Issue #10

INTEL WATCH

March 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

Repost

INTEL WATCH

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

HAVE YOU READ THE REPORT? LET US KNOW WHAT YOU THINK

Repost

INTELWATCH

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

HAVE YOU READ THE REPORT? LET US KNOW WHAT YOU THINK

Repost

INTEL WATCH

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

Repost

INTELWATCH

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

Repost

INTEL WATCH

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

Repost

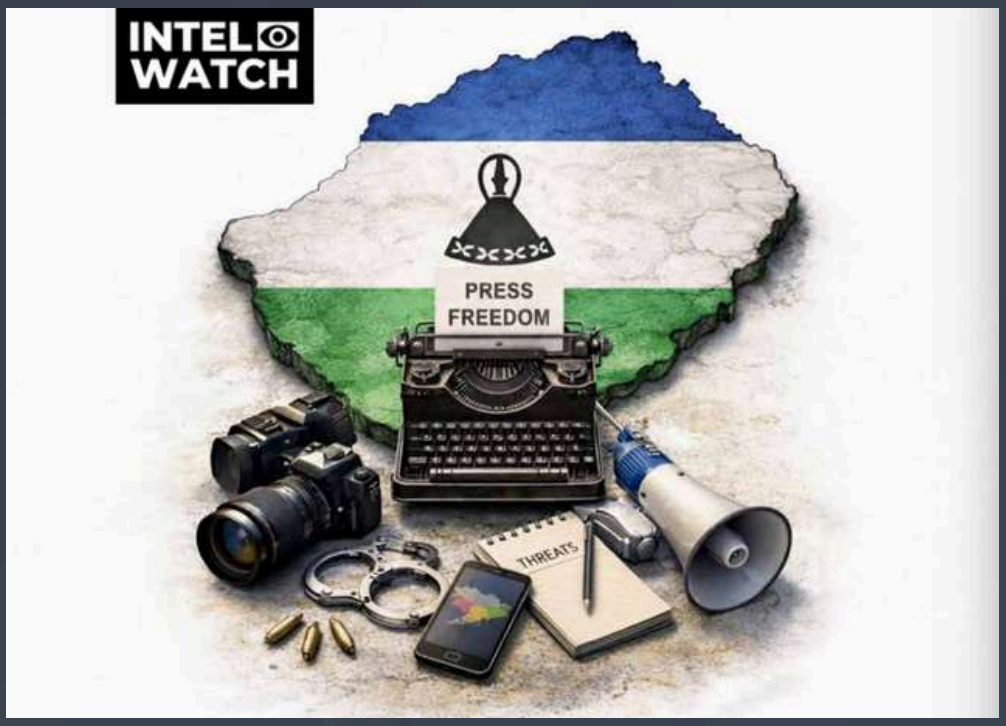
INTEL WATCH

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

Repost

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

STATS SA BREACHED IN CYBERATTACK

IMAGE SOURCE:BUSINESS TECH

South Africa's national statistics agency StatsSA has confirmed that it was breached in a ransomware cyberattack by a criminal group called XP95, which claims to have stolen over 450000 files (about154GB) of data from its human-resources database and is demanding roughly $100000 (about R1.7million) in ransom to prevent a public leak. The agency says the breach affected only its HR system used for job applications and that it will not pay the ransom, and has notified the country's information regulator while participating in a wider government response to growing cybersecurity threats affecting public entities, including another recent attack on the Gauteng Provincial Government. Experts see this as part of a broader rise in cyberattacks on sensitive government systems in South Africa – Business Tech

SOUTH AFRICA'S WEALTHIEST PROVINCE HIT BY MAJOR DATA HACK - PERSONAL RECORDS ON SALE FOR R420K

IMAGE SOURCE: MY BROADBAND

EA cybercrime group known as XP95 has claimed responsibility for hacking systems belonging to the Gauteng Provincial Government, South Africa's richest province, stealing about 3.8TB of personal data and offering the files for sale online for roughly R420,000 (~$25,000). The stolen information reportedly includes data from people who applied for government jobs, and samples shared on cybercrime channels suggest the breach gave attackers access to sensitive records that could be misused for identity theft or scams. This incident is part of a broader rise in cyberattacks against government and public sector systems in the country, highlighting ongoing risks to personal information and the need for stronger cybersecurity protections – My Broadband

SOUTH AFRICA TOPS AFRICA'S DEEPFAKE FRAUD RATES AS AI SCAMS EXPLODE

IMAGE SOURCE: WEETRACKER

According to the 2026 Digital Identity Fraud Report by Smile ID, South Africa currently records the highest deepfake-driven fraud rate in Africa, with about 22 % of fraud cases involving AI-generated impersonation and spoofing during biometric identity checks, as cheap and accessible AI tools are now used to create convincing fake videos, cloned voices and synthetic faces to bypass verification systems and exploit stolen data. Criminals are increasingly using these AI technologies to defeat liveness detection and impersonate both individuals and trusted figures in scams, leading to large-scale "injection attacks" and fraud attempts across financial services, while experts warn that fraud is shifting from traditional hacking to continuous deception of digital identity systems at scale - Weetracker

IRAN WAR ISN'T JUST PHYSICAL - SOUTH AFRICA'S NETWORKS FEELING THE CYBER-HEAT TOO

IMAGE SOURCE: CITIZEN

KThe article reports that South African organisations are facing a rise in cyber threats and breaches as global tensions from the conflict involving Iran escalate, with experts warning that hacktivist campaigns and opportunistic attackers are widening their targets beyond the Middle East into countries like South Africa. According to cybersecurity researchers, breaches in the country happen on average every few hours and most attacks could be prevented with stronger defenses, but fragmented systems and rapid digital adoption create vulnerabilities that can be exploited for data theft and disruption. The rising geopolitical conflict, coupled with broader global cybercrime patterns, means local businesses, government systems and critical infrastructure must improve their cybersecurity posture or risk costly intrusions and data loss - Citizen

NIGERIA TOPS AFRICA'S SURVEILLANCE SPENDING: SMART CITY TECH RAISES PRIVACY ALARMS

IMAGE SOURCE: EXTENSIA

According to recent research, Nigeria has become Africa's largest buyer of "smart city" surveillance technology, spending hundreds of millions of dollars on AI-enabled cameras and monitoring systems primarily supplied and financed by Chinese firms as part of broader smart city infrastructure deals, which also include facial recognition and vehicle-tracking tools. Researchers warn that this rapid expansion of public surveillance tech is happening with little legal oversight or safeguards for privacy, risking intrusive monitoring of citizens—including activists, journalists and ordinary people—without evidence the systems actually reduce crime, and raising broader concerns about human rights and government transparency across the continent - Extensia

HIGH-LEVEL WHATSAPP SCAM BUSTED IN TANZANIA — OFFICIALS TARGETED IN ELABORATE FRAUD RING

IMAGE SOURCE: PAN AFRICAN VISIONS

SenegA sophisticated WhatsApp fraud ring targeting influential Tanzanian officials—posing as government ministers to solicit urgent cash transfers—was exposed and dismantled in Tabora, after the Regional Commissioner narrowly avoided being defrauded and reported the scam to police, leading to the arrest of the suspect operating a scam hub with multiple phones and SIM cards. The incident highlights how cybercriminals are increasingly focusing on high-profile targets, exploiting trust and official imagery to deceive victims, with Tanzania's rapid growth in mobile and internet usage creating fertile ground for such fraudulent schemes that can cause significant financial and reputational harm – Pan African visions

SPYWARE & STOLEN PASSWORDS SURGE IN KENYA — ATTACKS JUMP 83% IN 2025

IMAGE SOURCE: AFRICA BUSINESS COMMUNITIES

The article reports that Kenya saw a dramatic 83% increase in spyware and password-theft attacks in 2025, driven by cybercriminals exploiting phishing, malicious apps, and social engineering to steal login credentials and install surveillance malware on devices. According to cybersecurity firms cited in the report, these attacks targeted both individuals and organisations—often through deceptive SMS links or fake apps—leading to stolen data, financial loss, and increased risks of identity theft. Experts warn that as digital adoption grows across the country, people and businesses with weak security practices remain especially vulnerable, pushing for stronger awareness campaigns, two-factor authentication, and better cybersecurity measures to protect citizens from rising digital threats – Africa Business Communities

MALWARE ON THE RISE: NIGERIANS URGED TO GUARD AGAINST DATA-STEALING THREATS

IMAGE SOURCE: PREMIUM TIMES

Cybersecurity firm Kaspersky has warned that Nigeria is experiencing an increase in malware designed to steal personal data from phones and computers, with attackers using tactics like phishing emails, fake apps, and malicious links to trick users into installing harmful software. These malicious programs can capture sensitive information such as passwords, banking details and personal files, putting individuals and businesses at risk of fraud and identity theft. Kaspersky's alert urges Nigerians to strengthen their digital habits by updating software, avoiding suspicious links, using security tools, and being cautious about downloads—highlighting that as more people go online, basic cybersecurity awareness becomes crucial to protect against growing cyber threats – Premium Times

AFRICA'S 'SMART CITIES' ARE BECOMING SURVEILLANCE STATES, WARN RESEARCHERS

IMAGE SOURCE: IDS

A new report by the Institute of Development Studies highlights the rapid expansion of AI-enabled "smart city" surveillance technologies across at least 11 African countries, including facial recognition cameras, automatic number-plate readers, and centralised control centres, mostly funded through Chinese loans and contracts. Researchers warn these systems are being deployed widely without strong legal safeguards for privacy or oversight, leaving citizens—especially political critics, journalists, and opposition groups—vulnerable to intrusive monitoring under the guise of modernising cities or fighting crime. The study finds no clear evidence that these mass surveillance systems have reduced terrorism or serious crime, and instead stresses that unregulated use of smart city tech threatens fundamental rights like privacy, freedom of movement, and expression - IDS

DIGITAL EYES ON THE BALLOT: EAST AFRICA'S ELECTIONS AT RISK FROM SURVEILLANCE

IMAGE SOURCE: THE STAR

Experts are warning that elections in East Africa—including in countries like Kenya, Tanzania, and Uganda—are increasingly vulnerable to digital surveillance and manipulation, as governments and other powerful actors deploy sophisticated technologies that can track voters, monitor online activity, and potentially influence political behaviour. Concerns include the use of mobile phone metadata, social media monitoring, biometric databases and AI tools to profile citizens, suppress dissent, or target opposition supporters, with critics arguing that weak legal protections and limited transparency make it easier for surveillance to be misused. Observers say such digital threats could undermine the fairness and credibility of elections, intimidate voters, and skew public discourse unless stronger safeguards and oversight are adopted before and during electoral processes – The Star

LEFT OUT AND LEFT BEHIND: HOW BIOMETRIC IDS IN AFRICA ARE BLOCKING ACCESS TO RIGHTSHACKERS RACE TO CLONE GEMINI FOR CYBERATTACKS

IMAGE SOURCE: PC MAG

New research shows that as biometric digital-ID systems roll out across many African countries, millions of people are being effectively excluded from essential services and basic rights because they cannot access or successfully register with these systems. These digital identity programmes—using fingerprints, facial scans and other personal data—have become tied to services like voting, healthcare, education and social protection, but factors such as disability, lack of technology, cost and mistrust mean many citizens struggle to enrol or choose not to participate. The report highlights that most biometric ID systems lack strong legal protections for privacy and data security, and without safeguards, these tools risk deepening inequality and locking vulnerable groups out of fundamental public services – PC Mag

WHY DRONES ARE SEEN AS A GROWING SECURITY THREAT TO NIGERIA AND AFRICA

IMAGE SOURCE: TRIBUNE ONLINE

Security expert and APC chieftain Ambassador Abayomi Nurain Mumuni warned that the rapid spread of drone technology across Africa is becoming a serious security concern for Nigeria and its neighbours, as unmanned aerial vehicles (UAVs) are increasingly used by non-state groups and hostile actors for surveillance, intelligence gathering, and even targeted attacks in conflict zones. He said this shift marks a major change in modern warfare and exposes weaknesses in traditional defence systems, urging Nigerian authorities to improve intelligence and surveillance capabilities, invest in drone detection and counter-UAV measures, and develop coordinated regional strategies to respond quickly to aerial threats. Mumuni also called for clear legal frameworks and increased cooperation with other countries, as well as investment in local drone technology to strengthen national preparedness and reduce dependence on foreign systems – Tribune online

AFRICAN LEADERS URGED TO BEWARE SURVEILLANCE RISKS IN CHINESE-FUNDED GOVERNMENT BUILDINGS

IMAGE SOURCE: THE NICHE

A geopolitical commentator has urged African leaders to be cautious about the potential surveillance vulnerabilities tied to government buildings funded and constructed by Chinese firms, warning that what are presented as "gifts" of infrastructure—such as foreign ministries, national parliaments and the revamped State House in Kenya—could act as conduits for intelligence collection by China. The concern draws on past allegations that the Chinese-built African Union headquarters in Addis Ababa secretly transmitted data to servers in China, a charge Beijing denied at the time, and suggests that similar risks could exist in the more than 200 Chinese-supported government facilities across the continent. While such projects can ease financial burdens and boost governance capabilities, critics argue the asymmetrical nature of China–Africa relations combined with the sophistication of Chinese surveillance technology could compromise sensitive communications and give Beijing strategic access to information from African governments - The Niche

WHAT EUROPE BANNED, BRAZIL IS USING: FACIAL RECOGNITION TRACKS SCHOOLKIDS

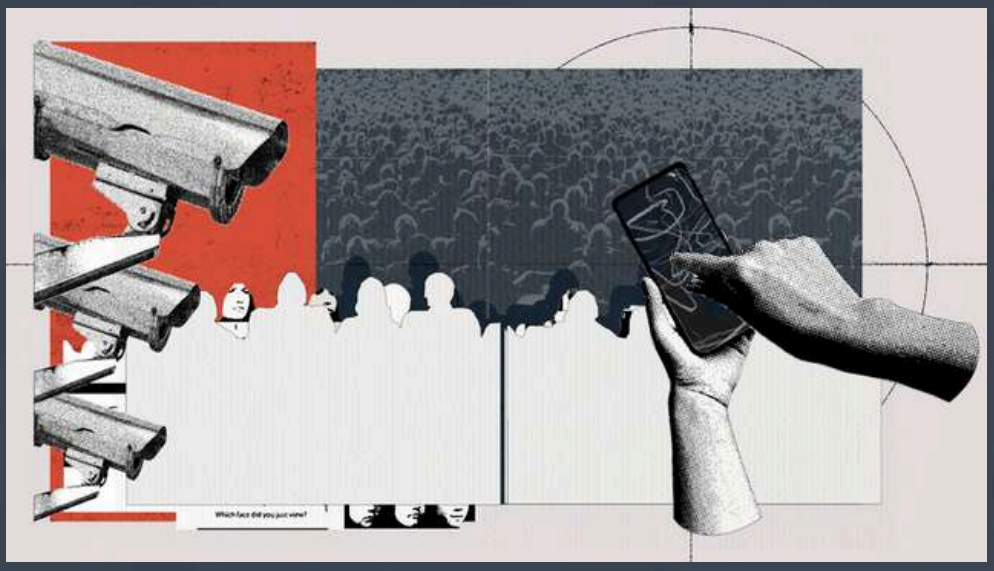


IMAGE SOURCE: TECH POLICY

The article reveals that while many European countries have moved to restrict or ban facial recognition technology over privacy and rights concerns, Brazilian schools are increasingly deploying similar systems to monitor students' movements and behaviour. Proponents in Brazil argue the tech improves safety and attendance tracking, but critics warn it exposes children to mass surveillance without robust legal safeguards, potentially normalising constant digital monitoring from an early age. The piece highlights broader global tensions over facial recognition's use—balancing security and administrative convenience against the risk of privacy violations, biased algorithms, and the long-term impact of subjecting minors to automated surveillance – Tech Policy

INTEL WATCH

Watching the watchers. Guarding the guardians.

YOUR TIRES ARE TALKING: HOW HACKERS CAN TRACK YOU WITHOUT GPS

IMAGE SOURCE: PPSA

The article explains that a common car safety feature—Tire Pressure Monitoring Systems (TPMS)—can be exploited by hackers to secretly track vehicles, because the sensors continuously broadcast unencrypted wireless signals containing unique IDs tied to each car. By placing cheap radio receivers near roads or parking areas, attackers can capture these signals and follow a vehicle's movements over time, building detailed profiles of drivers' routines such as commute patterns, work hours, and travel habits. Researchers warn this method is cheaper, harder to detect, and more discreet than camera-based tracking, since it doesn't require visual contact, and the lack of encryption or regulation means the vulnerability has persisted for years—turning a safety tool into a potential mass-surveillance risk - PPSA

MASS IPHONE SPYWARE EXPOSED: HACKERS' TOOL COULD INFILTRATE HUNDREDS OF MILLIONS OF DEVICES

IMAGE SOURCE: REUTERS

Researchers from cybersecurity firms including Google, iVerify and Lookout have uncovered a powerful new spyware exploit dubbed "Darksword" that was planted on dozens of Ukrainian websites and is capable of silently penetrating and stealing data from potentially hundreds of millions of Apple iPhones, especially those running older versions of iOS, simply when users visit a compromised site. This discovery marks a worrying trend in which extremely advanced mobile malware—similar in sophistication to other recently found tools like Coruna—is active in the wild, with attackers able to harvest sensitive information such as messages, passwords and cryptocurrency wallet details, underscoring how the market for large-scale iPhone-targeting spyware is growing - Reuters

HIDDEN IN PLAIN SIGHT: HOW HACKERS TURNED GOOGLE SHEETS INTO A GLOBAL SPY TOOL

IMAGE SOURCE: TIMES OF INDIA

Google has dismantled a sophisticated China-linked hacking group known as UNC2814 (or "Gallium") that conducted cyber-espionage for nearly a decade, targeting governments and telecom organisations across 42 countries. The group used a clever tactic of hiding malicious activity within everyday tools like Google Sheets, allowing them to send commands and extract stolen data while blending into normal internet traffic and avoiding detection. Their custom malware, called GRIDTIDE, enabled long-term access to compromised systems and helped steal sensitive information such as personal identities, communication records, and operational data. Google, working with partners, disrupted the operation by shutting down the hackers' infrastructure and accounts, marking a significant move against large-scale, state-linked cyber surveillance campaigns – Times of India

SPY TOOLS GONE ROGUE: LEAKED IPHONE HACKS NOW FUEL GLOBAL CYBERCRIME WAVE

IMAGE SOURCE: TECH SPOT

The article reports that highly sophisticated, government-grade iPhone hacking tools—originally developed for intelligence agencies—have leaked into the hands of cybercriminals and are now being used for widespread attacks. Tools like Coruna and DarkSword exploit dozens of iOS vulnerabilities, allowing hackers to silently infect devices through malicious or compromised websites and steal sensitive data such as messages, passwords, and even cryptocurrency. Researchers from Google and security firms found these tools can bypass many of Apple's built-in protections, especially on outdated devices, turning what were once targeted espionage capabilities into mass exploitation tools. The leak highlights a growing and dangerous trend where advanced cyberweapons escape controlled environments and become accessible to criminals, significantly increasing the risk to everyday users worldwide - Techspot

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

PRE-EMPTIVE CONTROL: HOW AI IS BEING USED TO CRUSH PROTESTS BEFORE THEY EVEN BEGIN

IMAGE SOURCE: DW

The article explains how some Middle Eastern governments are increasingly adopting advanced artificial intelligence tools—particularly "predictive policing" and conflict forecasting systems—to identify and suppress potential dissent before it materializes. By analysing massive datasets such as social behaviour, location data, and historical unrest patterns, these systems can flag individuals or regions as risks, enabling authorities to intervene early. Countries like the UAE and Saudi Arabia are investing heavily in surveillance infrastructure, often using technology sourced from China, to monitor populations through facial recognition and behavioural analysis. While officials frame these tools as enhancing security and urban management, human rights experts warn they could create a chilling effect, discouraging activism and enabling authoritarian regimes to silence opposition preemptively without transparency or accountability - DW

BIG BROTHER ON THE ROAD? UK STUDY QUIETLY TRACKED EV DRIVERS THROUGH THEIR PHONES

IMAGE SOURCE: ELECTRIFYING

The article reveals that the UK's Department for Transport (DfT) conducted a controversial multi-year study using anonymised mobile phone data from millions of users to analyse electric vehicle (EV) usage and travel patterns. Working with telecom providers like O2, the project tracked movement trends, app usage, and visits to EV-related websites to better understand how and where EVs are used, aiming to inform future transport policy. Although officials insist the data was aggregated and complied with privacy laws—meaning individuals could not be identified—the initiative has drawn criticism for resembling mass surveillance, with opponents arguing it raises serious concerns about government overreach and the ethics of monitoring citizens' behaviour without explicit awareness - Electrifying

INTEL WATCH

Watching the watchers. Guarding the guardians.

TRUMP PUSHES TO EXPAND THE SURVEILLANCE POWERS HE ONCE SLAMMED

IMAGE SOURCE: THE AMERICAN CONSERVATIVE

The article argues that Donald Trump is now backing an expansion of domestic surveillance powers under Section 702 of the Foreign Intelligence Surveillance Act (FISA)—despite previously criticizing such authorities as threats to Americans' privacy. It explains that recent legislative efforts supported by Trump and his allies would allow intelligence agencies to continue collecting and searching Americans' communications without requiring a warrant, even after a federal court ruled that such searches should need one. Critics say this reflects a broader pattern of growing executive power, warning that loosening safeguards could erode Fourth Amendment protections and enable ongoing mass surveillance, while Congress has largely failed to impose meaningful limits on intelligence agencies – The American Conservative

FAKE LIFELINE, REAL THREAT: SPYWARE MASQUERADES AS ISRAEL'S EMERGENCY ALERT APP

IMAGE SOURCE: INFOSECURITY MAGAZINE

The article describes a sophisticated mobile espionage campaign dubbed "RedAlert," where attackers exploited fear during the Israel-Iran conflict by distributing a fake version of Israel's trusted Red Alert rocket warning app via SMS phishing. The malicious app closely mimics the real one—sometimes even functioning normally—while secretly harvesting sensitive data such as messages, contacts, location, and device information, which is then sent to attacker-controlled servers. By impersonating official emergency alerts and leveraging public trust in crisis communication systems, the campaign increases the likelihood of users installing the spyware, highlighting how cybercriminals are weaponizing real-world conflicts and urgency to conduct surveillance and data theft on civilians – Infosecurity Magazine

RUSSIA'S 'MAX' SUPER-APP: A CONVENIENT MESSAGING TOOL OR A STATE SURVEILLANCE TRAP?

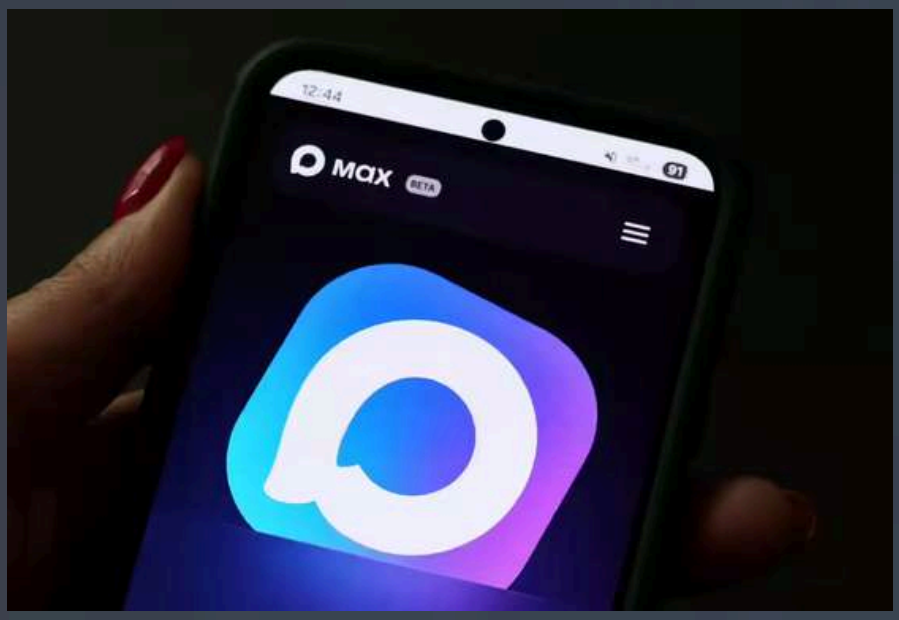


IMAGE SOURCE: ECONOMIC TIMES

The Russian government is aggressively promoting Max—a state-backed, multifunctional messaging "super-app" developed by VK that combines chat, social media, payments and access to government services—as a secure alternative to foreign platforms like WhatsApp and Telegram, even pre-installing it on new devices and restricting rivals within the country. However, critics and digital rights experts warn that its lack of end-to-end encryption and tight integration with domestic services could hand extensive access to personal communications and metadata to the state's security agencies, making it a powerful tool for surveillance under Moscow's "sovereign internet" agenda. While officials insist it enhances digital sovereignty and convenience, many users and observers fear the app will be used to monitor citizens' activity and limit privacy – Economic Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTELLIGENCE AGENCIES

SMART CITIES OR WATCH CITIES? NEW REPORT WARNS AFRICA'S SURVEILLANCE BOOM RISKS DIGITAL AUTHORITARIANISM

IMAGE SOURCE: BIOMETRIC UPODATE

A new report reveals that smart city projects in 11 African countries—often funded through Chinese loans and built with AI-enabled cameras, facial recognition, automated licence-plate readers and centralised monitoring systems—are being rolled out with minimal oversight, weak legal safeguards, and little public transparency, creating significant risks of digital authoritarianism and mass surveillance. Researchers warn that these technologies are frequently adopted under the banner of modernising infrastructure or fighting crime, yet there is no clear evidence they reduce serious offences, and governments lack adequate privacy, data protection and accountability frameworks to protect citizens' fundamental rights. The proliferation of such systems, combined with powerful analytics and cross-linked databases, could enable intrusive monitoring of citizens' movements and behaviours, heightening concerns about misuse against political opponents, journalists and vulnerable groups – Biometric Update

FLORIDA'S 'SPY BILL' SPARKS ALARM: CRITICS WARN OF A DANGEROUS SLIDE TOWARD MASS SURVEILLANCE

IMAGE SOURCE: ST AUGUSTINE RECORD

The article discusses growing backlash against a proposed Florida bill that would create a state-level counterintelligence and counterterrorism unit with broad surveillance powers, which critics fear could target ordinary citizens based on their beliefs or political views. Civil liberties advocates argue the legislation uses vague definitions of "threats," potentially allowing authorities to monitor, investigate, or even act against individuals and groups for their opinions rather than criminal activity. Opponents warn this could undermine First Amendment rights, enable government overreach, and pave the way for ideological policing, while supporters claim it is necessary for state security - highlighting an ongoing tension between public safety and personal freedoms – ST Augustine Record

INTEL WATCH

Watching the watchers. Guarding the guardians.

FLORIDA'S 'STATE CIA' PLAN: A DANGEROUS BLUEPRINT FOR MASS SURVEILLANCE?

IMAGE SOURCE: THE GUARDIAN

The article warns that a proposed Florida bill (HB 945) to create a state-level intelligence unit similar to the CIA could open the door to widespread domestic surveillance with limited oversight. Critics argue the legislation's vague language—allowing authorities to monitor individuals based on their "views" or "opinions"—echoes past abuses like the FBI's COINTELPRO program and risks enabling ideological policing. Experts say creating separate state intelligence agencies could fragment national security efforts while giving governments powerful tools to track political opponents, activists, and journalists, potentially chilling free speech. The piece concludes that once such surveillance powers are established, they are rarely rolled back, raising long-term concerns for civil liberties and democratic rights – The Guardian

FBI ADMITS IT'S BUYING AMERICANS' LOCATION DATA TO TRACK THEM

IMAGE SOURCE: HOTHARDWARE

The FBI's director, Kash Patel, confirmed during a U.S. Senate hearing that the bureau has resumed purchasing commercially available data on Americans' location and movement history from private data brokers, a practice that allows agents to track people's movements without obtaining a traditional warrant from a judge. Patel said the agency buys this information in ways he believes are consistent with U.S. law and the Constitution, but privacy advocates and some lawmakers are deeply concerned it could undermine Fourth Amendment protections and create a loophole for government surveillance. This marks a notable shift from earlier statements by former leadership that such purchases were not currently happening and has reignited debate over how privacy laws govern the collection and use of personal data - hothardware

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

LETTER TO THE EDITOR:
INFO@INTELWATCH.ORG.ZA

INTELWATCH

Watching the watchers. Guarding the guardians.

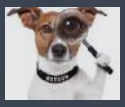
GET INVOLED!

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!