Issue #9

INTEL WATCH

February 2026

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

INTELWATCH EXCLUSIVE REPORTS

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTELWATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

UNDER SIEGE: MAPPING THREATS TO THE MEDIA IN SOUTH AFRICA

BY NALEDI SIKHAKHANE AND MAGNIFICENT MNDEBELE

Executive Summary

This report by Naledi Sikhakhane and Magnificent Mndebele provides a comprehensive examination of the multifaceted threats to media freedom in South Africa.

South African journalists are trapped in a surveillance hellscape: Pegasus spyware infections targeting newsrooms, rampant RICA abuses bypassing safeguards, unchecked SSIA intercepts exploiting Section 205 loopholes for bulk data grabs, and a ballooning CCTV/biometric/AI ecosystem—deployed by the South African Police Service, private security firms, and smart city projects carried on without privacy impact assessments or judicial oversight. The report exposes legal black holes enabling state capture of comms metadata, corporate spyware sales to intelligence agencies, and algorithmic profiling chilling dissent amid corruption probes. The "digital dragnet" is an existential threat to press freedom and civic space, necessitating an urgent RICA overhaul, an introduction of transparency registers for surveillance technology, and civil society vetoes to prevent fully-fledged repression from normalising in the Rainbow Nation.

Download the full report here

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

A DEMOCRACY AT THE CROSSROADS: MAPPING THREATS TO THE MEDIA IN BOTSWANA

BY MMAPULA MOLAPONG*

Executive Summary

This Intelwatch report by Mmapula Molapong and her co-author who cannot be named for professional reasons, lifts the veil to expose a Democracy at the Crossroads in Botswana. For decades, Botswana has been celebrated as a beacon of democratic stability; however, the authors' findings reveal a precipitous decline in press freedom, with the country's global ranking plummeting from 42nd in 2015 to 81st in 2025. Despite a historic political transition in late 2024, the media environment remains perilous, characterised by a suffocating legal framework of archaic colonial-era laws and a new administration whose early rhetoric—including unsubstantiated claims of "fake news" and threats of imprisonment for journalists—suggests that state hostility has merely changed hands rather than vanished.

The report provides a forensic analysis of the multi-faceted pressures currently besieging the Fourth Estate, ranging from the weaponisation of the Penal Code to the rise of 'Strategic Lawsuits Against Public Participation' (SLAPPs) designed to bankrupt independent newsrooms. It also documents a 'Digital Panopticon' where sophisticated surveillance technology is used to intercept journalistic communications, alongside gendered cyber-harassment aimed at silencing female voices. Without urgent structural reforms and genuine political will, Botswana risks sliding toward information authoritarianism.

Download the full report here

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

MEDIA CAPTURE AND THE ILLUSION OF MEDIA PLURALITY: MAPPING THREATS TO THE MEDIA IN ZIMBABWE

BY INTELWATCH

Executive Summary

This new Intelwatch report reveals a harrowing landscape for Zimbabwean journalism under the Emmerson Mnangagwa-led government, where the 'Second Republic's' initial promises of reform have been replaced by a sophisticated system of "lawfare" and elite capture. While the appearance of a diverse media environment exists, the report uncovers how the distinction between state and private media has become dangerously porous, with politically connected proxy owners to ensure narrative alignment with the ruling ZANU-PF party. Beyond ownership, the state has entrenched its control through the Broadcasting Services Amendment Act of 2025, which grants the President direct authority over licensing boards and mandates "The Government Hour"—a weekly slot for state propaganda—on all broadcast platforms.

Journalists on the ground face an onslaught on all fronts, ranging from physical violence and arbitrary arrests to the weaponisation of the Cyber and Data Protection Act and the 'Patriot' clauses to criminalise investigative reporting. These legal threats are compounded by a "digital enclosure" that subjects podcasters and webcasters to the same restrictive conditions as traditional media, alongside dire economic conditions where reporters earn as little as US$100 a month, leaving them vulnerable to ethical compromises. The report concludes that without urgent legislative reform to repeal repressive statutes and restore regulatory independence, the media will continue to function as a tool for regime legitimation rather than a democratic watchdog.

Download the full report here

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

SUFFOCATE AND SILENCE: MAPPING THREATS TO THE MEDIA IN MOZAMBIQUE

BY ESTACIO VALOI AND DAVID MATSINHE

Executive Summary

Aptly titled “Suffocate and Silence’, this Intelwatch report by Estacio Valoi and David Matsinhe reveals a disturbing and systematic state strategy to dismantle independent journalism and control public discourse. The report documents an escalating crisis of "closing civic space," where the Mozambican government has weaponised legal, economic, and digital tools to silence critical voices. Major threats include proposed repressive media bills that would institutionalize censorship through a state-controlled regulator, alongside severe physical risks such as arbitrary detention, torture, and enforced disappearances. This environment of impunity—highlighted by the chilling disappearances of journalists like Ibrahimo Mbaruco and Arlindo Chissale—has fostered a climate of fear and self-censorship that undermines the very foundations of democracy in the country.

The crisis is particularly acute in the conflict-torn Cabo Delgado province, which has been transformed into a near-total information incognito zone where journalists face kidnapping and murder for attempting to report on human rights abuses. Beyond physical violence, the state exerts control through pervasive digital surveillance and economic pressure, such as the partisan allocation of advertising to hollow out the financial sustainability of independent outlets.

Download the full report here

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

MAPPING THREATS TO THE MEDIA IN NAMIBIA

BY PHILLIP SANTOS AND FREDERICO LINKS

Executive Summary

This Intelwatch report by Phillip Santos and Frederico Links provides a comprehensive analysis of the evolving challenges facing one of Africa's most respected media landscapes. While Namibia is often celebrated as a beacon of constitutional democracy with robust protections for press freedom, the authors' research reveals a concerning array of emerging threats that risk undermining this foundation. From the chilling effects of a complex state surveillance framework—bolstered by mandatory SIM card registration and data retention—to the persistent dangers of colonial-era defamation and sedition laws, the report details how legislative instruments are being used to constrict the space for independent journalism. Furthermore, the rise of digital technologies has created an existential economic crisis for legacy media, leaving them vulnerable to external control as advertising revenue shifts toward global tech giants.

The report also shines a necessary searchlight on the targeted harassment and online trolling of female journalists, highlighting how patriarchal attitudes continue to pose a significant barrier to a truly representative and democratic public sphere. Beyond identifying these risks, the report offers strategic recommendations for the alignment of national laws with constitutional ideals and safeguard the independence of the fourth estate.

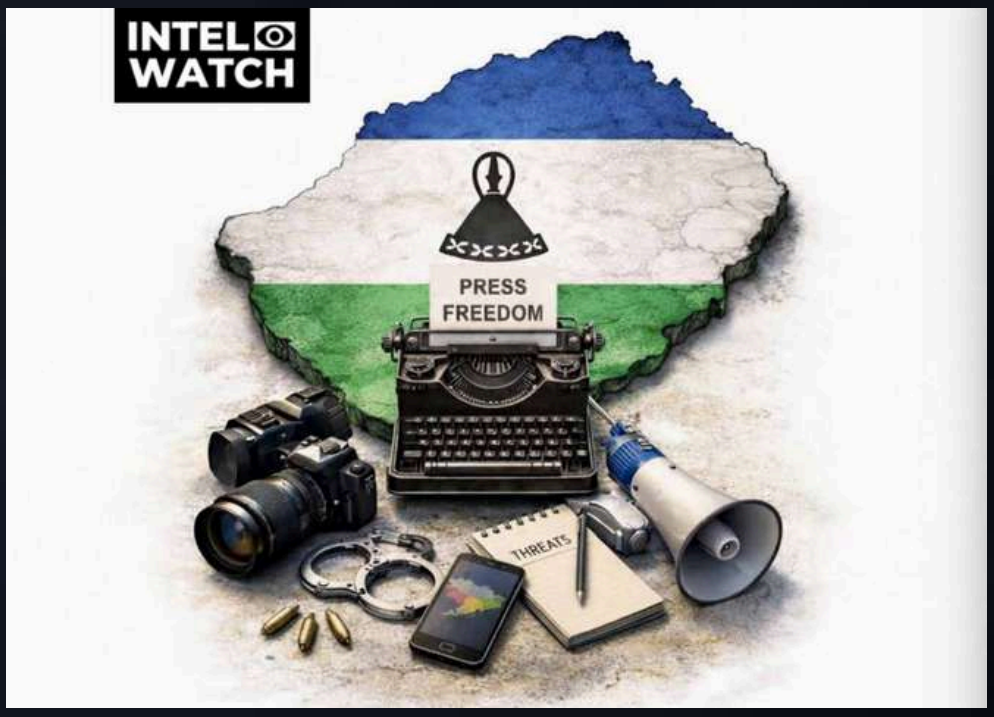
Download the full report here

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

MAPPING THREATS TO THE MEDIA IN LESOTHO

BY PASCALINAH KABI AND SECHABA MOKHETHI



Executive Summary

This Intelwatch report by Pascalinah Kabi and Sechaba Mokhethi reveals a deeply concerning environment where the democratic space for independent journalism in Lesotho is rapidly shrinking. Despite constitutional guarantees, the media is currently under siege from a maze of legal and regulatory threats, political capture, and economic coercion. There is the looming threat of the widely condemned Computer Crime and Cybersecurity Bill, which contains punitive clauses that could effectively criminalise investigative journalism and whistleblower activities under the guise of national security. This legislative overreach is compounded by the persistent delay in enacting an Access to Information law, leaving Lesotho as one of the few SADC nations without such a framework.

Beyond the law, the report highlights a distressing culture of impunity regarding the physical safety of journalists. The 2023 assassination of Ralikonelo Joki and the decade-long wait for justice in the army orchestrated shooting of Lloyd Mutungamiri underscore the severe risks faced by those who dare to speak truth to power. Additionally, female journalists are facing the twin threats of professional hazards and targeted gender-based violence.

Download the full report here

INTEL WATCH

Watching the watchers. Guarding the guardians.

EXCLUSIVE INTELWATCH REPORTS

A PRESS UNDER SIEGE: MAPPING THE MUTUALLY REINFORCING THREATS TO THE MEDIA IN ESWATINI

BY MAGNIFICENT MNDEBELE*

Executive Summary

This latest report reveals profound paradox where media freedom is constitutionally guaranteed in Eswatini but systemically besieged by an asphyxiating web of legacy laws, judicial weaponization, and economic capture.

From the strategic use of colonial-era statutes like the Sedition and Subversive Activities Act to the rise of ruinous "SLAPP" suits, the Eswatini government has engineered a hostile environment designed to stifle independent journalism and enforce a state-sanctioned narrative. The report highlights a critical inflection point in early 2025 with the acquisition of the Times of Eswatini Group by interests deeply intertwined with state power, further narrowing the space for genuine daily scrutiny of the monarchy and its corporate networks. Beyond legal and economic pressures, journalists now face a 'double jeopardy' of threats from both state repression and retributive violence from non-state actors. The findings detail how weak cybersecurity, state surveillance, and the collapse of self-regulatory bodies like the Media Complaints Commission have left the fourth estate more vulnerable than ever before. The report concludes that without urgent legal reform and renewed solidarity from the international community, the media sector faces a terminal slide toward managed propaganda.

Download the full report here

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

MORE THAN 40% OF SOUTH AFRICANS WERE SCAMMED IN 2025

IMAGE SOURCE: DARK READING

In 2025, South Africa grappled with a severe scam epidemic, with infoQuest's survey revealing 77% of adults targeted (57% in the prior 12 months, averaging three attempts each), 42% losing money—mostly R501-R5,000 (48% of cases)—via prevalent package/delivery scams (49%), phishing/SMS (41%), and job scams (39%), affecting all demographics uniformly. One-third of victims ("silent third") didn't report, primarily to banks (42%) or SAPS (32%), amid AI-powered deepfakes and digital banking fraud surges (65% of incidents, losses up to R1.4B), exploiting human error over technical breaches. SABRIC notes persistent threats despite 18% overall financial crime drop, urging vigilance against volume-based attacks - Dark Reading

SA FIRMS UNDER SIEGE: PHISHING & SOCIAL ENGINEERING TRAPS

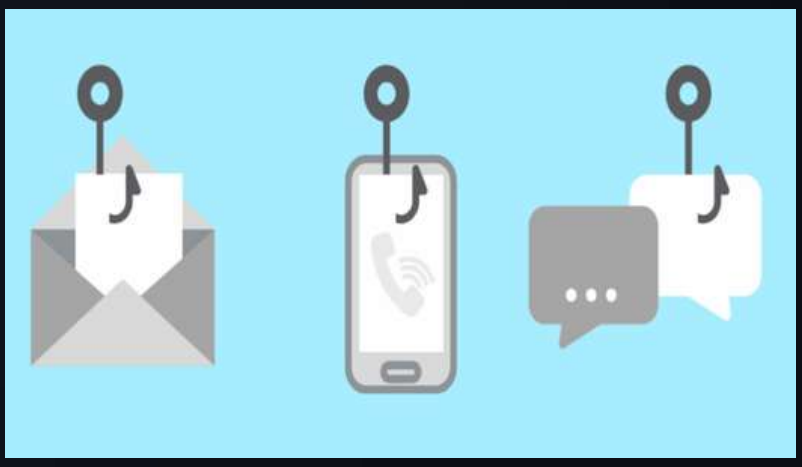


IMAGE SOURCE: TECH ECONOMY

ESET's H2 2025 Threat Report reveals phishing and social engineering as the dominant cybersecurity risks for South African organizations, accounting for 45.7% of detected threats—far exceeding Africa's 32.5% average—with attackers prioritizing monetizable initial access vectors amid global evolutions like AI-generated deepfakes, phishing sites, and ephemeral ad campaigns. Despite emerging AI-powered malware like PromptLock ransomware, traditional tactics prevail in SA, where NFC threats surged 87% exploiting card payments; Tony Anscombe, ESET's Chief Security Evangelist, stresses attacker focus on high-reward scams. Organizations must counter with layered defenses beyond URL blocking, as phishing kits democratize attacks via underground economies - Tech Economy

INTEL WATCH

Watching the watchers. Guarding the guardians.

SOUTH AFRICA FACES INCREASED CYBERATTACKS AGAINST GOVERNMENT AGENCIES

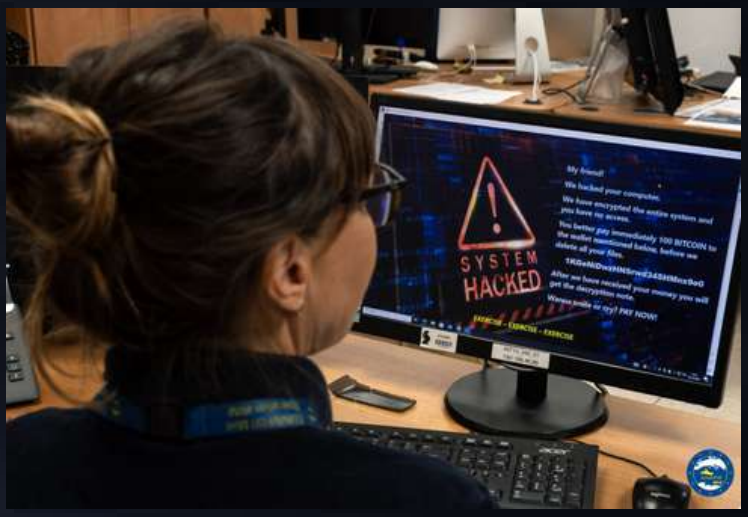


IMAGE SOURCE: DEFENCE WEB

South Africa grapples with surging cyberattacks on government and critical infrastructure, exemplified by the January 2025 South African Weather Service outage—disrupting aviation/marine forecasts regionally for Mozambique and Zambia—amid a 37% continental rise in 2024 (vs. 30% globally) per Check Point, with entities facing 1,450 attacks weekly. Breaches targeted the National Health Laboratory Service (blood tests halted), Companies and Intellectual Property Commission, $85B Government Employees Pension Fund, and State Security Agency pre-BRICS 2023, fueled by expanded attack surfaces and connectivity. Minister Khumbudzo Ntshavheni pledged accelerated National Cyber Security Framework rollout and Cyber Command enhancements, but experts like Adius Ncube urge strategic investment, integrated defenses, user education against phishing, and prioritization to avert inevitable major disruptions - Defence Web

---

DEEPFAKE SCAMS, AI MALWARE RAISE CYBER RISKS IN KENYA

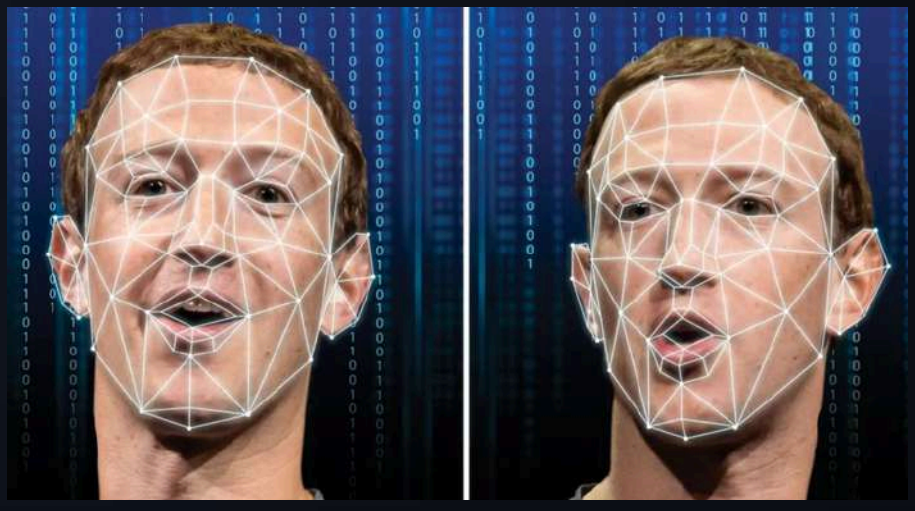


IMAGE SOURCE: CIO AFRICA

Kenya faces escalating cyber risks from AI-enhanced deepfake scams—such as investment fraud using hyper-realistic videos impersonating politicians—and AI-generated malware like PromptLock ransomware (first detected H2 2025), per ESET's Threat Report (June-November 2025), with social engineering via deepfakes, phishing sites, and Nomani scam variants (up 62% globally) dominating threats amid underreported ransomware. ESET experts like Allan Juma highlight rapid spread through social media and ads, urging organizations to bolster defenses beyond traditional tools as AI democratizes sophisticated attacks previously limited by technical skill - Cio Africa

INTEL WATCH

Watching the watchers. Guarding the guardians.

NIGERIA CYBER STORM: RANSOMWARE & PHISHING INVASION LOOMS

IMAGE SOURCE: TECH AFRICA NEWS

Deloitte's Nigeria Cybersecurity Outlook 2026 warns of intensifying ransomware and phishing threats as digital services, payments, and data rapidly migrate online, with Nigeria ranking third in Africa for 2024 phishing incidents (3,459 cases per Interpol) amid $3 billion cybercrime losses from 2019-2025 (~$500M annually). Attackers leverage accessible AI for hyper-realistic impersonations of banks/colleagues/regulators, enabling system infiltration, data exfiltration, encryption, and ransom demands—targeting SMEs, hospitals, schools, and agencies with limited cybersecurity—while broader African trends amplify risks via social engineering and instant messaging. Deloitte urges affordable resilience via staff awareness, Zero Trust frameworks, AI-human threat detection, strong account protections, activity monitoring, and recovery plans, stressing early preparation over complex solutions - Tech Africa News

SENEGAL'S NATIONAL ID HACKED: RANSOMWARE EXPOSES MILLIONS

IMAGE SOURCE: THE RECORD

Senegal's Directorate of File Automation (DAF), responsible for national ID cards, passports, and biometric data, confirmed a ransomware breach by the Green Blood Group after servers were compromised on January 19, 2026, forcing temporary closure of services and disrupting issuance for 19.5 million citizens. The group claims to have exfiltrated 139GB (or up to 139TB per some reports) of sensitive data including citizen records, biometrics, immigration files, and backups, leaking samples and an IRIS Corporation (Malaysian ID system supplier) executive email as proof, with Senegal Numérique SA also hit. Officials insist data integrity remains intact pending investigation and restoration, while IRIS dispatched experts; the incident exposes legacy infrastructure vulnerabilities in biometric systems - The Record

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI FUELS AFRICA'S CYBER ONSLAUGHT

IMAGE SOURCE: IT ONLINE

Check Point warns that African organizations face 3,153 weekly cyberattacks—60% above global averages—as AI-driven threats dominate 2026, with autonomous "agentic AI" outpacing governance in Kenya, Nigeria, and South Africa, mainstream deepfake fraud via voice cloning/SIM swaps (R5B+ annual SA losses), and cloud misconfigurations surpassing malware in hybrid environments. Other trends include AI-enhanced ransomware, IoT/OT vulnerabilities in leapfrogging infrastructure, supply chain risks, and quantum threats demanding prevention-first resilience through public-private collaboration amid systemic digital risks - IT Online

AI BLIND TO GENDER: AFRICAN WOMEN EXPOSED

IMAGE SOURCE: DEV DISCOURSE

A new study in AI & Society reveals that gender-blind AI design in African healthcare, finance, education, and digital ID systems amplifies privacy risks for women, whose concerns encompass bodily integrity, reputation, and social standing beyond standard data protection—leading to coerced data disclosure, surveillance repurposed for patriarchal control, and exclusion from datasets that perpetuate bias. Women often limit participation as self-protection, skewing AI models further against them amid weak laws and non-participatory design; the proposed Gender Equality and Inclusion by Design (GEIbD) framework urges embedding gender analysis, continuous risk checks, inclusive stakeholder input, capacity building, and rights-based governance throughout AI lifecycles to prevent structural harms - Dev Discourse

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI CODE HACK: BBC REPORTER'S LAPTOP SEIZED ZERO-CLICK

IMAGE SOURCE: BBC

A BBC reporter's laptop was remotely hacked via Orchids, a popular "vibe-coding" AI platform that lets non-coders build apps through text prompts, when cybersecurity expert Etizaz Mohsin exploited an unresolved flaw to inject malicious code into the reporter's project without any clicks, downloads, or warnings—changing the wallpaper to a hacker skull and granting full file access in seconds. This zero-click vulnerability, discovered in 2025 but ignored despite repeated alerts to Orchids' small team, highlights risks in agentic AI tools that autonomously execute code, potentially enabling spyware or ransomware; experts like NordPass's Olis Arbuskas urge isolated testing environments, as similar platforms like Claude Code remain untested amid surging no-code adoption - BBC

FAKE ZOOM TRAP: STEALTH SPYWARE SNEAKS IN

IMAGE SOURCE: CSO

Malwarebytes uncovered a phishing scam where fake Zoom meeting invites at uswebzoomus[.]com lure victims into a convincing waiting room, complete with scripted participants like "Matthew Karlsson" and looping audio chimes, triggering a deceptive "Update Available" prompt amid simulated network issues that downloads and silently installs a covert version of Teramind—legitimate enterprise surveillance software abused for unauthorized monitoring. The installer runs in "Hidden Agent" mode without taskbar icons, system tray entries, or Add/Remove Programs visibility, using proxy tunnels to mask data theft, aggressive self-restart services, and preconfigured attacker servers to log keystrokes, screenshots, and activity undetected by many antivirus tools, affecting nearly 1,500 Windows users in 12 days. Experts urge treating affected machines as compromised and warn of similar Google Meet variants amid rising corporate tool abuse - CSO

INTEL WATCH

Watching the watchers. Guarding the guardians.

HACKERS RACE TO CLONE GEMINI FOR CYBERATTACKS

IMAGE SOURCE: PC MAG

Google's Threat Intelligence report reveals state-backed hackers from North Korea, Iran, China, and Russia exploiting Gemini AI for cyber reconnaissance, phishing, malware generation like fileless HONESTCUE, and "model extraction" attacks using over 100,000 API prompts to steal proprietary reasoning logic—distinct from traditional hacks via authorized developer access. While no successful cloning occurred, private firms and researchers probed for IP theft to replicate financial or coding models unregulated, prompting Google to bolster defenses and warn AI developers of rising distillation threats amid agentic AI misuse in operations. North Korea's UNC2970 and Iran's APT42 notably used Gemini for target intel, tailored social engineering, and local-context translation before disruptions - PC Mag

---

IPHONE SPYWARE SILENTLY SILENCES APPLE'S PRIVACY DOTS

IMAGE SOURCE: FORBES

Jamf researchers reveal Intellexa's Predator spyware bypasses iPhone's orange (mic) and green (camera) indicators—introduced in iOS 14—by gaining kernel-level access to intercept sensor activity before it triggers SpringBoard UI updates, nullifying Objective-C self-pointers in private frameworks to silently drop recording state changes without errors or visible alerts. Unlike device shutdown mimics, Predator keeps the phone fully functional while its VoIP module captures audio/video undetected, evading legitimate app restrictions amid recent Apple spyware notifications tied to iOS 26.3 updates. Users should watch for overheating, slowdowns, or odd apps; restarts disrupt it temporarily, but experts advise isolating suspect devices as these findings aid forensic detection of commercial spyware eroding core iOS privacy - Forbes

INTEL WATCH

Watching the watchers. Guarding the guardians.

META GLASSES UNLEASH SECRET FACE SCANS

IMAGE SOURCE: WEB PRO NEWS

Users have demonstrated real-time facial recognition on Meta's Ray-Ban smart glasses using third-party apps and on-device AI, sparking a privacy firestorm by silently identifying strangers via Meta's vast social graph without consent or visible indicators—bypassing the white LED meant to signal recording. The "Name Tag" feature, eyed for 2026 rollout under "super sensing" upgrades like Aperol and Bellini models, lets wearers query names, profiles, or connections (e.g., Instagram public accounts) amid Zuckerberg's push for always-on AI that logs daily life, raising stalking, doxxing, and mass surveillance fears despite internal safety debates. Critics decry weakened privacy oversight, urging opt-out tools and LED enforcement as countermeasures proliferate, like apps alerting to nearby scanning glasses - Web Pro News

CHINA'S APTS UNLEASH ELITE MALWARE ON ASIA

IMAGE SOURCE: DARK READING

Chinese-linked advanced persistent threat groups, including those tied to APT41 (Earth Baku) and APT31 (Fireant), are hammering Southeast Asian targets—government ministries, air traffic control, telecoms, and media—with sophisticated espionage tools like Rakshasa proxy, DLL sideloading via old Bitdefender files, custom keyloggers, and SharpGPOAbuse since late 2023. These actors blend living-off-the-land techniques with high-end implants for credential theft and data exfiltration, lingering months undetected across sectors to harvest intelligence amid regional tensions. While exact attribution varies, the tool overlap and geographic focus point to state-backed operations prioritizing espionage over disruption, urging Asian orgs to hunt for these TTPs in hybrid environments - Dark Reading

WHATSAPP IMPLEMENTS SHIELD AGAINST SPYWARE AND PHISHING

IMAGE SOURCE: MIX VALE

WhatsApp has rolled out "Strict Account Settings"—a one-tap lockdown mode for journalists, activists, and high-risk users—automatically blocking media/attachments from unknown senders, disabling link previews to thwart spyware-laden thumbnails, silencing calls from strangers, enforcing two-step verification, and restricting profile visibility (last seen, photo, about) to contacts only while limiting group adds. This "maximum protection" complements end-to-end encryption with backend hardening like CFI, safer memory allocators, and IP-masking call routing, trading convenience for defense against advanced phishing and surveillance amid rising state-sponsored threats. Available globally via Settings > Privacy > Advanced on primary devices (not web/desktop companions), it mirrors Apple's Lockdown Mode for elite threat protection - Mix Vale

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

ANGOLA: PROMINENT JOURNALIST HACKED WITH PREDATOR SPYWARE

IMAGE SOURCE: AMNESTY

Amnesty International confirmed Predator spyware—sold by Intellexa to governments for surveillance—targeted Teixeira Cândido, prominent Angolan journalist, press freedom activist, and ex-Secretary General of the Syndicate of Angolan Journalists, via WhatsApp phishing in May 2024. After rapport-building, attackers sent fake news links from April, with Cândido clicking one on May 4, granting full iPhone access to microphone, camera, messages, and data undetected; forensic traces tied it to Predator domains, marking Angola's first verified case amid a suspected broader campaign since 2023. Cândido described feeling "naked," demanding accountability as Angola tightens press controls pre-2027 elections; Amnesty urges spyware bans and investigations into buyers - Amnesty.

OFFLINE AND SILENCED: AFRICA'S QUIET RISE OF INTERNET REPRESSION

IMAGE SOURCE: INFRASTRUCTURE NEWS

Africa faced a record 21 internet shutdowns across 15 countries in 2024—its worst year—escalating to 28 continent-wide in 2025 amid elections and protests, with Tanzania's nationwide blackout on October 29 voting day, Ethiopia's 30 systematic cuts since 2016, Senegal's February 2024 protest silencing, and conflict-driven outages in Sudan/DRC crippling transparency and economies. These "national security" pretexts cost sub-Saharan Africa $1.6 billion in 2024 alone, devastating mobile money, humanitarian aid, and 1.5 million jobs while telecoms comply under license threats despite the African Commission's 2024 anti-shutdown resolution. Globally, 296 disruptions hit 54 nations as governments normalize digital repression, blocking dissent documentation and narrative control amid weak enforcement - Infrastructure News

INTEL WATCH

Watching the watchers. Guarding the guardians.

CELLEBRITE USED ON KENYAN ACTIVIST AND POLITICIAN BONIFACE MWANGI

IMAGE SOURCE: CITIZEN LAB

Citizen Lab confirmed Kenyan police used Cellebrite's forensic extraction tools on prominent activist and 2027 presidential hopeful Boniface Mwangi's Samsung phone during his July 19, 2025 arrest amid anti-government protests, removing its password protection and potentially dumping all messages, photos, files, financial data, and passwords without his consent. Traces of Cellebrite's "com.client.appA" app appeared on July 20-21 while the device was in custody, fitting a pattern of surveillance abuses including FlexiSPY on filmmakers and warrantless NIS wiretaps targeting dissenters. Mwangi felt deeply violated, exposing family photos and campaign plans; researchers slam Cellebrite's lax vetting of rights-abusing regimes and demand it halt sales to Kenyan agencies - Citizen Lab

---

SAUDI SPY HACK ENDS IN LONDON BEATDOWN

IMAGE SOURCE: BBC

YouTuber Ghanem al-Masarir, a Saudi dissident whose satirical videos mocking Crown Prince Mohammed bin Salman racked up 345 million views, had his iPhones infected with NSO Group's Pegasus spyware in 2018 via phishing texts disguised as news offers, enabling full surveillance of his location, calls, camera, and microphone. This fueled relentless stalking by apparent regime supporters in London—repeated street harassment, a child singing pro-King Salman praises on camera, death threats like "Your days are numbered"—culminating in a premeditated August assault outside Harrods by two men with an earpiece who punched him while yelling about his criticisms, as confirmed by forensic experts from Citizen Lab. In January 2026, London's High Court ruled Saudi Arabia liable, awarding al-Masarir over £3 million ($4.1M) for the hack, attack, lost YouTube income, and trauma-induced depression that derailed his career; he now lives reclusively in Wembley, uncertain if Riyadh will pay - BBC

INTEL WATCH

Watching the watchers. Guarding the guardians.

RUSSIA BOOTS WHATSAPP, SHOVES SPY APP ON 100M USERS

IMAGE SOURCE: G BLOCK

Russia fully blocked WhatsApp on February 12, 2026, after throttling it since 2025—citing Meta's "extremist" status and failure to store user data locally or delete "banned content"—to herd over 100 million users onto state-owned Max, a WeChat-style super-app lacking end-to-end encryption for easy Kremlin surveillance of messages, calls, and government services. Pre-installed on all new devices since 2025 and mandated for public workers/students, Max integrates payments and IDs while Roskomnadzor accuses WhatsApp of enabling fraud/terrorism; Meta slammed the move as regressive, endangering privacy amid Ukraine war dissent crackdowns. Critics like Amnesty decry it as transparent digital repression, with VPNs now essential as Telegram faces similar curbs - G Block

---

ICE'S SURVEILLANCE APP IS A TECHNO-AUTHORITARIAN NIGHTMARE

IMAGE SOURCE: THE GUARDIAN

TICE's Mobile Fortify app turns agents' smartphones into portable biometric scanners, capturing faces or contactless fingerprints in real-time against 200M+ image and 270M-record federal databases like IDENT, CBP's Traveler Verification Service, FBI files, and State Department visas—yielding instant hits on immigration status, criminal history, or travel data without warrants or office returns. Deployed since May 2025 and used 100,000+ times (including on children), it enables street-level checks at protests, neighborhoods, or buses, misusing border photos for inland policing amid known facial recognition errors and DHS security lapses allowing risky apps. Critics decry this unchecked mission creep as techno-authoritarianism chilling free speech, with senators demanding halts and lawsuits exposing its dragnet on citizens - The Guardian

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTELLIGENCE AGENCIES

AFRICA'S DIGITAL ID BOOM SPARKS SURVEILLANCE FEARS

IMAGE SOURCE: TECH AFRICA NEWS

Forty-nine African nations have embraced digital ID systems by early 2026, with 35 deploying biometrics for elections, financial inclusion, and services—covering over 500 million registrations continent-wide via AU-backed interoperability frameworks that link IDs to mobile money, health, and governance, potentially unlocking 3-13% GDP growth per UNECA estimates. Pioneers like Rwanda (98% adult coverage), Benin, Malawi, Tanzania, and Somalia tout streamlined welfare, counter-terrorism, and cross-border verification, yet critics flag data breaches in Kenya/Nigeria, exclusion of 500 million ID-less citizens (especially refugees/displaced), weak privacy laws, and surveillance risks as authoritarian regimes exploit centralized biometrics for repression without robust cybersecurity or consent. Amid 2026's continental DPI push, calls grow for harmonized regulations balancing innovation against mass tracking threats - Tech Africa News

EPSTEIN & BARAK PIMP PALESTINIAN-TESTED SPY TECH TO NIGERIA

IMAGE SOURCE: ALJAZEERA

A Drop Site News investigation uncovers how Jeffrey Epstein and ex-Israeli PM Ehud Barak exploited Nigeria's Boko Haram crisis over a decade, marketing "field-proven" biometric surveillance—initially battle-tested on Palestinians at Gaza's Erez crossing—to Nigerian officials for profit in oil and logistics. Barak invested $15M in FST Biometrics (co-founded by ex-Israeli intel chief Ze'i Farkash), securing deals like facial recognition at Babcock University and Ogun State campuses framed as counter-terror "crowd filtering," while embedding cyber expertise via World Bank projects and Elbit Systems' internet surveillance despite legislative resistance. DOJ emails reveal Epstein's guidance turning security ties into DP World port bids and energy ventures, raising alarms over Israeli firms' African expansion using occupation-honed tools amid Nigerian instability - Aljazeera

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI ACCENTS FUEL INDIA'S MUSLIM WITCH HUNT

IMAGE SOURCE: FRONTLINE

Maharashtra's BJP government and IIT Bombay are building a 60% accurate AI tool to flag "illegal" Bangladeshi migrants and Rohingya refugees by profiling speech patterns, tone, and language, despite linguists warning that Bengali dialects span West Bengal, Assam, and Bangladesh—ensuring massive false positives against Indian citizens. In a climate of BJP-fueled suspicion, this pseudoscience risks automating lynchings and deportations of poor Bengali Muslim workers, as seen in 2025 Odisha mob killings and Maharashtra expulsions later reversed amid trauma. Opaque datasets and overlap with Gaza-style algorithmic oppression signal state-encoded bigotry, not border security, as India hosts an AI summit preaching ethics abroad while weaponizing it at home - Frontline

TRUMP SPYWARE BLITZ ARMS ICE AGAINST "OVERTHROW" THREATS

IMAGE SOURCE: AOL

The Trump administration unleashed a massive spyware spending spree post-July 2025 funding bill, funneling over $170 billion to ICE—including $1.4 billion in September contracts—for eye-scanning apps from B12 Technologies ($4.6M, verifying identities from 15 inches even through glasses), Clearview AI facial recognition ($3.75M despite error-prone arrests), warrantless phone tracking from PenLink processing billions of daily location signals from hundreds of millions of devices, and Paragon Solutions spyware restarted at $2M for remote hacks of encrypted apps. This arsenal targets undocumented migrants and alleged domestic threats like protesters, with expanded social media monitoring hubs in Vermont/California probing targets' families/coworkers on Facebook, Instagram, and X, amid ACLU cries of First/Fourth Amendment violations and mission creep into citizen surveillance. Critics decry the unchecked escalation as techno-authoritarianism, with congressional oversight demands ignored in the deportation push - AOL

INTEL WATCH

Watching the watchers. Guarding the guardians.

ISRAEL'S ZERO-CLICK SPY ENGINE POWERS WESTERN AGENCIES

IMAGE SOURCE: EURO NEWS

Radiant Research Labs, founded in May 2023 by ex-IDF Unit 8200 operatives Tal Slomka and Tzvika Moshkowitz—both NSO Group veterans—has rapidly developed ten classified zero-click cyber tools that infiltrate phones and computers without user interaction, no links or files required, focusing on the core "engines" behind hacks rather than end-user spyware like Pegasus. Post-October 7, Radiant aided IDF intelligence in tracking hostages, while selling exclusively to democratic allies like the US, UK, Canada, Australia, NZ, Netherlands, France, Germany, Japan, and South Korea under Israel's defense export strategy ensuring "ethical standards." Amid US sanctions on NSO/Intellexa for journalist targeting, the Trump administration embraces such offensive capabilities aligning with its priorities, as Radiant plans confidential defense conferences with top Israeli cyber officials - Euro News

UK POLICE TO USE AI FACIAL RECOGNITION TECH LINKED TO ISRAEL'S WAR ON GAZA

IMAGE SOURCE: ALJAZEERA

UK police will deploy Corsight AI's facial recognition software nationwide via 50 live-scanning vans under a £20M Home Office contract awarded to Digital Barriers, despite the Israeli firm's tech integration into IDF Gaza operations where intelligence officials privately question its accuracy amid genocide allegations. Announced January 26, 2026, as part of sweeping reforms including a £115M Police.AI hub, the expansion targets watchlists, missing persons, and deterrence—expanding from 10 vans—while civil liberties groups warn of mass surveillance normalization, bias against minorities, and ethical conflicts given Corsight's role in Palestinian profiling. Oversight includes a public AI register and data standards, but campaigners decry unchecked rollout echoing Israel's occupation toolkit now policing British streets - Aljazeera

INTEL WATCH

Watching the watchers. Guarding the guardians.

APPLE BUYS SECRETIVE ISRAELI FACE TECH

IMAGE SOURCE: THE CRADLE

Apple acquired Q.ai, a low-profile Israeli startup specializing in AI-driven facial surveillance and micro-expression analysis, in a reported $2 billion deal—its second-largest ever after Beats—led by serial entrepreneur Aviad Maizels, whose prior firm PrimeSense powered iPhone Face ID. Q.ai's tech deciphers facial movements for emotion detection, whispered speech interpretation in noisy settings, and enhanced imaging, positioning Apple to dominate AI wearables like smart glasses against Meta and Google amid intensifying multimodal AI races. Critics raise alarms over privacy as this secretive firm's capabilities—previously unmarketed publicly—bolster Apple's Siri upgrades and Vision Pro, potentially enabling pervasive emotion-tracking surveillance despite the company's privacy brandings - The Cradle

---

FLORIDA BILL COULD UNLEASH SWEEPING NEW SURVEILLANCE POWERS

IMAGE SOURCE: ST AUGUSTINE

Florida's HB 945 and SB 1712, advancing through the 2026 legislative session, would create a secretive FDLE counterintelligence unit to detect, identify, and neutralize "adversary intelligence entities"—defined as persons whose actions, views, or opinions threaten state or US interests—via "patterns of life" analysis and arrests without oversight, sparking civil liberties alarms over viewpoint-based surveillance. Sponsored by Republicans Danny Alvarez and Jonathan Martin, the bills fund a 10-person leadership team overseeing seven regions, mirroring federal efforts but lacking guardrails, as critics like Sen. Carlos Guillermo Smith and First Amendment Foundation's Bobby Block warn of political policing amid paired measures labeling groups "domestic terrorists" and shielding designations in secrecy. Paired with Cellebrite funding requests for FDLE and State Guard, the proposals risk constitutional erosion, with the session ending March 13 - ST Augustine

INTEL WATCH

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

INTEL WATCH

Watching the watchers. Guarding the guardians.

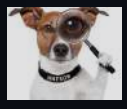
GET INVOLED!

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

FIND US ON SOCIAL MEDIA

@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!