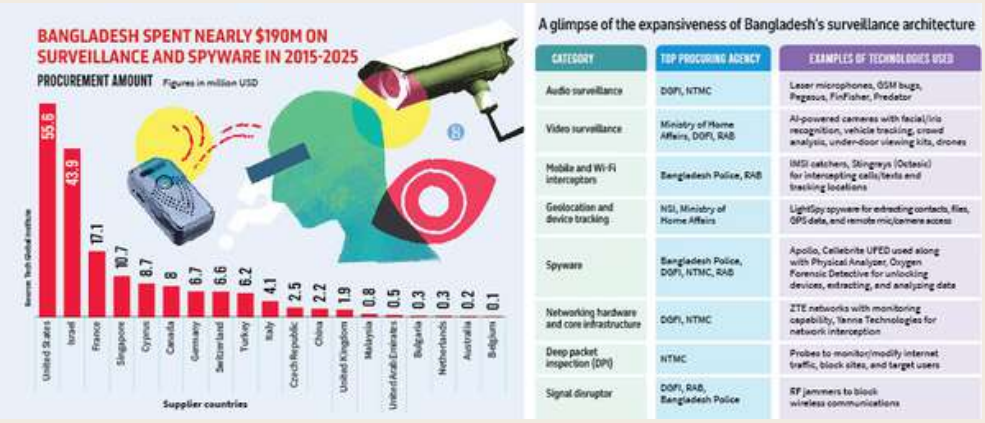

IMAGE SOURCE: THE BUSINESS STANDARD

The Sheikh Hasina regime in Bangladesh has reportedly spent millions on advanced surveillance and crowd control technologies, with Israel identified as one of the top suppliers of spyware and cyber surveillance equipment. Classified documents reveal that Bangladesh secretly purchased powerful Israeli spyware, such as Picsix's P6 Intercept, capable of mass surveillance, intercepting voice calls, text messages, and online activities, while also enabling interference with communications. Israeli experts trained Bangladeshi intelligence officers in using this aggressive and intrusive technology, which acts like a fake cell tower to capture data from hundreds of phones simultaneously. This secret acquisition and usage raise significant concerns about privacy violations and repression, especially since Bangladesh has no formal diplomatic relations with Israel and had banned Israeli travel up until recent years. The regime's investment in such sophisticated spyware has fueled fears of heightened government monitoring and suppression of political dissent and public protests in Bangladesh - The business standard

HASINA'S REGIME PURCHASED $190M IN SURVEILLANCE, SPYWARE TOOLS: STUDY

IMAGE SOURCE: DAILY SUN

The Sheikh Hasina regime in Bangladesh has secretly spent millions acquiring advanced spyware and surveillance technologies, primarily from Israeli company Picsix Ltd, through covert contracts disguised with front companies and third-party countries to mask Israel's involvement. The centerpiece of this procurement is the P6 Intercept, a powerful mass surveillance tool functioning as a fake cell tower that can track and intercept communications from 200 to 300 mobile phones simultaneously, including calls, text messages, internet activity, and even altering message content. Israeli intelligence experts trained Bangladeshi military personnel to operate this aggressive spyware, which is reportedly used to monitor and control political opponents, protestors, and dissidents during mass gatherings. This secret acquisition and use of intrusive surveillance technology raise serious privacy and human rights concerns, especially given Bangladesh's lack of formal relations with Israel and the regime's growing repression of political dissent and civil society - Daily Sun

AL SPENT $190 MILLION ON SURVEILLANCE TECH TO SUPPRESS OPPOSITION: REPORT

IMAGE SOURCE: THE REPORT

Between 2015 and 2025, the Bangladesh government under the Awami League (AL) regime spent nearly $190 million on importing and deploying over 160 advanced surveillance and spyware technologies, much of which was procured through opaque processes and third-party countries. These tools, including IMSI catchers, Wi-Fi interceptors, Cellebrite, FinFisher, and Predator, were largely used for extensive monitoring without legal warrants, targeting political opponents, journalists, activists, and ordinary citizens, especially around elections and mass protests. The National Telecommunications Monitoring Centre (NTMC) was the largest buyer, with significant purchases of internet traffic monitoring and decryption tools. Other key agencies such as Rapid Action Battalion (RAB), the police, and the Directorate General of Forces Intelligence (DGFI) also invested in surveillance technologies. Notably, about $40 million of these technologies originated from Israeli companies, acquired through intermediaries to circumvent diplomatic restrictions. The report highlights significant legal gaps in Bangladesh's outdated surveillance laws, granting broad powers to law enforcement with little oversight, thereby shifting the purpose of surveillance from citizen protection to political control and suppression of dissent. The report recommends urgent legal and institutional reforms to prevent Bangladesh from evolving into a model of digital authoritarianism where surveillance enforces political power rather than public interest and safety - The Report

INTEL WATCH

Watching the watchers. Guarding the guardians.

RUSSIA TO PRE-INSTALL WHATSAPP CLONES ON EVERY PHONE IN THE COUNTRY

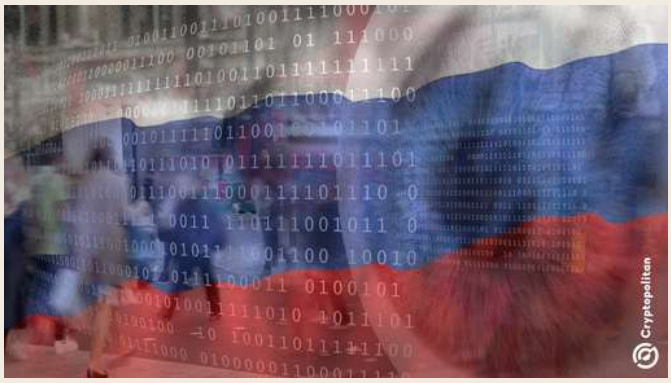

IMAGE SOURCE: CRYPTO POLITAN

Starting September 1, 2025, Russia will require all mobile phones and tablets sold in the country to come pre-installed with Max, a government-backed messaging app developed by VK, a Kremlin-controlled tech company. Max offers messaging, video calls, mobile payments, and access to state services. While Russian state media denies the app functions as spyware and claims it requires fewer permissions than apps like WhatsApp and Telegram, critics warn it collects extensive personal data—including call logs, financial information, purchase history, and location details accessible to the Federal Security Service (FSB) and Kremlin operatives for real-time monitoring. This move follows legislation mandating a homegrown messenger linked to public services and coincides with increased restrictions on foreign apps like WhatsApp and Telegram, with Moscow signaling potential bans on these platforms. Max's mandatory pre-installation is part of Russia's broader strategy to increase digital sovereignty and control over citizen communications, likened by critics to China's WeChat and described as a "Digital Gulag." Additionally, from January 1, 2026, all smart TVs sold in Russia will come preloaded with LIME HD TV, providing free access to state television channels - Crypto Politan

TRUMP ADMINISTRATION TO BEGIN CONTINUOUS POLICE-STATE SURVEILLANCE OF 55 MILLION US VISA HOLDERS

IMAGE SOURCE: WORLD SOCIALIST WEBSITE

The US State Department will implement continuous immigration vetting for all 55 million visa holders, involving constant surveillance of social media, law enforcement, and immigration records, extending even beyond US borders. This unprecedented monitoring will use AI to identify "anti-American" and "terrorist" behavior, targeting especially those who support causes like Palestine or espouse anti-capitalist ideologies. Privacy protections are effectively stripped away, with mandatory disabling of phone and app privacy features during visa interviews. Concurrently, the federal government has intensified militarized policing in Washington DC and opened the largest immigrant detention center in US history at Fort Bliss, Texas, where detainees face brutal, inhumane conditions and enforced disappearances under the radar of international law. This dual strategy of mass digital surveillance and expansive detention aims to repress immigrants and stifle dissent, criminalizing opposition under broad anti-terrorism and ideological pretexts while establishing a framework for mass repression of the working class at large - World Socialist website

INTEL WATCH

Watching the watchers. Guarding the guardians.

TRUMP MAY STRIKE DEAL WITH ISRAELI SPYWARE FIRM ACCUSED OF TARGETING JOURNALISTS, ACTIVISTS

IMAGE SOURCE: THE AMERICAN BAZAAR

President Donald Trump appears poised to reactivate a $2 million contract with Paragon Solutions, an Israeli spyware company known for its invasive hacking tools like Graphite that can infiltrate encrypted apps such as WhatsApp and Signal. Despite branding itself as a more "ethical" spyware firm, Paragon's technology has been linked to surveillance efforts against journalists, activists, and vulnerable groups. The spyware has been used globally by government agencies in countries including Italy, Canada, and Australia, raising significant human rights and privacy concerns. The renewed contract with U.S. Immigration and Customs Enforcement (ICE) highlights the tension between national security interests and civil liberties, emphasizing the urgent need for transparency and oversight to prevent abuse of such powerful surveillance technology. Prominent intelligence figures at Paragon have not prevented controversy, leaving democratic nations to wrestle with balancing security and privacy rights - The American Bazaar

AI STARTUP SAYS IT WILL END CRIME BY BLANKETING THE ENTIRE UNITED STATES IN EVER-WATCHING SPY CAMERAS

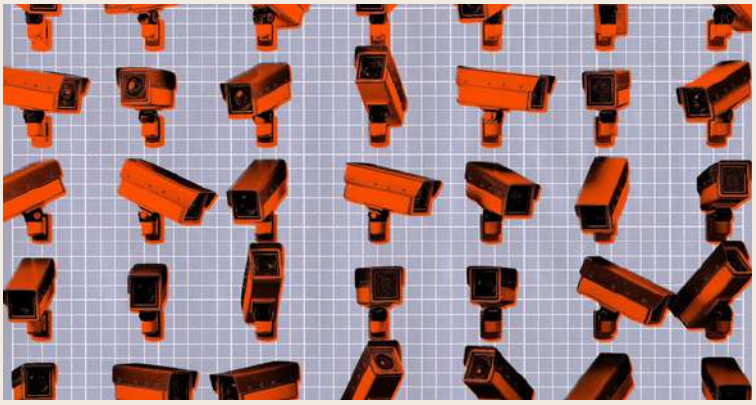

IMAGE SOURCE: FUTURISM

Garrett Langley, CEO of the surveillance startup Flock Safety, aims to drastically reduce crime in the United States by expanding a massive network of over 80,000 AI-powered cameras and surveillance drones currently used by police departments, private businesses, and homeowners. Valued at $7.5 billion, Flock Safety offers a subscription-based service that integrates fragmented private CCTV systems into one centralized web, making it easier for law enforcement to access footage and solve crimes. The company boasts partnerships with over 5,000 law enforcement agencies and 1,000 private organizations. While supporters claim this technology can create safer communities without sacrificing civil liberties, critics warn it disproportionately targets minority and immigrant populations, who are already heavily policed and incarcerated. Langley acknowledges the controversy but remains steadfast, arguing that meaningful change often provokes opposition - Futurism

Watching the watchers. Guarding the guardians.

HAVE YOUR SAY!
LETTER TO THE EDITOR

Dear Readers:

Welcome to the "Letter to the Editor" section of our newsletter - a safe space dedicated to your voice and your views. As an organisation rooted in the Global South but whose work extends across borders, our mission is to promote democratic oversight of intelligence and surveillance activities worldwide. We monitor, report, educate, and advocate to ensure that surveillance laws and practices respect human rights and democratic principles.

We strongly believe that meaningful change begins with dialogue, and that's where you come in. We invite you to share your thoughts about the issues we cover, your concerns, and experiences related to surveillance in your community or country and suggest topics or questions you want us to explore. Your insights help shape the conversation and strengthen our shared commitment to Defending Human Rights, Protecting Civic Space in the digital age, amplifying the need for transparency and accountability and holding power accountable.

Send your letters, stories, or feedback to us at advocacy@intelwatch.org.za, and together, let's strengthen the global movement for democratic oversight.

We look forward to hearing from you and building a Intelwatch-out community where everyone's voice matters.

Warm regards
The Intelwatch Team

INTELO WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

Sign up to get occasional news and briefings on intelligence oversight and surveillance reform in Southern Africa and beyond

FIND US ON SOCIAL MEDIA

@IntewatchNews

HAVE ANY QUESTIONS?

info@intelwatch.org.za

Global Dialogue

Funded by the European Union

We are grateful for the support of our donors!