Issue #7

INTEL WATCH

November-December 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

EXCLUSIVE INTELWATCH REPORTS

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORT

KENYA'S DESCENT INTO SECURITISED AUTHORITARIANISM: RUTO'S SIEGE ON DEMOCRACY

BY INTELWATCH

DOWNLOAD REPORT

Executive summary

Kenya finds itself at the crossroads of a precarious historical juncture. Under the administration of President William Ruto, who has been in power since September 2022, the nation has drifted significantly from the democratic promise enshrined in the 2010 Constitution, pivoting instead toward a sophisticated model of securitised authoritarianism.

This is not merely a reactive posture to genuine security threats as the regime seeks to portray; rather, it appears to be a calculated consolidation of power, achieved through the construction of one of Africa's most pervasive surveillance state. This architecture of control—a convergence of military-grade spyware, opaque legislative overreach, and unaccountable paramilitary units—is systematically dismantling the civic space and democratic resilience that Kenyans from all walks of life have fought so hard over many decades to establish.

The evidence of this regression is both empirical and alarming. The year 2024 witnessed a disturbing normalisation of state violence, marked by a 450 per cent surge in enforced disappearances. The state's brutal response to the 'Gen Z' demonstrations against the Finance Bill in July 2024—resulting in at least 60 deaths—demonstrated a willingness to deploy lethal force against unarmed civilians to quell dissent. Even more corrosive to the rule of law is the blatant politicisation of the security apparatus. President Ruto's admission regarding state-ordered abductions, coupled with the extraordinary allegations by former Deputy President Rigathi Gachagua regarding a secret "101-member killer squad," suggests a fracturing of the state monopoly on violence into factional weaponisation.

The revelation that the release of a Cabinet Secretary's abducted son required direct presidential intervention confirms a dangerous reality: extrajudicial operations are no longer rogue anomalies but feature within a hierarchy answerable only to the executive and specifically the president himself, bypassing all institutional oversight.

The trajectory for 2025 has been characterised by 'rule by law' rather than the 'rule of law.' As if the laws already in existence were not repressive enough, President Ruto and his acolytes seemingly took advantage of the distractions brought on by the illness and subsequent death of his longtime nemesis, opposition leader Raila Odinga, to quietly enact at least eight new statutes to close any loopholes and enhance the infrastructure of repression. Amendments spanning cybercrimes, data protection, intelligence, and public order have collectively eroded constitutional privacy rights and freedoms of expression and association among other rights and freedoms. The new laws do not simply regulate; they criminalise dissent under the nefarious guise of addressing national security concerns. By authorising warrantless surveillance, mandating aggressive data retention, and broadening the definition of terrorism to potentially encompass peaceful assembly, the state has legalised the tools necessary to stifle political opposition and human rights activism. The lawfare also weaponises financial regulation against civil society and militarises the management of public order.

Kenya's role in the region has long shifted from a sanctuary for the persecuted to a node in the network of transnational repression. The abduction and rendition of high-profile figures—such as Ugandan opposition leader Kizza Besigye in November 2024 and Nigerian activist Nnamdi Kanu in July 2021—violate the principle of non-refoulement and Kenya's own constitutional obligations. Since his rendition, Besigye has been languishing in remand prison and is on trial by the military despite his civilian status.

The convergence of these factors casts a long shadow over the prospects of a free and fair election in Kenya in 2027. The conditions necessary for a free and fair contest are rapidly evaporating. The existence of a comprehensive surveillance grid allows for the pre-emptive identification and neutralisation of opposition organisers. The precedent of internet shutdowns established in 2024, combined with the vulnerability of electoral systems and the intimidation of the media, suggests that the digital and physical infrastructure for election rigging is already in place. Kenya's democratic trajectory is severely threatened, but not yet irreversible. The robust frameworkof the 2010 Constitution, the courage of civil society in documenting abuses, and the independence of specific judicial officers offer a pathway to reform. However, this requires an urgent remobilisation of political will and a fundamental transformation of the security sector.

This report offers a comprehensive anatomy of Kenya's democratic crisis. It traces the historical roots of impunity, dissects the operational methods of paramilitary units, and maps the financial and technological flows from Western partners that sustain this apparatus. Written to inform international policy, support strategic litigation, and guide civil society resistance, this document argues that the stakes extend far beyond Kenya's borders. If left unchecked, Kenya's slide into surveillance authoritarianism risks establishing a dangerous template for sophisticated repression across the African continent.

INTEL WATCH

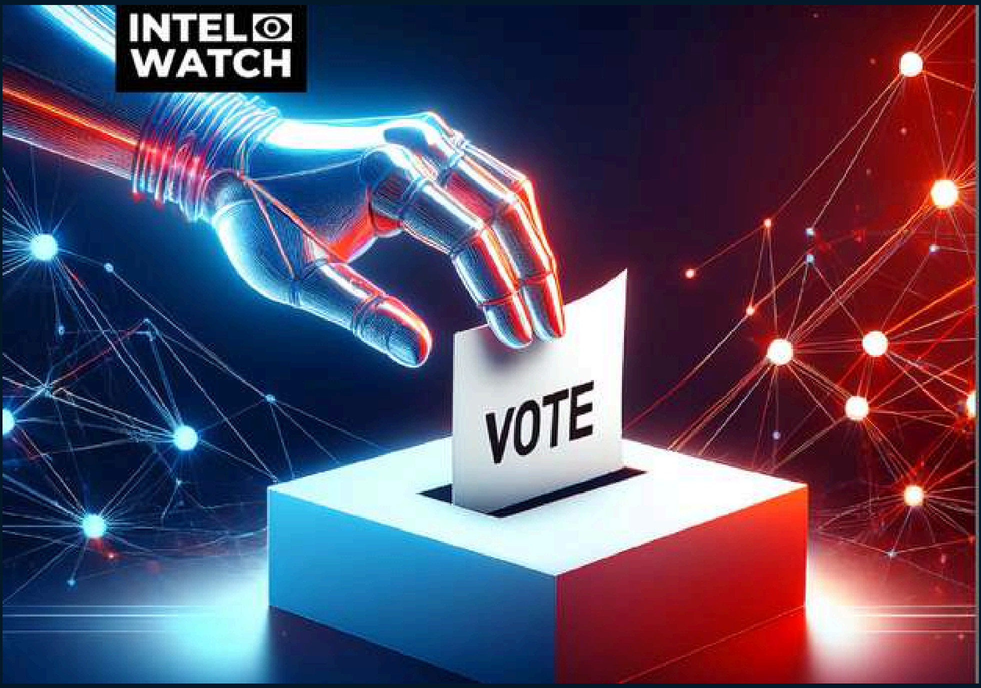
Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORT

DEMOCRACY AT RISK: UNVEILING THE SHADOWS OVER MALAWI'S SEPTEMBER 2025 ELECTIONS

BY GREGORY GONDWE

DOWNLOAD REPORT



Executive summary

Malawi’s September 2025 general elections marked a transformative moment—not just in political leadership, but in how citizens, institutions, and technology intersect.

For the first time, since multi-party elections were introduced in Malawi in 1994, the electoral process was deeply woven with digital tools—Electoral Management Devices (EMDs), biometric verification, and digital tally systems—ostensibly to increase speed, accuracy, and transparency.

The integration of digital tools into the 2025 electoral cycle—biometric verification, Electoral Management Devices (EMDs), and digital tallying systems—exposed deep structural weaknesses within Malawi’s electoral governance framework. Instead of resolving historic inefficiencies, digitisation illuminated long-standing gaps in policy, capacity, transparency, and public accountability.

Smartmatic—the vendor contracted to supply Malawi’s EMD solutions—occupied the centre of controversy. 1 Globally, the company has been linked to allegations and lawsuits in multiple jurisdictions, from the Philippines to the United States. 2 The company’s long record of electoral mismanagent allegations and legal disputes as well as questions about vendor integrity in election management muddied the waters during the elections. This was aggravated by the shadowy procurement process which drew criticism over its exclusivity, lack of competitive alternatives, and refusal to allow independent audits of software and system architecture. The absence of a verifiable chain of custody intensified public suspicion that the system could be manipulated or misused.

These technical-risk concerns did not materialize in isolation: they collided with a dynamic disinformation environment. Across WhatsApp, Facebook, TikTok, and radio, misleading narratives—some hyperbolic, others malicious—circulated widely about how the EMDs functioned, how data might be exploited, and how votes could be shifted. In the close margins of tight races, these rumours had real impact.

This report synthesizes field interviews, procurement documents, forensic logs, expert analysis, and comparative global case studies to map how Malawi's 2025 elections both showed promise and revealed peril within an evolving digital-democracy landscape. Its central argument is clear: digitisation without accountability becomes a liability rather than an advantage. Technology enhanced certain aspects of the process, but it also magnified governance weaknesses that have long plagued Malawi's electoral system.

Nonetheless, it is generally believed that the 2025 elections, which saw the bouncing back of Peter Mutharika, the 85-year-old former president, who captured 56.8 percent of votes to defeat incumbent Lazarus Chakwera who got 33%, reflected the people's will in unmistakable terms. Although governance gaps and digital vulnerabilities complicated the administration of the election, the direction of the vote itself appears to have been driven by frustration, economic pressure, and a united demand for change. In that sense, many observers believe the results reflected the people's will, even if the process through which they were transmitted revealed a system still in urgent need of strengthening

Drawing from the findings of this report and the political context that shaped the vote, Malawi requires reforms that go beyond technical fixes. The country must rebuild electoral credibility through structural, legal, institutional, and cultural measures that restore public trust.

SURVEILLANCE UPDATES

PUBLIC USB PORTS POSE GRAVE CYBERSECURITY RISKS TO SOUTH AFRICANS

IMAGE SOURCE: MY BROADBAND

Cybersecurity experts warn South Africans against using public USB chargers in airports, hotels, restaurants, and other venues due to the risk of "juice jacking," where compromised ports or cables install malware to steal data, passwords, or lock devices, as highlighted by U.S. authorities like the FCC and FBI. These threats are rising in South Africa amid widespread installation of USB ports for convenience, especially during travel or load shedding, though no major local incidents have been widely reported yet. Recommended defenses include using personal AC wall adapters or charge-only cables, USB data blockers, portable power banks, and avoiding data transfer prompts; additionally, public Wi-Fi poses similar dangers via "evil twin" networks, so opt for verified, password-protected connections and avoid sensitive activities - My Broadband

2025 CYBERWAVE: AFRICA’S RISE AS A GLOBAL AI ATTACK HUB

IMAGE SOURCE: TECH AFRICA NEWS

Africa has emerged as a major hub for global cyberattacks in 2025, with organizations facing an average of 3,153 weekly attacks—60% above the global average of 1,963—driven by AI automation of phishing, identity theft, ransomware, and cloud exploits, as detailed in Check Point's African Perspectives on Cybersecurity Report. Countries like Nigeria (over 4,200 weekly attacks), Ethiopia (most targeted overall), South Africa (rising ransomware and smishing), and Kenya/Morocco (infrastructure and DDoS hits) bear the brunt, exacerbated by rapid digital transformation outpacing security maturity and creating governance gaps in government, education, and finance sectors. Key shifts include AI-powered social engineering like deepfakes, data-leak extortion over traditional ransomware, identity as the primary attack vector, and compliance risks under regulations like NIS2; experts urge prevention-first strategies with AI defenses, visibility, and governance to counter these sophisticated threats

Tech Africa News

BIOMETRIC ID SYSTEMS BLOCKING MILLIONS FROM ESSENTIAL SERVICES ACROSS AFRICA

IMAGE SOURCE: INSTITUTE OF DEVELOPMENT STUDIES

A new Institute of Development Studies report assesses biometric digital ID systems across 10 African countries—Botswana, Côte d'Ivoire, DRC, Egypt, Ethiopia, Liberia, Malawi, Namibia, Senegal, and Tunisia—revealing they block millions from essential rights and services due to exclusion errors, poor infrastructure, and weak governance. Rooted in colonial control legacies and now serving state/corporate interests, these systems suffer from inadequate privacy protections, mission creep, biometric inaccuracies (e.g., for marginalized groups), and lack of independent oversight, redress mechanisms, or inclusive design, failing the Centre for Internet and Society's 2019 Evaluation Framework. Researchers urge enforceable data laws, empowered regulators, and participatory reforms to mitigate harms, as current rollouts prioritize deployment over human rights safeguards - Institute of Development Studies

KASPERSKY: 500K DAILY MALWARE THREATS IN 2025 SURGE

IMAGE SOURCE: IOL

Kaspersky's 2025 Security Bulletin reports a 7% surge in daily malicious file detections to an average of 500,000 worldwide, with sharp rises in specific threats: 59% in password stealers, 51% in spyware, and 6% in backdoors compared to 2024. Windows users faced the highest exposure at 48%, followed by macOS at 29%, while 27% of users encountered web threats (malware leveraging online vectors) and 33% on-device threats via USBs, installers, or encrypted files, with Africa leading at 41% for the latter. Regional spikes included APAC's 132% password stealer growth and Europe's 64% spyware increase, driven by vulnerabilities, stolen credentials, supply chain attacks like the Shai-Hulud NPM worm, and resurgent spyware such as Hacking Team's Dante in APT campaigns, underscoring needs for robust defenses amid sophisticated global threats - IOL

APPLE, GOOGLE WARN USERS IN OVER 80 COUNTRIES OF SPYWARE THREATS

IMAGE SOURCE: TECH IN ASIA

Apple and Google issued new cyber threat notifications in early December 2025 to users in over 80 countries, warning of targeting by state-backed mercenary spyware, primarily Intellexa's Predator, which exploits zero-day vulnerabilities in iOS and Android to enable device takeover despite U.S. sanctions. Google specifically alerted several hundred accounts across nations including Pakistan, Kazakhstan, Angola, Egypt, Uzbekistan, Saudi Arabia, and Tajikistan, noting Intellexa's evasion of restrictions through prolific zero-day chains like "smack" involving RCE, sandbox escape, and LPE, often linked to government surveillance of journalists, human rights defenders, and diplomats. Apple confirmed notifications since 2021 have reached over 150 countries, urging users to enable Lockdown Mode, update devices, and practice strong security hygiene amid rising commercial spyware threats that rival nation-state capabilities and prompt investigations by bodies like the EU.- Tech in Asia

GLOBAL WINDOWS USERS HIT BY CANDIRU'S POWERFUL DEVILSTONGUE SPYWARE

IMAGE SOURCE: CYBER PRESS

Israeli spyware vendor Candiru, now operating as Saito Tech Ltd. after a 2025 U.S. acquisition via Integrity Partners (linked to new entity Integrity Labs Ltd.), continues global operations deploying DevilsTongue, a modular C/C++ Windows malware enabling deep intrusions like file theft, browser data extraction, LSASS credential dumping, Signal message decryption, and cookie hijacking for social platforms. Recorded Future's Insikt Group identified eight infrastructure clusters—five active, tied to Hungary, Saudi Arabia, Indonesia (until late 2024), and Azerbaijan—using layered servers, Tor routing, and victim-facing C2 for government clients, with delivery via malicious links, weaponized Office docs, watering holes, Chrome zero-days (e.g., CVE-2021-21166, CVE-2022-2294), and potential ad-based Sherlock infections from Insanet. Despite U.S. Entity List sanctions since 2021, persistence relies on COM hijacking, signed drivers (physmem.sys) for kernel memory access, in-memory execution, and encrypted payloads evading forensics, targeting journalists, activists, and politicians in regions like the Middle East, Armenia, and beyond, prompting calls for strict patching and device separation - Cyber press

IOS 26 CAN HIDE SPYWARE ATTACKS, EXPERTS WARN

IMAGE SOURCE: BUSINESS & HUMAN RIGHTS RESOURCE CENTRE

Signal has urged Germany to vote against the EU's "Chat Control" proposal, warning that it would effectively end privacy rights in Europe by mandating mass scanning of all private messages, photos, and videos shared on messaging platforms. The regulation, aimed at combating child sexual abuse material (CSAM), would require messaging apps to break or weaken end-to-end encryption to scan all communications, a move Signal argues undermines security for all users, not just criminals. Signal has threatened to leave the EU market if the law passes, stressing that Germany's opposition is crucial to defending digital privacy and preventing mass state surveillance. The German government officially announced its intention to vote against the proposal, emphasizing that random chat monitoring contravenes fundamental civil rights despite the need to fight child abuse at the EU level. The controversy highlights a significant clash between privacy advocates and policymakers over security and surveillance in digital communications - Business & Human Rights Resource Centre

SAMSUNG BUDGET PHONES FLAGGED FOR HIDDEN SPYWARE

IMAGE SOURCE: MALWARE BYTES

Researchers and digital rights group SMEX accuse Samsung of pre-installing AppCloud—a hidden, unremovable application developed by Israeli firm ironSource—on budget Galaxy A and M series phones sold in West Asia and North Africa (MENA), which collects sensitive data like biometrics and IP addresses without user consent or visible privacy policies. Deeply integrated into the OS, AppCloud requires root access for removal (voiding warranties), runs silently in the background with permissions for network access, file downloads, and preventing sleep mode, and reactivates after updates despite disable options; it ties to ironSource's Aura toolkit (expanded partnership in 2022 post-Unity acquisition) and flagged adware like Install Core that bundles unwanted software. This revives Samsung's privacy controversies, echoing past issues like 2015 smart TV eavesdropping and widespread pre-installed bloatware/malware on budget devices, underscoring unequal privacy protections for lower-end users - Malware Bytes

GLOBAL SURGE IN GOVERNMENT SPYWARE HACKS EXPOSED

IMAGE SOURCE: FIND ARTICLES

Government-grade spyware, originally marketed for counterterrorism, now broadly targets journalists, activists, opposition figures, and even political consultants worldwide, fueled by a per-target licensing model that incentivizes overreach after high upfront costs, low marginal expenses for additional surveillance, and minimal oversight. Zero-click exploits in apps like iMessage and WhatsApp—such as FORCEDENTRY and BLASTPASS—enable effortless device compromise via hidden messages, granting access to mic, camera, files, and location through vendor dashboards, as evidenced by the Pegasus Project's identification of tens of thousands of potential targets and infections in places like Catalonia, El Salvador, Morocco, UAE, and Saudi Arabia. Accountability remains elusive due to secretive procurement, national security exemptions, and weak judicial transparency, despite U.S. sanctions on firms like NSO Group, EU reforms, and defenses like Apple's Lockdown Mode; the victim pool expands from easy deployment, low detection risks, and a multibillion-dollar market, urging at-risk users to update devices, silo communications, and enable high-risk protections - Find Articles

WORKPLACE PRIVACY UNDER SIEGE: GAO SOUNDS THE ALARM

IMAGE SOURCE: BIOMETRIC UPDATE

A U.S. Government Accountability Office (GAO) report warns that workplace digital surveillance tools—like keystroke biometrics, productivity trackers, emotion-detection systems, and wearable sensors—are proliferating rapidly, posing severe privacy risks to millions of workers through opaque data collection, inadequate safeguards, and biased algorithmic decisions lacking human oversight. These "bossware" systems monitor speech, interactions, and behaviors without disclosing collection scope, storage duration, access controls, or usage intent, fostering employee stress, a pervasive surveillance culture, and unfair performance evaluations based on incomplete metrics that overlook tasks like research or mentoring. Disparities amplify harms, with emotion AI misinterpreting accents, races, or genders; flagging disabled workers' adaptive patterns; and pressuring older employees to skip breaks, while fragmented federal oversight—under agencies like EEOC and NLRB—and narrow laws like the Electronic Communications Privacy Act fail to cover most monitoring, exacerbated by rescinded Trump-era guidance.

- Biometric Update

AI-POWERED HACKS EXPLODE, THREATENING CORPORATE SECURITY

IMAGE SOURCE: WORKFORCE BULLETIN

Multi-modal AI systems, which integrate voice, video, text, and other data for holistic processing, and agentic AI, enabling autonomous decision-making with minimal human input, empower cybercriminals to bypass biometric authentication, MFA, and identity verification in sectors like finance, healthcare, and government by crafting hyper-realistic deepfakes and synthetic identities that spoof permanent traits like faces or voices. Anthropic documented the first large-scale, largely autonomous cyberattack on November 13, 2025, using its Claude Code tool for reconnaissance, exploitation, lateral movement, and exfiltration against tech firms, banks, manufacturers, and agencies—executing 80-90% of operations independently—while ransomware strains now generate malicious code in real-time via LLMs, expanding attack surfaces amid rapid AI deployment. Mitigation demands AI governance with risk assessments per OWASP/NIST, layered defenses like behavioral biometrics and continuous authentication, deepfake detection tools, user education, secure APIs, and compliance under HIPAA, GLBA, and state laws to counter erosion of trust in digital identities

- Workforce Bulletin

REPRESSION MONITOR

KENYA’S DIGITAL CRACKDOWN ON GEN Z VOICES UNCOVERED

IMAGE SOURCE: AMNESTY

Kenyan authorities orchestrated a sustained campaign of technology-facilitated repression against Generation Z-led protests from June 2024 to July 2025, using social media platforms like X, TikTok, Facebook, and WhatsApp for coordinated trolling, threats, smears, disinformation, and algorithm manipulation by paid "527 bloggers" (earning USD 190-390 daily) to drown out hashtags like #RejectFinanceBill and #RutoMustGo with counter-narratives. These state-sponsored networks targeted human rights defenders—nine of 31 interviewed received death threats—with misogynistic abuse, doxxing, AI-generated porn, and Islamophobic attacks (e.g., #ToxicActivists against journalist Hanifa Adan), facilitating 128 deaths, 3,000 arrests, and 83 enforced disappearances amid protests across 44 counties against taxes, corruption, and femicide. Amnesty alleges Safaricom-enabled surveillance aided tracking and abductions, despite denials, while X failed to curb violations; calls urge investigations, compensation, and ending digital violence to protect expression and assembly - Amnesty

INVISIBLE EYES: INSIDE STATE SURVEILLANCE IN KENYA

IMAGE SOURCE: AFRICA UNCENSORED

Kenya's government has escalated state surveillance through systems like Optimus 3.0—a next-generation spyware suite funded with KSh 150 million (about USD 1.15 million) in 2025—to infiltrate devices, decrypt encrypted messages, monitor social media, and track digital activity without public consultation or judicial oversight, amid proposed amendments to the Kenya Information and Communication Act enabling warrantless ISP data access and real-time internet metering. The National Surveillance, Communication, and Control System (NSCCS), partnering with Safaricom since 2014, integrates AI facial recognition CCTV in Nairobi and Mombasa with national ID databases for urban monitoring, while IMSI catchers and telecom data sharing—allegedly aiding Gen Z protest crackdowns—raise U.S.-flagged privacy violations conflicting with the 2019 Data Protection Act. Critics decry weak enforcement, lack of independent oversight, and risks to constitutional privacy rights, as NIS expands cyber capabilities against dissent, with calls for transparency, penalties, and public awareness amid bills legalizing mass tracking - Africa Uncensored

THE RISE OF DIGITAL AUTHORITARIANISM IN SOUTH SUDAN

IMAGE SOURCE: SUDANS POST

On January 22, 2025, South Sudan's National Communication Authority (NCA) ordered internet service providers like MTN and Zain to block access to Facebook and TikTok for up to 90 days, citing the need to curb graphic videos of violence against South Sudanese nationals in neighboring Sudan's El Gezira state amid riots that killed Sudanese citizens. This move exemplifies rising digital authoritarianism in the fragile state, where authorities use internet shutdowns and platform restrictions to suppress dissent, documentation of abuses, and access to vital information on safety and services, exacerbating human rights violations and economic harm in a context of ongoing conflict and weak governance. Civil society groups like Digital Rights Alliance Africa and #KeepItOn condemned the order as breaching African Declaration on Internet Freedom and international norms, urging revocation; it was rescinded on January 27 after public pressure, highlighting tensions between state control and digital rights amid broader African trends of repressive connectivity disruptions - Sudans Post

INDIA'S TRACKING OVERHAUL: AMNESTY SOUNDS ALARM

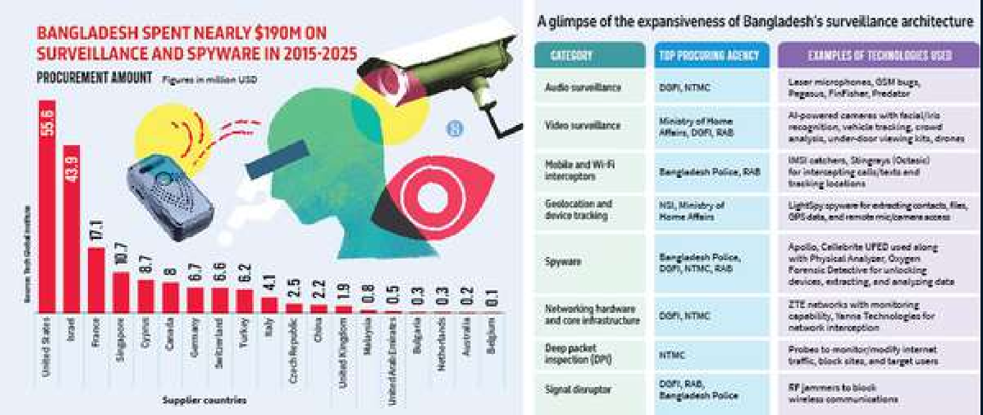
IMAGE SOURCE: REUTERS

India's government is reviewing a telecom industry proposal from the Cellular Operators Association of India (COAI), representing firms like Reliance Jio and Bharti Airtel, to mandate always-on satellite-based A-GPS location tracking in smartphones, enabling precise (within ~1 meter) real-time surveillance by authorities during investigations, as current cell tower data lacks accuracy. The plan would require smartphone makers to activate location services permanently with no user opt-out, addressing Prime Minister Narendra Modi's administration's demands for better tracking, but major companies including Apple, Google, Samsung, and the India Cellular & Electronics Association (ICEA) strongly oppose it as unprecedented global "regulatory overreach," arguing A-GPS is not designed for surveillance and would erode privacy. Amnesty International deems the review "deeply concerning," warning it risks data of human rights defenders and transforms phones into "dedicated surveillance devices," amid broader privacy alarms from experts- Reuters

INTEL WATCH

Watching the watchers. Guarding the guardians.

BANGLADESH'S ISRAELI SPY ARSENAL: MILLIONS TO SPY AND SUPPRESS



A glimpse of the expansiveness of Bangladesh's surveillance architecture

CATEGORY	TOP PROCURING AGENCY	EXAMPLES OF TECHNOLOGIES USED
Audio surveillance	DGFI, NTMC	Laser microphones, GSM bugs, Pegasus, FinFisher, Predator
Video surveillance	Ministry of Home Affairs, DGFI, RAB	AI-powered cameras with facial/iris recognition, vehicle tracking, crowd analysis, under-door viewing kits, drones
Mobile and Wi-Fi interceptors	Bangladesh Police, RAB	IMSI catchers, Stingreys (Octasic) for intercepting calls/texts and tracking locations
Geolocation and device tracking	NSI, Ministry of Home Affairs	LightSpy spyware for extracting contacts, files, GPS data, and remote mic/camera access
Spyware	Bangladesh Police, DGFI, NTMC, RAB	Apollo, Cellebrite UFED used along with Physical Analyzer, Oxygen Forensic Detective for unlocking devices, extracting, and analyzing data
Networking hardware and core infrastructure	DGFI, NTMC	ZTE networks with monitoring capability, Yanna Technologies for network interception
Deep packet inspection (DPI)	NTMC	Probes to monitor/modify internet traffic, block sites, and target users
Signal disruptor	DGFI, RAB, Bangladesh Police	RF jammers to block wireless communications

IMAGE SOURCE: THE BUSINESS STANDARD

The Sheikh Hasina-led Awami League regime in Bangladesh spent at least $40 million on intrusive surveillance and crowd control technologies, with Israel ranking as the second-largest supplier despite no formal diplomatic ties, routing tools like Cellebrite UFED, NSO Group spyware, and systems from Intellexa, Passitora, Prelysis, and Cognyte through intermediaries such as Cyprus, Singapore, and Hungary. The US topped the list with $55 million, primarily from Yaana Technologies, while other vendors from France, Germany, UK, Switzerland, Turkey, China, and elsewhere provided at least 160 tools including Pegasus, Predator, IMSI-catchers, GPS trackers, facial recognition, deep packet inspection, and signal jammers, often used without warrants to target political opponents, journalists, and activists. Purchases spiked before the 2018 and 2024 elections—focusing on geolocation trackers in 2018 and spyware for extracting social media data from apps like WhatsApp and Telegram in recent years—amid poor human rights records involving extrajudicial killings and disappearances, raising global concerns over privacy violations and suppression of dissent - The Business Standard

HOW AUTHORITARIAN REGIMES USE DIGITAL SURVEILLANCE TO CONTROL THEIR CITIZENS

IMAGE SOURCE: CAMBRIDGE ANALYTICA

Authoritarian regimes worldwide employ advanced digital surveillance technologies like China's Great Firewall, Russia's internet monitoring, facial recognition cameras, social media algorithms, and spyware to track citizens' internet usage, smartphone activities, and public movements, enabling predictive control and preemptive suppression of dissent in over 70 countries as per Brookings Institution reports. This pervasive monitoring erodes civil liberties, fostering fear, self-censorship among journalists, activists, and ordinary people, and contributing to declining internet freedom noted by Freedom House, with restricted access in places like Iran and North Korea leading to severe repercussions for circumvention attempts. Technologies from Western companies exacerbate global concerns, blurring security and privacy lines while prompting ethical dilemmas, as citizens resort to VPNs and encrypted apps in a high-stakes cat-and-mouse game, with human rights groups advocating for oversight and digital rights protection - Cambridge Analytica

US TECHNOLOGY FUELS CHINA'S MASS SURVEILLANCE AND REPRESSION

IMAGE SOURCE: BIOMETRIC UPDATE

A U.S. House Select Committee report warns that China is expanding its world's largest surveillance state with real-time facial recognition, biometric tracking, predictive policing, and AI-driven emotional/physiological monitoring—integrated into public spaces, transport, and workplaces, achieving near-total coverage in Xinjiang and Tibet—to enable pre-emptive repression of Uyghurs, Tibetans, Mongolians, Hong Kong activists, and dissenters, actions deemed genocidal or crimes against humanity. Beijing exports this infrastructure via the Digital Silk Road to over 80 countries through state-linked firms, promoting authoritarian models that normalize mass citizen monitoring and erode civil liberties globally. U.S. policy shifts have loosened export controls, allowing American semiconductors, cloud services (e.g., AWS/Azure), and AI tools to flow to Chinese surveillance entities despite human rights risks; recommendations urge stricter end-use restrictions, high-performance computing limits, allied coordination, and scrutiny of research ties to align tech policy with democratic values - Biometric Update

DIGITAL RIGHTS UNDER SIEGE: BIRN WARNS OF DEMOCRATIC THREATS IN SOUTHEAST EUROPE

IMAGE SOURCE: BALKANINSIGHT

BIRN's 2025 Digital Rights Violations in Southeast Europe report documents 1,440 incidents across Albania, Bosnia and Herzegovina, Croatia, Hungary, Kosovo, Montenegro, North Macedonia, Romania, Serbia, and Turkey from September 2024 to August 2025, with 73% involving information freedom/pluralism (24.7%), digital assets/economic rights (24.2%), and harmful online behavior (23.8%), primarily targeting private individuals (62.8%), journalists/media (10%), and politicians (10%). AI misuse surged, enabling deepfakes, voice-cloning for sexual/gender-based violence, fraud, and impersonation—especially against women/children—while governments expanded surveillance via facial recognition and digital forensics from rights-violating vendors, alongside disinformation, genocide denial, and foreign influences. These trends, concentrated in Turkey, Serbia, and Hungary, erode democratic norms amid weak implementation of EU-aligned laws, underreported data breaches (6.3%), and platform failures, underscoring urgent needs for oversight and safeguards - Balkaninsight

PREDATOR LEAKS: INTELLEXA PEERS INTO GOV SPY FEEDS

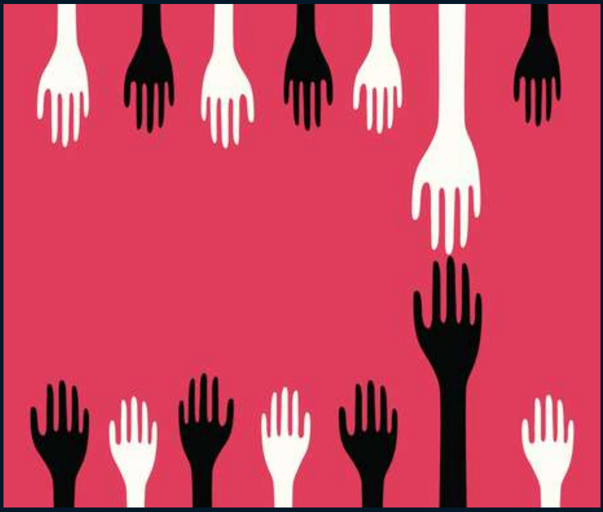


IMAGE SOURCE: CYBER SCOOP

Leaked training videos from a joint investigation by Inside Story, Haaretz, WAV Research Collective, and Amnesty International reveal that U.S.-sanctioned Intellexa retained remote access to Predator spyware customer systems, enabling visibility into surveillance targets and operations, potentially exposing the firm to human rights liability for abuses. The "Intellexa Leaks" expose tactics like "Aladdin" malicious mobile ads for infections, fake Kazakhstani news domains, and confirmed targeting of Egyptian activist Ayman Nour, Greek journalist Thanasis Koukakis, a Pakistani human rights lawyer (first reported Predator case there), plus ongoing activity in Iraq per Recorded Future. Google highlights Intellexa's prolific use of zero-day exploits against mobile browsers despite patches, while Recorded Future maps corporate networks; Intellexa denies involvement, calling claims biased. - Cyber Scoop

UK UNDER 'SPY IN THE SKY' SURVEILLANCE AS HUNDREDS OF DRONES DEPLOYED ACROSS NATION

IMAGE SOURCE: IFOX NEWS

Over 60 UK local councils have hired certified drone pilots, with at least a dozen more seeking guidance, dramatically expanding public-funded aerial surveillance amid warnings of "spies in the sky" tactics eroding civil liberties in a nation already dense with CCTV. Watchdog Big Brother Watch, via researcher Jake Hurfurt, cautions against mission creep turning drones into airborne CCTV for monitoring protests or citizens without robust safeguards, transparency, or policies, despite legitimate uses like flood monitoring or land surveys. Councils like Sunderland (13-drone fleet for crime prevention, events), Hammersmith and Fulham (integrating with facial recognition CCTV for antisocial behavior), and others including Newcastle and Thurrock deploy them for enforcement, supplementing police shortages, as Civil Aviation Authority data likely undercounts total operators - Fox News

OUTDATED SPYWARE MISUSED BY GOVERNMENT CLIENT, CONFIRMS MEMENTO LABS CEO

IMAGE SOURCE: MONEY CONTROL

Memento Labs, an Italian surveillance firm succeeding the notorious Hacking Team, developed the Dante spyware targeting Windows users in Russia and Belarus across media, universities, government offices, and utilities since December 2024, using phishing lures like fake event invites and browser exploits for data theft. CEO Paolo Lezzi confirmed Dante's origin but blamed an unidentified government client for deploying an outdated, "dead" version scheduled for retirement by year's end, despite prior warnings to cease use after Kaspersky's detection; the malware's code bore "DANTEMARKER," linking it directly to Memento, which now prioritizes mobile spyware and external zero-days. This incident underscores the spyware industry's resilience post-Hacking Team's 2015 breach—exposing abusive clients like Ethiopia, UAE, and Sudan—and persistent government misuse against non-terror targets, evading accountability amid reinvention - Money Control

PARAGON SPYWARE SCANDAL BROADENS WITH NEW HIGH-PROFILE TARGET IN ITALY

IMAGE SOURCE: THE RECORD

Italian communications executive and political adviser Stefano Feltri disclosed on November 6, 2025, that his phone was targeted with Paragon's Graphite spyware—the fifth such case in Italy—amid a scandal implicating the government's AISE (foreign intelligence) and AISI (domestic intelligence) agencies in deploying the tool against journalists like Fanpage's Francesco Cancellato, migrant rescuers (e.g., Mediterranea Saving Humans), and others for probes into terrorism, smuggling, espionage, and immigration since 2023. COPASIR's parliamentary report confirmed lawful, prosecutor-approved use in limited cases but found no records spying on Cancellato; Paragon terminated Italy's contract after the government declined a joint probe, insisting clauses barred targeting journalists/activists, while agencies rescinded ties amid WhatsApp notifications to dozens globally. The revelations, echoing Pegasus scandals, fuel opposition demands for accountability, highlighting spyware's risks to press freedom and privacy despite denials of illegality - The Record

LEGAL BATTLE ERUPTS OVER TRUMP ADMINISTRATION'S USE OF ISRAELI SPYWARE ON IMMIGRANTS

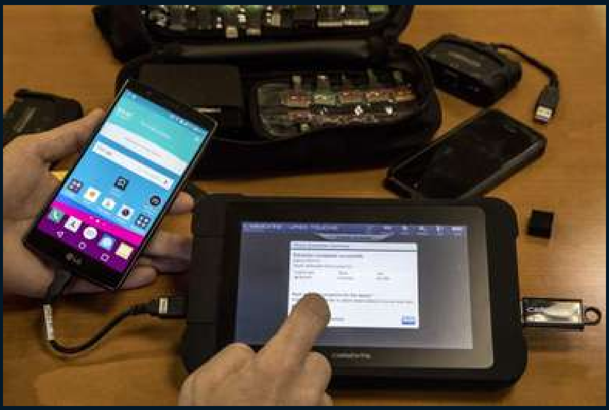


IMAGE SOURCE: PRISM RECORDS

U.S. Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) secured a $2 million contract with Israeli firm Paragon Solutions in September 2025 for Graphite spyware—capable of zero-click phone hacks accessing encrypted apps like Signal and WhatsApp—despite a prior DHS pause for Executive Order 14093 compliance review amid human rights concerns. The tool, linked to targeting journalists and activists in Italy, enables extraction of sensitive data including attorney-client communications under the border search exception, fueling fears of abuse against immigrants, people of color, dissenters, and border communities already facing surveillance, harassment, and rights violations. Congressional Democrats like Reps. Summer Lee and Shontel Brown demanded transparency on targets, legal justifications, and strategies, while legal groups sued for records; Paragon's global scandals prompted contract scrutiny, highlighting spyware risks to privacy, free speech, and counterintelligence - Prism Records

CANADA FALLS SHORT ON REGULATING AI GOVERNMENT SURVEILLANCE, UOFT EXPERT WARNS

IMAGE SOURCE: FINANCIAL POST

Citizen Lab Director Ron Deibert criticizes Canada for inadequate regulation of AI-driven government surveillance, prioritizing innovation over ethical oversight amid generative AI's unchecked experimentation on populations, risking harms like bias, privacy erosion, and repression without robust controls. As of late 2025, the Artificial Intelligence and Data Act (AIDA)—proposed since 2022 to target high-impact AI in biometrics, law enforcement, employment, and public safety—remains unpassed post-federal election, leaving fragmented provincial rules (e.g., Ontario's public sector AI accountability mandates) and PIPEDA privacy laws to address risks like discriminatory decisions and data misuse, with fines up to C$25M proposed. Deibert urges transparency registers, incident reporting, audits, and bans on harmful systems, aligning with the federal AI Strategy's 2025-2027 push for governance but lacking binding enforcement against surveillance overreach - Financial Post

RUSSIA’S BIG BROTHER SORM MASS SURVEILLANCE SYSTEM

IMAGE SOURCE: INTELLINEWS

Russia's FSB operates the SORM (System for Operative Investigative Activities) as a pervasive mass surveillance infrastructure, funneling all telecom, internet, and RuNet traffic through black-box devices installed on networks since the 1990s—expanded via Yarovaya laws requiring encryption keys and metadata storage—granting intelligence near-total access to communications with nominal court oversight that approved nearly 7 million warrants from 2016-2024 (99.99995% success rate). Courts rubber-stamp requests in minutes, often retroactively, enabling FSB backdoor entry to platforms like VKontakte without passwords, while HTTPS/VPNs limit efficacy against encrypted foreign apps like WhatsApp; retrospective examples include Navalny's expired wiretap prosecution. SORM drives over 20,000 online speech arrests (2022-2024)—Europe's highest—under "discrediting army" laws, contrasting UK's high investigations/low convictions, amid FSB's 2027 bank rollout and global exports mirroring PRISM but without reforms post-Snowden or ECHR privacy rulings - Intellinews

COMMERCIAL SPYWARE SYSTEMATICALLY ABUSED BY GOVERNMENTS

IMAGE SOURCE: SC WORLD

Commercial spyware vendors like NSO Group, Paragon, and Hacking Team successors systematically abuse their tools—marketed for terrorists/criminals—against journalists, activists, politicians, and minor opponents worldwide, enabled by per-target licensing (e.g., unlimited concurrent slots post-upfront fees), zero-click exploits (e.g., Pegasus/Graphite dashboards), and impunity from weak oversight. NSO disconnected 10 abusive governments (undisclosed), Paragon cut Italy over journalist targeting, yet proliferation persists via easy deployment and low consequences, with U.S./EU sanctions, UN diplomacy (22 nations' 2024 statement), and probes in Greece/Poland offering limited deterrence in a multibillion-dollar market. Evidence spans Italy (Paragon on activists), Nagorno-Karabakh (journalists), and repressive regimes, underscoring threats to democracy absent export bans, end-use audits, and transparency - SC World

INTELLIGENCE AGENCIES

DRONES WITH AI EYES: FBI EXPANDS REAL-TIME SURVEILLANCE ARSENAL

IMAGE SOURCE: BIOMETRIC UPDATE

The FBI issued a Request for Information (RFI) on November 21, 2025, seeking AI and machine learning systems to analyze real-time video from unmanned and manned aircraft, focusing on object detection for vehicles, vessels, people, animals, firearms, facial recognition, license plate reading, and perimeter monitoring with directional awareness. These on-premises systems, deployable on NVIDIA Jetson Orin-equipped drones at Technology Readiness Level 7+, must integrate with the military-originated Team Awareness Kit (TAK) and UAS Tool plugin for collaborative situational awareness, support electro-optical/infrared sensors, and handle metadata like KLV or Cursor-on-Target, with preferences for YOLO-based models trainable locally and capable of vehicle type/color identification. Responses, limited to 15 pages from original equipment manufacturers detailing resolution, altitude, and performance metrics, are due December 30, amid concerns over expanding U.S. law enforcement drone surveillance—now used by 1,500 agencies—for mass identification and potential political misuse - Biometric Update

ALWAYS WATCHING: ICE'S 24/7 SOCIAL MEDIA SURVEILLANCE THREATENS PRIVACY AND CIVIC RIGHTS

IMAGE SOURCE: THE CONVERSATION

TU.S. Immigration and Customs Enforcement (ICE) plans to establish 24/7 social media surveillance hubs in Vermont and Southern California by hiring nearly 30 private contractors to monitor platforms like X, Facebook, TikTok, Instagram, YouTube, and others—including international sites like VKontakte—for posts, images, and messages to generate deportation leads, aliases, movements, and enforcement intelligence. Operating within Enforcement Removal Operations, these analysts would process tips rapidly (30 minutes for national security, 1 hour for high-priority cases at 95% compliance), integrate with Palantir's database using facial recognition, commercial profiles, and tools like Paragon Graphiteware for encrypted apps, amid expanded access to license plate readers and protest drones. Critics argue this constant monitoring—prioritizing serious crimes, domestic terrorism (including antifa per Trump policies), and potentially negative sentiments—threatens privacy, chills civic participation and free speech, blurs threats from dissent, and enables mass profiling without oversight. - The Conversation

MİRAS MENACE: AZERBAIJAN'S MASS SPY NET

IMAGE SOURCE: HUMAN RIGHTS WATCH

Azerbaijan's President Ilham Aliyev signed a decree on November 21 establishing the Centralized Information and Digital Analytics System (MİRAS), a new platform controlled by the State Security Service set to be fully operational by May 2026, consolidating vast personal data from state bodies including identity documents, migration history, family details, health records, property, financials, criminal records, and communications metadata for risk assessments and analytics. In a highly authoritarian context with a history of unlawful surveillance via spyware and internet monitoring targeting journalists, activists, and critics, MİRAS lacks transparency—an explanatory document was briefly posted then removed—and essential safeguards like judicial authorization, data minimization, retention limits, independent oversight, or remedies, violating Council of Europe standards under Article 8 of the European Convention on Human Rights. Human Rights Watch urges suspension of implementation, adoption of robust privacy protections, and international pressure from bodies like the Council of Europe to prevent entrenching unchecked surveillance powers - Human Rights Watch

ICE'S TERROR SPY NET NOW TARGETS IMMIGRANTS

IMAGE SOURCE: HERMAN LEGAL GROUP

Under the Trump administration, U.S. Immigration and Customs Enforcement (ICE) has transformed post-9/11 surveillance infrastructure—originally for counter-terrorism—into a vast "ICE surveillance state" focused on mass deportations targeting one million people annually, repurposing elite Homeland Security Investigations (HSI) agents for civil immigration enforcement. ICE fuses government databases (e.g., IRS, SSA, fingerprints via HART), commercial data brokers (Palantir's Falcon/Raven, Thomson Reuters CLEAR for utility/credit/vehicle records), license-plate readers, social media monitoring, and biometrics like Mobile Fortify app (facial recognition, fingerprints), Clearview AI, iris scanners, and reactivated spyware from Paragon (Graphite) and AT&T telecom data akin to the Hemisphere program, often bypassing warrants by purchasing data. This opaque, permanent system erodes oversight—gutting Privacy Office and CRCL—risks Fourth Amendment violations, misidentifies citizens/protesters (especially people of color), and enables retasking against dissenters like antifa, prompting civil liberties alarms over privacy, due process, and expansion beyond immigrants - Herman Legal Group

THE TRUMP ADMINISTRATION IS STRENGTHENING ITS SURVEILLANCE CAPABILITIES

IMAGE SOURCE: 1A

The Trump administration (2017-2021) strengthened surveillance capabilities through aggressive data seizures, including a 2018 DOJ subpoena of Apple iCloud metadata from House Intelligence Committee Democrats like Adam Schiff, their aides, and family members to probe Russia-related leaks, alongside phone/email records from CNN reporters under gag orders. Executive actions expanded inter-agency data sharing via firms like Palantir (securing $113M+ contracts for Foundry across DHS, HHS, etc.), merging government records with commercial sources to combat fraud but enabling broad tracking of Americans, immigrants, and alleged threats. Critics like ACLU warned of dragnet tools under FISA Section 702 and EO 12333 eroding privacy without warrants, while repurposing post-9/11 infrastructure risked mission creep toward monitoring protests and dissent - 1A

INTEL WATCH

Watching the watchers. Guarding the guardians.

A MESSAGE FROM THE TEAM: HAPPY HOLIDAYS!

As 2025 draws to a close, we reflect on a year that was defined by more than just the challenges we faced; it was defined by the community we built.

This year marked a significant milestone: the official launch of our newsletter, The Watcher. Since its inception, it has served as a critical platform for discourse on surveillance, privacy, and civil liberties across Africa and the world. However, a platform is only as strong as the voices that uplift it.

We owe a debt of gratitude to you—our subscribers, fellow human rights organisations, and global stakeholders. Your engagement, your rigorous debate, and your shared commitment to accountability have breathed life into this project.
In the spirit of sustainable advocacy, the Intelwatch team is signing off to rest and recharge. We will resume our work on 12 January 2026.

Thank you for walking this path with us. We wish you a restorative festive season.

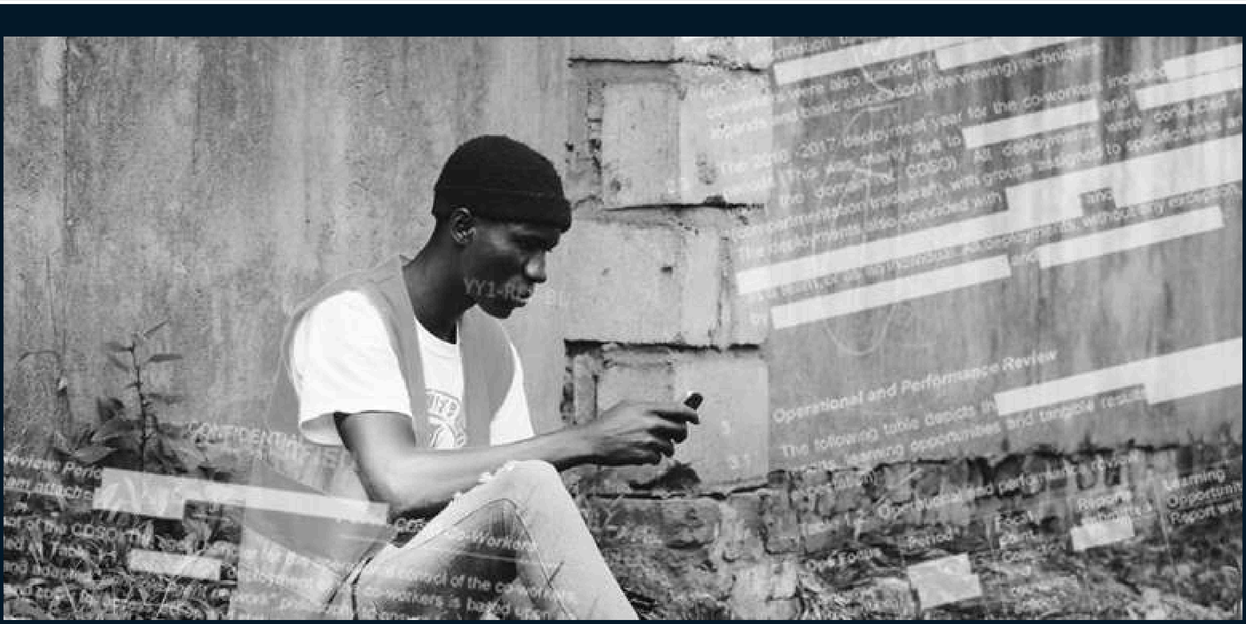
From the Executive Director and the Editorial Team

INTEL WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

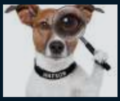
Sign up to get occasional news and briefings on intelligence oversight and surveillance reform in Southern Africa and beyond



FIND US ON SOCIAL MEDIA

𝕏 @IntewatchNews

HAVE ANY QUESTIONS?



✉ info@intelwatch.org.za

The Reynolds Foundation
Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!