Issue #13

INTEL WATCH

June 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

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #13 OF THE WATCHER

How does an online campaign become a real-world threat? In Issue #13 of The Watcher, we look into the resurgence of South Africa's xenophobic online movement, tracing how social media campaigns, anonymous networks, and digital mobilisation have helped transform anti-immigrant narratives into a powerful and potentially dangerous force. We also explore a troubling question: are social media platforms profiting from outrage, misinformation, and anti-foreigner hate through engagement-driven algorithms and creator economies?

This issue also takes readers into the heart of South Africa's escalating cybersecurity crisis, examining major data breaches, attacks on public and private institutions, and warnings that AI-powered cyberattacks could soon overwhelm organisations that fail to prepare. From vulnerabilities within government systems and healthcare infrastructure to customer data exposures and ransomware incidents, the digital threat landscape is becoming increasingly difficult to ignore.

Beyond cybersecurity, The Watcher uncovers the rapid expansion of surveillance technologies across Africa and the world. Readers will explore facial recognition at borders, AI-powered monitoring in schools, smart glasses capable of discreet recording, and growing concerns over the use of spyware, biometric systems, and advanced surveillance tools by governments and private actors alike.

The issue further examines how artificial intelligence is reshaping both security and repression. From AI-enabled cybercrime and deepfake-driven threats to the growing use of surveillance technologies against activists, journalists, and civil society groups, we reveal how emerging technologies are increasingly being deployed to monitor, influence, and control.

Packed with investigations, regional developments, and global case studies, Issue #13 shines a light on the systems operating behind the screens - challenging readers to think critically about privacy, accountability, and the future of democratic freedoms in a world where technology is watching more than ever before.

As always, The Watcher is here to ensure that those who watch us remain firmly in the light.

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

WARNING FOR PEOPLE WITH DRIVER'S LICENCES VISITING ESTATES IN SOUTH AFRICA

IMAGE SOURCE: TOPAUTO

The article warns that estates, complexes, and gated communities in South Africa may soon face tighter rules on how they collect and store visitor information, especially when scanning driver's licences, IDs, or using facial recognition at access points. It says the Information Regulator is finalising a POPIA code of conduct for gated access, and that many common practices — like open visitor books, copying personal details, or keeping data too long — could become non-compliant. The main concern is that these sites may be collecting more information than necessary and not safeguarding it properly, which raises privacy and data-breach risks (30 June 2026). TopAuto

GAUTENG EXPANDS SURVEILLANCE NETWORK AS IMMIGRATION ENFORCEMENT BECOMES TECH-DRIVEN OPERATION

IMAGE SOURCE: NEWSNOTE

South Africa is expanding its use of drones, CCTV cameras, and other surveillance tools in Gauteng as part of a broader, tech-driven migration and enforcement strategy. The reporting links this to rising pressure over illegal immigration and public protests, with authorities saying they want real-time monitoring, faster detection, and tighter coordination across law enforcement agencies. The broader trend is that immigration control is becoming more intelligence-led and digitally monitored, rather than relying only on conventional patrols and checkpoints (30 June 2026) . Newsnote

INTEL WATCH

Watching the watchers. Guarding the guardians.

HOW SOUTH AFRICA'S XENOPHOBIC ONLINE MACHINE WAS REBOOTED IN 2026

IMAGE SOURCE: DAILY MAVERCIK

South Africa's 2026 xenophobic online surge didn't start with politics or violence but with Mazwi Kubheka's disappearance, whose #BringMazwiBack/#JusticeForMazwi campaigns on X evolved into digitally coordinated anti-immigrant mobilisation linking undocumented migrants to crime, corruption, and state failure—revealing a 6-year-entrenched ecosystem built since 2020's #PutSouthAfricansFirst and Operation Dudula, now self-sustaining via anonymous channels, political backing, and fringe vigilante groups pushing an unfounded June 30 "deadline" for undocumented migrants to leave, triggering threats, machete-brandishing posts, and thousands fleeing borders amid violent attacks with scant police response, proving warnings ignored as this intentionally modern xenophobic machine leverages emotionally charged incidents into broader anti-foreigner narratives blaming migrants for unemployment and societal woes (1 June 2026). Daily Maverick

DO DIGITAL PLATFORMS PROFIT FROM ANTI-FOREIGNER HATE?

IMAGE SOURCE: DAILY MAVERICK

As anti-immigrant rhetoric intensifies in South Africa ahead of calls for undocumented foreigners to leave the country, concerns are growing that social media platforms may be financially benefiting from content that spreads fear, misinformation, and hostility toward migrants. The argument is that modern platforms are not neutral hosts of content but creator economies that reward engagement, meaning posts that provoke outrage and anger can generate visibility, influence, and even revenue for content creators. Critics say this creates incentives for accounts to amplify anti-foreigner narratives, conspiracy theories, and inflammatory content, while platforms often provide little transparency about how such content is moderated, demonetised, or promoted. The debate raises broader questions about the responsibility of digital platforms in preventing online hate from translating into real-world harm and violence (18 June 2026). Daily Maverick

INTEL WATCH

Watching the watchers. Guarding the guardians.

POLITICAL HACKS IN SA DISTRACT FROM BIGGER CYBERSECURITY CRISIS

IMAGE SOURCE: MY BROADBAND

Palo Alto Networks warns that politically charged hacks in South Africa (like the 2025 Nullsec Nigeria claim to breach the Department of Correctional Services amid anti-foreigner violence) distract from the graver, systemic reality: SA is Africa's top cyber target (40% of Africa's ransomware, 35% of infostealer attacks), facing 577 hourly incidents, R5.8B annual losses, and 47% of organizations reporting 1-5 breaches/year, with 88% suffering multiple breaches, driven by AI-powered attacks, identity compromises (54% of breaches), and peripheral/IoT blindspots (38% of breaches) due to inadequate defensive capabilities, outdated infrastructure, and insufficient monitoring—only 41% assess threats daily—making the real crisis not hacktivism but crippling vulnerability that leaves finance, healthcare, and government sectors exposed to sophisticated criminal networks (1 June 2026). My Broadband

---

CYBERATTACKS A GROWING THREAT TO SOUTH AFRICA'S HEALTHCARE SYSTEM

IMAGE SOURCE: SUNDAY TIMES

South Africa’s healthcare system is facing an escalating wave of cyberattacks as hospitals and medical facilities become increasingly digitised and dependent on connected systems. Health institutions are being targeted by ransomware and other forms of cyber intrusion that can disrupt services, compromise sensitive patient data, and force facilities to revert to manual, paper-based operations during outages. Research highlighted in the report shows that healthcare organisations across Africa are experiencing thousands of attacks weekly, with South Africa among the most affected due to outdated systems, limited cybersecurity funding, and shortages of skilled professionals. Experts warn that these vulnerabilities can directly impact patient safety by delaying treatment, disrupting laboratory services, and undermining trust in digital health platforms. The situation has prompted calls for stronger cybersecurity governance, better investment in infrastructure, and treating cyber resilience as a core component of patient care rather than just an IT issue (8 June 2026). Sunday Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

TOP MEDICAL AID IN SOUTH AFRICA HIT BY DATA BREACH.

IMAGE SOURCE: MY BROADBAND

Profmed has notified customers that a data breach exposed some personal information after an unauthorised person appears to have accessed third-party service provider systems using compromised login credentials. PPS Healthcare Administrators, which runs Profmed and manages services for six medical schemes, said the exposed data may include member names, identity numbers, contact details, membership numbers, and scheme option information, while stressing that its own internal systems were not affected. The administrator said it had isolated affected systems, reset credentials, brought in cybersecurity specialists and legal advisers, and was in the process of notifying the Information Regulator under POPIA. It also warned that the stolen information could be used for phishing, impersonation, banking fraud, and other social-engineering attacks, and urged members to stay alert for suspicious calls, emails, and messages (25 June 2026). MyBroadband

---

OLD APP, NEW THREAT: PICK N PAY DATA BREACH EXPOSES LEGACY SYSTEM RISK

IMAGE SOURCE: TECH CABAL

Pick n Pay has confirmed a cyberattack that exposed customer data from an older version of its delivery platform, formerly known as Bottles and later rebranded as Asap!, affecting users who registered on or before 2022. The compromised information includes names, contact details, delivery addresses, and limited payment card data, although the retailer says full card numbers and CVV codes were not stored and therefore cannot be used for direct card fraud. The incident has raised concerns about the security risks posed by legacy systems and poor data-retention practices, with cybersecurity experts arguing that outdated platforms and unnecessary storage of customer records often create vulnerabilities long after services are retired. Pick n Pay has notified affected customers, reported the breach to South Africa's Information Regulator, and launched an investigation while reviewing its historical data management processes (1 June 2026). Tech Cabal

INTEL WATCH

Watching the watchers. Guarding the guardians.

SOUTH AFRICA HAS FIVE MONTHS TO BRACE FOR AI-POWERED CYBERATTACKS, EXPERTS WARN

IMAGE SOURCE: IT WEB

Cybersecurity experts are warning that South African organisations have a narrow three-to-five-month window to strengthen their defences before a new wave of AI-driven cyberattacks becomes more widespread. According to security leaders from Palo Alto Networks, advanced AI models are dramatically accelerating the discovery and exploitation of software vulnerabilities, enabling attackers to launch more sophisticated attacks faster, cheaper, and at greater scale than ever before. The warning comes amid a surge in local cyber incidents affecting major organisations, including retailers, banks, government entities, and political organisations. Experts say AI is transforming cybercrime from a largely human-driven activity into one that can increasingly operate autonomously, forcing businesses to rethink traditional security approaches and invest in proactive threat detection, resilience, and AI-enabled defense strategies (2 June 2026). My Broadband

COPYING THE WRONG PERSON ON AN EMAIL COULD BE CONSIDERED A DATA BREACH IN SOUTH AFRICA

IMAGE SOURCE: MY BROADBAND

The article explains that under South Africa's Protection of Personal Information Act (POPIA), accidentally emailing personal information to the wrong recipient can be considered a reportable data breach. This follows an enforcement notice against Central Johannesburg TVET College, where confidential employee information was mistakenly shared with unauthorised staff. The Information Regulator ruled that recalling the email and investigating the incident did not remove the legal obligation to notify both the regulator and affected individuals. The case highlights that organisations must have strong data protection measures and clear breach response procedures, as even accidental disclosures may require formal reporting under POPIA (29 June 2026). MyBroadband

INTEL WATCH

Watching the watchers. Guarding the guardians.

WARNING ABOUT NEW TECH THAT CAN SECRETLY RECORD YOU IN SOUTH AFRICA

IMAGE SOURCE: MY BROAD BAND

Cybersecurity experts are warning South Africans about the growing privacy and security risks posed by smart glasses, such as Meta's Ray-Ban smart glasses, which can discreetly record photos and videos from a wearer's perspective. According to cybersecurity researcher Allan Juma, these internet-connected devices could be vulnerable to hacking, especially if users fail to update their software or connect through unsecured public Wi-Fi networks. Beyond cybersecurity concerns, the technology raises significant privacy questions, as people can be recorded in public without their knowledge, despite small indicator lights designed to show when recording is taking place. Experts say current legislation, including South Africa's POPIA framework, has not fully caught up with wearable surveillance technologies, creating uncertainty around consent and data protection. The warning comes amid growing international concerns about smart glasses being used for covert recording and the potential future integration of AI-powered features such as facial recognition, which could further intensify privacy risks (28 May 2026). My Broadband

SABS EXECUTIVES IN TROUBLE AFTER A CRIPPLING CYBERATTACK

IMAGE SOURCE: MY BROADBAND

Two senior executives at the South African Bureau of Standards (SABS) are facing disciplinary proceedings after a crippling ransomware attack exposed serious failures in cybersecurity governance. A forensic investigation found that the executives did not implement critical security recommendations issued in 2022 by the Auditor-General and the State Security Agency, leaving SABS systems vulnerable to attack in November 2024. The breach caused widespread operational disruption, including encrypted systems, manual salary payments, and a prolonged shutdown of core services while the organisation attempted recovery and system rebuilding. Authorities have since moved to hold individuals accountable, with charges formally issued and hearings scheduled, as part of broader efforts to address governance breakdowns and prevent similar incidents in the future (2 June 2026). My Broadband

INTEL WATCH

Watching the watchers. Guarding the guardians.

INSIDE SITA: INVESTIGATION FINDS WIDESPREAD SECURITY WEAKNESSES DESPITE GOVERNMENT ASSURANCES

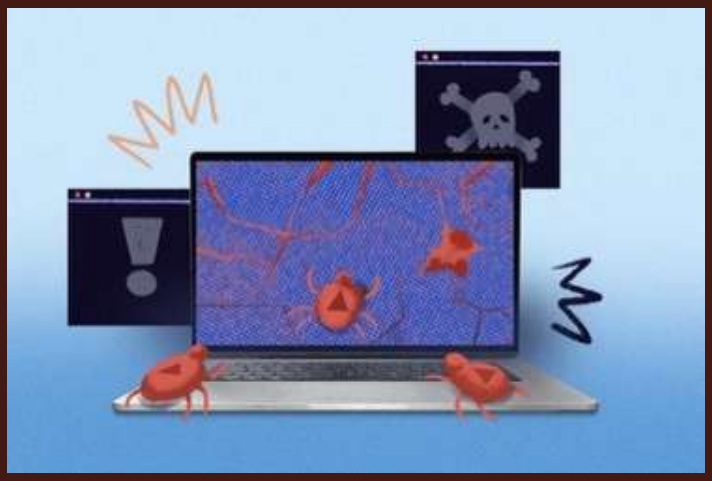


IMAGE SOURCE: GROUND UP

The State Information Technology Agency (SITA) claims its systems are secure, but an independent investigation into its publicly accessible infrastructure found extensive cybersecurity weaknesses across government digital services it manages. Using internet-scanning tools, researchers identified thousands of exposed services linked to SITA-controlled networks, including more than 900 known software vulnerabilities, many of them classified as critical. These weaknesses were found across multiple government departments and systems, with some outdated software and security flaws reportedly dating back many years. The findings suggest that large parts of South Africa's government IT environment may be exposed to potential cyber threats due to legacy systems, poor maintenance, and inconsistent patching practices. While SITA has rejected claims of a cyberattack and insists its monitoring systems are active, the analysis raises concerns about the difference between declared security and real-world exposure in public-sector digital infrastructure (3 June 2026). Ground Up

CYBER-ATTACK HITS AVBOB AS SYSTEMS GO OFFLINE

IMAGE SOURCE: IOL

South African funeral insurance provider AVBOB has confirmed that a cyberattack caused significant disruption to its digital systems and forced parts of its operations offline. The incident affected access to certain online services, prompting the company to activate its incident response processes while working with specialist cybersecurity partners to restore functionality. AVBOB stated that it is prioritising recovery and system stabilisation, while also investigating whether any customer or policyholder data may have been exposed during the breach. The organisation has assured clients that services are being restored and urged caution around payment links to avoid potential fraud attempts during the outage. The attack adds to a growing list of cyber incidents targeting South African financial and insurance institutions, highlighting increasing risks to critical customer-facing digital infrastructure (June 2026). IoL

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI DRIVEN CYBER THREATS FORCE SOUTH AFRICAN BUSINESSES TO RETHINK SECURITY STRATEGIES

IMAGE SOURCE: IOL

Cybersecurity experts warn South African businesses face a critical 3–5 month window to strengthen defenses before AI-driven exploits become widespread, as frontier AI systems now identify software vulnerabilities at levels comparable to top human security experts, fundamentally changing the threat landscape by accelerating attack speed from days to minutes and scaling attacks exponentially. Global leaders report attacks escalate from initial compromise to critical impact in just 72 minutes (down from nine days), driven by attackers and cyber cartels using generative AI, agentic AI, and automation to rapidly build ransomware, develop exploit code, and automate campaigns, with identity compromise (valid credentials) as the primary breach entry point—most attackers "log in" rather than "hack in". South Africa, Africa's top cyber target facing 62% ransomware surge in 2023, must prioritize proactively identifying/fixing vulnerabilities via AI-powered scanning, reducing exposure by managing attack surfaces including AI systems/machine identities, and ensuring security systems can defend against sophisticated threats including deepfake fraud, AI-generated malware, and prompt injection attacks (June 2026). IoL

SOUTH AFRICAN FANS WARNED ABOUT CYBER THREATS AND SURVEILLANCE RISKS AT THE 2026 WORLD CUP

IMAGE SOURCE: IOL

South African football fans planning to attend or follow the 2026 FIFA World Cup are being warned about increased cyber risks linked to the tournament's heavy digital infrastructure and global attention. Threats include phishing scams targeting ticket sales, fake travel booking sites, fraudulent streaming services, and identity theft attempts aimed at fans using mobile apps and online payment systems. With matches hosted across North America, organisers are also deploying advanced surveillance technologies such as facial recognition, AI-powered CCTV, and biometric entry systems, meaning fans may be tracked or processed through multiple digital checkpoints. Experts caution that South Africans are particularly vulnerable due to high levels of online fraud exposure and the excitement around major sporting events, which scammers often exploit. The guidance emphasises careful verification of ticketing platforms, secure payment methods, and awareness of how personal data may be collected and used across stadium and travel systems during the tournament (June 2026). IoL

INTEL WATCH

Watching the watchers. Guarding the guardians.

CYBERSECURITY SKILLS SHORTAGE LEAVES SOUTH AFRICA'S CRITICAL SYSTEMS EXPOSED

IMAGE SOURCE: THE CITIZEN

South Africa's growing exposure to cyber threats is being worsened by a severe shortage of cybersecurity professionals, with more than half of organisations struggling to recruit skilled talent. As cyberattacks increase in frequency and sophistication—targeting banks, government departments, telecoms, and major private-sector institutions—many organisations lack the internal capacity to defend their systems effectively. The gap is partly driven by a mismatch between demand and available expertise, with employers often seeking experienced specialists while overlooking or underutilising entry-level candidates who need practical training and mentorship. Experts say this shortage is not just a hiring issue but a broader structural challenge linked to education pipelines, limited hands-on training opportunities, and rapid technological change that outpaces skills development. The result is a persistent vulnerability in both public and private sector systems, where critical services and sensitive data remain at heightened risk of cyberattacks (11 June 2026). The Citizen

GLOBAL CYBERSECURITY LEADER OFFICIALLY SETS UP SOUTH AFRICAN PRESENCE

IMAGE SOURCE: HYPERTEXT

Global cybersecurity leader Sophos has officially established Sophos South Africa (Pty) Ltd—a local legal entity at Mushroom Farm Retail Centre, Midrand—to strengthen operations in South Africa and support sub-Saharan Africa growth, enabling local invoicing, partner enablement, compliance, and expanded regional investment amid rising demand for cybersecurity services (1 June 2026). Hypertext

INTEL WATCH

Watching the watchers. Guarding the guardians.

NIGERIA LEADS AFRICA IN SPAM CALLS

IMAGE SOURCE: THE GUARDIAN

Nigeria has been ranked the most spammed country in Africa, with data showing that 51% of all unknown calls received by users in 2025 were identified as spam or fraud—meaning more than one in every two unfamiliar calls is potentially malicious. The country also ranks eighth globally and leads the continent ahead of South Africa, Kenya, Ghana, and Ethiopia. The findings, based on Truecaller's global insights, highlight that Nigeria's spam landscape is unusually shaped by telecom and operator-linked outreach, which accounts for about 35% of unwanted calls, alongside sales, telemarketing, and scam attempts. This mix makes it harder for users to distinguish between legitimate service messages and fraudulent calls, contributing to growing mistrust in mobile communication. Experts warn that the broader impact goes beyond financial loss, as people increasingly ignore unknown calls, which can also disrupt access to essential services like healthcare, banking, and deliveries (6 May 2026). The Guardian

NIGERIA DENIES CYBERATTACK ON NATIONAL EDUCATION DATABASE

IMAGE SOURCE: ALL AFRICA

Nigeria's Federal Government has denied claims that its national education database was compromised in a cyberattack, responding to reports suggesting that sensitive student and institutional data may have been exposed. Officials insist that the system remains secure and operational, and that no evidence has been found to support allegations of a breach affecting the platform used to manage education records across the country. The government emphasised that routine security monitoring is ongoing and that safeguards are in place to protect data integrity and prevent unauthorised access. The denial comes amid heightened sensitivity around cybersecurity in Nigeria's public sector, where digital transformation efforts in education and other services have expanded rapidly. Authorities say misinformation about system breaches can create unnecessary public concern and undermine trust in national digital infrastructure, while reaffirming their commitment to strengthening cybersecurity resilience across government platforms (16 June 2026). All Africa

AFRICA FACES NEARLY 3,000 CYBERATTACKS PER ORGANISATION EACH WEEK AS THREAT LEVELS SURGE

IMAGE SOURCE: AFRICA BUSINESS COMMUNITIES

African organisations are experiencing an average of nearly 3,000 cyberattacks per week per organisation, according to cybersecurity threat intelligence data, placing the continent among the most heavily targeted regions globally. The surge is driven by increasingly sophisticated tactics such as AI-powered phishing, identity-based intrusions, ransomware campaigns, and exploitation of misconfigured cloud systems. Countries like Nigeria, Angola, and South Africa are among the most targeted, with some sectors—particularly financial services, government, telecoms, and education—facing the highest levels of sustained attack activity. Experts warn that the scale and frequency of these attacks reflect a broader shift toward automated, industrialised cybercrime, where attackers can launch large volumes of coordinated operations at low cost and high speed. The findings highlight urgent needs for stronger cybersecurity investment, skills development, and coordinated defence strategies across the continent (15 June 2026). Africa Business Communities

AI BOOM FUELS NEW CYBER THREATS ACROSS EAST AFRICA, KASPERSKY WARNS

IMAGE SOURCE: IAFRICA

Speaking at the AI Everything Kenya x GITEX Kenya event in Nairobi, cybersecurity company Kaspersky warned that the rapid adoption of artificial intelligence is creating new security risks for businesses and individuals across Kenya and East Africa. The company highlighted growing threats such as AI-powered phishing, deepfake fraud, social engineering attacks, ransomware, and the rise of "Shadow AI"- employees using unauthorized AI tools that may expose sensitive company data. Kaspersky reported sharp increases in password-stealing malware and spyware attacks in Kenya during 2025 and noted that many workers are using AI tools without adequate cybersecurity training. The company urged organizations to establish clear AI governance policies, strengthen security controls, educate employees, and regularly assess AI-related risks to ensure innovation is balanced with cyber resilience (1 June 2026). iAfrica

INTEL WATCH

Watching the watchers. Guarding the guardians.

ISRAEL SHUTS INVESTIGATION INTO SALE OF PEGASUS SPYWARE TO GHANA, REIGNITING SPYWARE ACCOUNTABILITY CONCERNS

IMAGE SOURCE: GHANA BUSINESS NEWS

Israeli authorities have closed a long-running investigation into the sale of NSO Group's Pegasus spyware to Ghana, a case tied to allegations of corruption and improper export approvals. The deal, which involved the purchase of surveillance equipment through a local intermediary, had previously led to convictions in Ghana, where several public officials were jailed for procurement violations and financial misconduct linked to the transaction. Pegasus, a powerful spyware tool capable of taking over smartphones and accessing calls, messages, and microphones, has been widely criticized globally for enabling surveillance of journalists, activists, and political opponents. Although Israel had earlier signaled intent to investigate whether export controls and anti-corruption rules were breached, the probe was repeatedly delayed across multiple agencies and ultimately shelved, raising concerns from activists about accountability and the oversight of commercial spyware exports (29 May 2026). Ghana Business News

UNIVERSITY OF NOTTINGHAM CYBERATTACK SPARKS WARNING FOR GHANA'S EDUCATION SECTOR

IMAGE SOURCE: MODERN GHANA

A major cyberattack on the University of Nottingham has raised global concern after hackers gained access to sensitive systems holding personal data for hundreds of thousands of current and former students. The breach, which exposed large volumes of contact and identity-related information, has been described as a serious warning for universities worldwide as they expand digital systems and cloud-based student records. In Ghana, cybersecurity commentators and analysts have highlighted the incident as a direct warning for local institutions, urging universities to strengthen their cyber defences as they increasingly adopt online learning platforms and digital administration systems. They argue that Ghana's education sector is particularly vulnerable due to limited cybersecurity funding, shortages of skilled professionals, and growing reliance on interconnected digital infrastructure. The case underscores how a single breach in one country can serve as a cautionary example for others, especially in sectors handling large amounts of sensitive personal data (17 June 2026). Modern Ghana

INTEL WATCH

Watching the watchers. Guarding the guardians.

PHONES, SPYWARE AND POWER: ALLEGATIONS OF AN EXPANDING SURVEILLANCE STATE IN KENYA

IMAGE SOURCE: GOTTA NEWS

The article explores allegations that Kenya's government has expanded its digital surveillance and spyware capabilities in the aftermath of the 2024 Gen Z protests, which were driven by anti-tax sentiment and broader frustrations over governance and economic hardship. It describes claims that state security agencies increasingly rely on phone tracking, spyware, and digital intelligence tools to monitor activists, journalists, and protest organisers, contributing to a climate of fear and self-censorship among young political voices. The piece links these developments to a broader pattern of post-protest repression, where digital tools are allegedly used alongside traditional policing methods to identify, intimidate, and detain critics. Human rights advocates argue that this expanding surveillance ecosystem risks undermining constitutional freedoms such as privacy, expression, and peaceful assembly, while government officials typically justify enhanced monitoring as necessary for national security and maintaining public order (26 May 2026). Gotta News

ZIMBABWE INTENSIFIES FIGHT AGAINST RISING CYBERCRIMES

IMAGE SOURCE: CONNECTING AFRICA

Zimbabwe is intensifying efforts to combat a rising wave of cybercrime as the country's rapid digital expansion increases exposure to online threats such as fraud, hacking, malware, and data breaches. According to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) and other officials, cybercrime incidents have grown alongside rising internet penetration and wider use of mobile and financial digital services. Authorities say existing laws, including the Cyber and Data Protection framework and provisions in the criminal code, already cover many cyber offences, but enforcement, coordination, and public awareness still need strengthening. The government is working with law enforcement and security agencies to improve incident response, build cyber resilience, and enhance training for investigators and judges. Officials also emphasize that education and awareness among citizens are critical, as most cybercrimes—especially online fraud and phishing—exploit human behavior as much as technical vulnerabilities (27 May 2026). Connecting Africa

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI-POWERED ZERO-DAY ATTACKS RAISE THE STAKES FOR AFRICA'S CYBERSECURITY FUTURE

IMAGE SOURCE: BUSINESS DAY

A new wave of AI-assisted cyberattacks is reshaping the global threat landscape, with experts warning that artificial intelligence is now being used not only to defend systems but also to identify and exploit previously unknown software vulnerabilities, known as zero-day exploits. The article argues that Africa's rapidly expanding digital economy—spanning fintech, e-government, healthcare, and education—is particularly vulnerable due to uneven cybersecurity maturity, reliance on imported technologies, and limited cyber talent. It highlights the risks to critical sectors such as financial services and public infrastructure, where successful attacks could undermine trust, disrupt services, and threaten national security. To address these challenges, the author calls for stronger cybersecurity frameworks, AI-driven threat detection, investment in local cyber skills, greater regional collaboration, and a push toward digital sovereignty through indigenous technology development and resilience-building initiatives (21 May 2026). Business Day

INFRASTRUCTURE A MUST TO BOOST AFRICA'S AI SOVEREIGNTY

IMAGE SOURCE: ISS

Africa's AI ambitions remain aspirational without massive investments in power, connectivity, and computing infrastructure—the continent faces severe deficits with only 42% of Africans having internet access (vs. 70% global average), 1B lacking electricity, and minimal data center capacity, forcing reliance on expensive foreign cloud services that undermine sovereignty. The AU's 2024 Continental AI Strategy and 2050 Africa's Digital Transformation Strategy aim for AI sovereignty, but lack of infrastructure—data centers, high-speed networks, GPUs—means Africa cannot develop or deploy AI independently, risking continued dependence on China, US, and EU for both technology and data storage. Investments needed include renewable energy (solar, hydro) to power data centers, subsea fiber-optic cables and 5G for connectivity, and local data centers/neural processing units for computing, with models like Kenya and Rwanda's digital transformation showing progress possible but requiring sustained state-private sector collaboration (28 May 2026). ISS

INTEL WATCH

Watching the watchers. Guarding the guardians.

AFRICA FACES $57.8 BILLION CYBERCRIME BILL AS BANK BOARDS BECOME PERSONALLY ACCOUNTABLE

IMAGE SOURCE: AFRICA.COM

Africa lost an estimated $57.8 billion to cybercrime in 2025, driven by a sharp rise in digital banking fraud, AI-enabled scams, and large-scale social engineering attacks targeting individuals and financial institutions across the continent. The scale of losses has intensified pressure on regulators and the financial sector, with governance expectations now shifting toward holding bank boards and senior executives personally liable for cybersecurity failures and weak risk controls. This change reflects growing recognition that cyber resilience is no longer just an IT concern but a core leadership responsibility tied to financial stability and customer trust. Experts warn that as banks expand digital services and interconnected financial ecosystems, weak oversight and inconsistent security practices significantly increase systemic risk, making stronger board-level accountability, investment in cyber defenses, and tighter regulatory enforcement essential to reduce future losses and restore confidence in Africa's financial systems (10 June 2026). Africa.com

FAKE CAPTCHA MALWARE CAMPAIGN USES GULOADER TO STEAL WINDOWS USERS' DATA

IMAGE SOURCE: INFOSHARE SYSTEMS

Windows users are being targeted by a malware campaign that uses fake CAPTCHA verification pages to trick them into unknowingly running malicious commands, which then install the GULoader malware loader. The attack relies on compromised websites that display convincing "verify you are human" prompts, but instead of completing a normal CAPTCHA, victims are guided into executing system-level commands that trigger hidden scripts. Once activated, GULoader acts as a stealthy downloader that can install additional malicious payloads, including information-stealing malware capable of capturing passwords, browser data, and other sensitive information. Security researchers warn that this "ClickFix" style social engineering tactic is especially dangerous because it bypasses traditional download warnings by making users execute the malware themselves, and it is increasingly being used across multiple large-scale cybercrime campaigns (17 June 2026). Info share systems

INTEL WATCH

Watching the watchers. Guarding the guardians.

DATA OF 600,000 GAZA HOUSEHOLDS EXPOSED IN WFP CYBER-ATTACK

IMAGE SOURCE: THE NEW HUMANITARIAN

A cyber-attack targeting the World Food Programme (WFP) has exposed personal data belonging to around 600,000 households in Gaza, marking what may be one of the largest breaches of humanitarian beneficiary information ever recorded. The breach affected WFP's self-registration system used by Palestinians applying for food and cash assistance, with attackers gaining access to sensitive details including names, identification numbers, phone numbers, and location data. WFP confirmed the incident occurred in mid-May and said it took steps to shut down the affected system, contain the intrusion, and strengthen security measures, while an investigation is ongoing and no group has claimed responsibility. The incident has raised serious concerns among digital rights and humanitarian experts, who warn that such data—especially in a conflict zone—could be misused to track or endanger vulnerable individuals, highlighting long-standing weaknesses in cybersecurity practices within the aid sector (2 June 2026). The New Humanitarian

NOVO NORDISK HIT BY $25M EXTORTION ATTEMPT AFTER MASSIVE DATA BREACH CLAIM

IMAGE SOURCE: REUTERS

A cyber extortion group has claimed responsibility for breaching Danish pharmaceutical giant Novo Nordisk and stealing more than 1.3 terabytes of sensitive data over a period of roughly two months. The attackers allege the stolen material includes source code, clinical trial information, proprietary drug research (including data on unreleased treatments), and personal data relating to employees, doctors, and patients. After reportedly demanding a $25 million ransom that was not paid, the group has threatened to leak or sell parts of the data, escalating the incident into a major "hack-and-leak" extortion case. Novo Nordisk has confirmed it experienced a cybersecurity incident involving limited internal systems and says it is working with authorities and cybersecurity experts while maintaining normal operations. The full scope and authenticity of the leaked data remain under investigation (16 June 2026). Reuters

CRITICAL INFRASTRUCTURE ATTACKS BRING NATIONS TO THEIR KNEES

IMAGE SOURCE: ITWEB

Critical infrastructure is increasingly becoming a prime target for cyberattacks, with experts warning that successful breaches could disrupt essential services such as power, water, transport, and communications, potentially destabilising entire economies. The discussion highlights how attackers—including cybercriminal groups, hacktivists, and nation-state actors—are shifting focus from isolated corporate systems to large-scale national infrastructure, where the impact of disruption is far greater. As these systems become more interconnected and digitised, vulnerabilities in one sector can cascade into others, amplifying damage and making recovery more difficult. The piece stresses that traditional cybersecurity approaches are no longer sufficient for these environments, and calls for a shift toward resilience-focused strategies such as zero-trust architectures, stronger public-private collaboration, and treating infrastructure security as a core national security priority rather than a technical afterthought (8 June 2026). ITWeb

---

SOCIAL MEDIA GROUP SCAM TRICKS USERS INTO INSTALLING PHONE SPYWARE

IMAGE SOURCE: INSIDE HALTON

A growing online scam is targeting users through fake social media groups and trusted-looking communities that trick victims into installing spyware on their phones. The scheme typically begins with scammers posing as group admins or members offering exclusive content, services, or "security tools," then directing users to click links or download apps that secretly contain surveillance software. Once installed, the spyware can access sensitive data such as messages, photos, contacts, and even location information, often running silently in the background without obvious signs. Security experts warn that these scams rely heavily on social engineering—manipulating trust rather than exploiting technical flaws—and are increasingly spreading across platforms where users assume group environments are safe. Victims often only discover the compromise when unusual device behaviour appears or financial and personal accounts are misused (16 June 2026). Inside Halton

MAJOR STALKERWARE LEAK EXPOSES PRIVATE MESSAGES AND PHOTOS OF CELEBRITIES AND INFLUENCERS

IMAGE SOURCE: ITWEB

A large stalkerware-related data breach has exposed highly sensitive private communications belonging to a European celebrity, with tens of thousands of screenshots reportedly capturing chats, images, and app activity across platforms such as WhatsApp, Instagram, Facebook, and TikTok. The compromised data appears to have been collected through spyware installed on the victim's device, continuously recording screen activity and syncing it to an unsecured online database that was later discovered publicly accessible. The leaked material included personal conversations with influencers and public figures, as well as financial details, invoices, and intimate exchanges, highlighting how stalkerware not only invades a primary victim's privacy but also exposes everyone they interact with. Cybersecurity researchers warn that these incidents reflect a broader trend where consumer spyware tools marketed as monitoring or parental control apps are being misused for surveillance and coercive control, and are themselves increasingly vulnerable to secondary breaches that amplify the damage (11 June 2026). It Wire

---

WHATSAPP CATCHES FRESH NSO SPYWARE ATTACKS IN 2026

IMAGE SOURCE: MEMEBURN

WhatsApp has uncovered and disrupted fresh spear-phishing campaigns linked to the Israeli spyware firm NSO Group, even though a U.S. court had previously issued a permanent injunction banning NSO from targeting WhatsApp users. The attacks used "1-click" phishing tactics, where victims were tricked into tapping malicious links that redirected them to external sites capable of compromising their devices. Meta says it detected the activity through user reports and internal investigation, then shut down associated accounts and groups created by the attackers. The company is now asking a U.S. court to hold NSO in contempt for violating the injunction and continuing operations aimed at WhatsApp users. The incident reinforces concerns that commercial spyware tools like Pegasus continue to evolve and rely heavily on social engineering rather than breaking encryption directly, making user awareness and platform defenses critical (13 June 2026). MemeBurn

INTEL WATCH

Watching the watchers. Guarding the guardians.

CYBERCRIMINALS USE FAKE DATING PROFILES TO TARGET RUSSIAN SOLDIERS IN NEW ESPIONAGE CAMPAIGN

IMAGE SOURCE: DIGITAL SHIELD

A newly identified cyberespionage group is using fake dating profiles and romantic messaging scams to target Russian military personnel, particularly those stationed in border regions and combat zones. The attackers pose as women seeking relationships or offering humanitarian support, gradually building trust through chat platforms like Telegram before tricking victims into downloading malicious apps or entering credentials on fake websites. Once compromised, the malware—capable of stealing files, tracking location data, recording conversations, and accessing messages—gives attackers broad surveillance over infected devices. Researchers say the campaign relies heavily on social engineering rather than technical exploits, using emotional manipulation and romance bait to extract sensitive military information for intelligence-gathering purposes (12 June 2026). Digital Shield

HIDDEN SPYWARE IN WAR ZONES MAY BE FAR MORE COMMON THAN REPORTED

IMAGE SOURCE: TECH POLICY

The increasing use of spyware in modern conflicts suggests that covert surveillance operations are becoming a routine part of warfare rather than rare exceptions. Governments and military-linked actors are believed to be deploying commercial and state-developed spyware tools to infiltrate smartphones used by soldiers, activists, and civilians, enabling real-time access to messages, location data, and communications. Because these tools are often built by private surveillance vendors and operate quietly on compromised devices, their use is difficult to detect and frequently goes unreported, making the true scale of deployment unclear. Experts warn that this normalization of spyware in conflict blurs the line between traditional intelligence gathering and active warfare, raising concerns about civilian privacy, escalation of cyber conflict, and the lack of clear international rules governing digital espionage on the battlefield (11 June 2026). Tech Policy

CHINA-LINKED HACKERS DEPLOY DUAL-STAGE SPYWARE ATTACK ON CZECH AND TAIWANESE TARGETS

IMAGE SOURCE: DIGITAL SHIELD

China-linked cyber espionage actors are targeting organisations in the Czech Republic and Taiwan using a sophisticated dual-method attack campaign designed to maximise infection success and evade detection. The operation begins with spear-phishing emails that deliver malicious ZIP files disguised as legitimate communications, such as meeting invitations or government notices. Inside the attachments, multiple execution paths are used: one relies on user-triggered shortcut files that launch PowerShell scripts, while another uses a self-contained malware dropper that activates automatically when an executable is opened. Both routes ultimately deploy a multi-stage payload involving a loader (Rust-based "Rustcloak") and a command-and-control agent known as "Azureveil," which enables remote control, data theft, and stealthy communication via cloud infrastructure. Security researchers note that the campaign is carefully designed to avoid sandbox detection and maintain persistence, reflecting a broader trend of state-linked groups combining social engineering with modular malware and cloud-based command systems to conduct intelligence gathering across government, academic, and financial sectors (2 June 2026). Dark Reading

FRANCE'S SECURE GOVERNMENT CHAT APP TCHAP HIT BY CYBER BREACH

IMAGE SOURCE: ENTREVUE.FR

France's state-run secure messaging platform Tchap was recently compromised after attackers gained access through a hijacked user account, allowing them to enter public chat rooms used by government employees. Cybersecurity authorities detected the intrusion and quickly blocked the affected account while launching an investigation to determine the extent of the exposure. Officials say private conversations remained protected by end-to-end encryption, but public channels—where sensitive administrative discussions can still take place—may have been accessed. While the breach appears limited in official assessments, an attacker has claimed to have extracted large volumes of data, including tens of thousands of user accounts and hundreds of thousands of messages, though these figures have not been verified. The incident has raised concerns about human-factor vulnerabilities, particularly social engineering, even in systems designed for high-security government communications (9 June 2026). Entrevue.fr

INTEL WATCH

Watching the watchers. Guarding the guardians.

THE AI ARMS RACE IS CHANGING CYBERSECURITY ECONOMICS

IMAGE SOURCE: SUUPLY NETWORK AFRICA

AI is fundamentally reshaping cybersecurity economics by driving down attack costs while increasing defense value—attacks now cost less and scale faster than defenses can keep up, forcing a structural reset in cyber-risk pricing, insurance, and management. This creates a $2 trillion opportunity in securing AI and developing AI security platforms, with model security, data pipeline protection, and AI governance becoming critical cyber spend components. The race is also straining computing supply chains: AI workloads demand massive GPU/memory capacity beyond supply capabilities, causing exponential cost increases for GPUs, memory, storage, and power, raising participation barriers and making AI-driven security infrastructure harder to secure. Africa faces a paradoxical role—integral to global AI supply chains (DRC's cobalt, Ghana's e-waste, data labeling labor) yet excluded from benefits through "digital extractivism," while needing massive resources to catch up globally, potentially diverting budgets from healthcare/education. The continent must assert agency, strengthen governance, and develop AI systems rooted in African values to shape equitable outcomes rather than remain a consumer of foreign technology (27 May 2026). Supply Network Africa

---

THE SPLINTERNET: HOW A FRACTURED INTERNET IS REWRITING GLOBAL CONNECTIVITY

IMAGE SOURCE: OPEN CANADA

The article explains the concept of the “splinternet,” which describes the gradual fragmentation of the once-open global internet into separate, semi-isolated digital ecosystems shaped by governments, corporations, and regional regulations. Instead of a single universal network where information flows freely, the internet is increasingly splitting into “digital blocs” where access to content, platforms, and services varies depending on geographic and political boundaries. This fragmentation is driven by factors such as data sovereignty laws, censorship regimes, trade disputes, and national security concerns, leading countries to build tighter control over their digital spaces. The piece argues that this trend undermines the original vision of a borderless internet, creating challenges for global communication, innovation, and shared standards, while also raising concerns about digital inequality and the concentration of power among a few dominant tech and state actors (1 June 2026). Open Canada

FORD REHIRES HUMAN ENGINEERS AFTER AI FAILS TO MATCH QUALITY CHECKS

IMAGE SOURCE: BBC

Ford has rehired more than 300 experienced engineers after discovering that its AI systems were not delivering the expected level of accuracy in vehicle quality checks. The company had introduced AI tools and automated inspection systems across its manufacturing plants to improve efficiency and reduce costs, including AI-powered cameras designed to detect defects on production lines. However, executives admitted that these systems lacked the practical knowledge and context that veteran inspectors had built up over years of experience, leading to gaps in quality control. Ford is now bringing back these workers not only to perform inspections but also to help train and improve its AI systems. The company says this "human-in-the-loop" approach has helped it regain stronger quality rankings in industry assessments, highlighting that while AI can boost productivity, it still struggles to fully replace human expertise in complex real-world manufacturing environments (30 June 2026). BBC

REPRESSION MONITOR

AI SPY IN THE BOARDROOM: HOW FOREIGN SURVEILLANCE RISKS CORPORATE SECRETS IN SOUTH AFRICA

IMAGE SOURCE: BUSINESS DAY

South African companies operating or partnering with Chinese firms face growing concerns about corporate espionage enabled by extensive state-linked surveillance systems. In China, foreign executives are reportedly subject to highly integrated monitoring that combines visa data, facial recognition networks, travel records, and AI-driven analytics to build detailed real-time profiles of individuals and their movements. This system can map relationships between visiting executives, local partners, and suppliers, potentially revealing sensitive business negotiations and strategic intentions. Critics argue that such surveillance infrastructure creates an uneven playing field, where state access to aggregated data can be used—directly or indirectly—to gain commercial advantage, influence negotiations, or identify key corporate relationships. The piece highlights broader concerns about data asymmetry, privacy risks, and the difficulty for foreign firms to protect proprietary information in environments where surveillance is deeply embedded in both public and commercial systems (1 June 2026). Business Day

WITHOUT WARRANTS: ILLEGAL SURVEILLANCE CHOKES NIGERIA'S CIVIC SPACE

IMAGE SOURCE: ICIR

Illegal surveillance practices without proper warrants are contributing to a shrinking civic space in Nigeria, where journalists, activists, and civil society organisations report being increasingly targeted through digital monitoring, cyberattacks, and alleged phone tracking. These actions are described as part of a broader pattern in which civic groups face intimidation and disruption, making it harder for them to investigate corruption, report on governance issues, or organise public advocacy. Although Nigerian law contains provisions meant to protect privacy and require judicial oversight for interception of communications, the investigation highlights concerns that these safeguards are often weakly enforced or bypassed in practice under broad "national security" justifications. The result, according to critics and rights groups, is growing self-censorship and reduced accountability, as fear of surveillance discourages open communication and limits democratic participation (30 May 2026). ICIR

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI CAMERAS IN SCHOOLS: SAFER CAMPUSES OR EXPANDING SURVEILLANCE?

IMAGE SOURCE: BUSINESS EXPLAINER

AI-powered security cameras are being increasingly introduced in schools to enhance campus safety by turning existing CCTV systems into intelligent monitoring tools that can detect potential threats in real time. These systems typically use computer vision to identify incidents such as unauthorized access, fights, weapon threats, or unusual behaviour, and then send instant alerts to school staff or security teams so they can respond faster than with traditional recording-only surveillance. Supporters argue that this shift from passive monitoring to proactive detection can improve emergency response times, reduce reliance on human monitoring, and make schools safer without replacing existing infrastructure. However, concerns persist around privacy, data collection, and the potential normalisation of constant surveillance in educational environments, especially when AI systems analyse student behaviour or integrate advanced identification tools. Critics also warn that the effectiveness of such systems depends heavily on accuracy, transparency, and strict limits on how data is stored and used (16 June 2026). Business Explainer

THE WATCHING MACHINE: HOW SURVEILLANCE POWER IS BEING PRIVATISED AND HIDDEN IN PLAIN SIGHT

IMAGE SOURCE: GEOSTRATA

Modern surveillance is increasingly being outsourced to private technology companies, shifting control over monitoring, identification, and enforcement from public institutions to corporate actors. Firms such as Palantir, Clearview AI, and other data analytics and spyware providers now supply governments with integrated systems that combine facial recognition, social media scraping, biometric scanning, and phone extraction tools to track individuals across borders and databases. In practice, this means decisions about who is flagged, investigated, detained, or deported are often shaped by privately built algorithms and proprietary infrastructures, even though these systems operate within public enforcement frameworks. This arrangement creates a blurred chain of accountability, where human officials act on machine-generated outputs without full transparency about how those outputs are produced or validated. The broader concern is that surveillance has become not just a state function, but a commercial ecosystem—one that is expanding faster than the legal and ethical frameworks meant to govern it, leaving significant gaps in oversight, rights protection, and public scrutiny (13 June 2026). GeoStrata

META'S SMART GLASSES "NAMETAG" LEAK REVEALS HIDDEN FACE RECOGNITION PLANS

IMAGE SOURCE: GAMES GG

Meta has been found to have quietly embedded an unreleased facial recognition system, internally called "NameTag," into its AI app connected to Ray-Ban and Oakley smart glasses. The system is designed to identify people seen through the glasses' camera by creating biometric "faceprints" and matching them against locally stored data on a user's phone, potentially alerting the wearer when a known person is detected. Although the feature has not been activated for users, evidence shows its core components were distributed through app updates used by millions of people, raising concerns that the company was far further along in developing real-time identification than previously disclosed. Privacy experts warn that such technology could normalise wearable surveillance in everyday life, effectively turning smart glasses into tools for scanning, identifying, and profiling people without their knowledge or consent. Following public scrutiny, reports indicate that Meta has begun removing the facial recognition components from the app, though questions remain about whether similar features will reappear in future updates (11 June 2026). Games.GG

FOOTBALL FANS, YOU'RE BEING WATCHED: THE HIDDEN SURVEILLANCE BEHIND MODERN STADIUMS

IMAGE SOURCE: THE JAPAN TIMES

Modern football stadiums and matchday environments are increasingly embedded with surveillance technologies that track and analyse fans in real time, turning sporting events into highly monitored digital spaces. Systems such as facial recognition cameras, ticketing-linked identity databases, mobile tracking via apps and Wi-Fi networks, and behavioural analytics tools are being used to monitor crowd movement, identify individuals, and assess fan behaviour. While these tools are often justified as necessary for security, fraud prevention, and crowd control, they also enable detailed profiling of spectators without clear transparency about how long data is stored or how it is shared. The result is a matchday experience where attending a game is no longer just physical participation, but also a form of continuous data generation, raising concerns about privacy, consent, and the expanding reach of surveillance beyond traditional security contexts (10 June 2026). Wired

INTEL WATCH

Watching the watchers. Guarding the guardians.

SILENCED BY SPYWARE: THE HIDDEN COST OF BEING A TARGET

IMAGE SOURCE: IDN-INDEPTHNEWS

Constant, large-scale digital monitoring is increasingly shaping how people think, speak, and participate in public life, creating a global "surveillance ecosystem" that affects citizens, activists, journalists, and civil society groups. Driven by governments and private actors, this system combines tools like facial recognition, biometric tracking, spyware, and continuous data collection to monitor behavior across both online and offline spaces. While often justified through national security or crime prevention narratives, such pervasive surveillance is contributing to a "chilling effect," where people self-censor out of fear that their communications or activities are being watched or recorded. Over time, this reduces public debate, weakens civic participation, and discourages collective action, as individuals and organisations adjust their behaviour to avoid potential risks. The result is a quieter public sphere where freedom of expression and association are increasingly constrained not by direct censorship, but by the anticipation of being constantly observed (15 June 2026). IDN-InDepthNews

FROM SPYWARE SELLERS TO SPY TARGETS: HOW DEMOCRACIES DRIFT INTO DIGITAL AUTHORITARIANISM

IMAGE SOURCE: THE CONVERSATION

The article argues that some democratic governments are increasingly adopting the same surveillance and censorship tools once associated with authoritarian states, blurring the line between protector and perpetrator of digital repression. It highlights how commercial spyware—such as Pegasus and similar tools—originally exported under the justification of counterterrorism and crime prevention has in several cases been linked to the surveillance of journalists, activists, and political opponents both domestically and abroad. Countries including Israel and India are used as key examples to show how spyware exports, weak oversight, and national security justifications have enabled a global ecosystem where surveillance technologies are normalised and widely deployed. The piece warns that this trend is part of a broader shift toward "digital authoritarianism," where even democracies contribute to shrinking civic space through monitoring, censorship, and platform control, gradually eroding privacy, accountability, and democratic freedoms (5 June 2026). The Conversation

INTEL WATCH

Watching the watchers. Guarding the guardians.

ISRAEL AND INDIA SHOW HOW DEMOCRACIES DRIFT TOWARDS DIGITAL AUTHORITARIANISM

IMAGE SOURCE: SCROLL.IN

Israel and India illustrate how democracies can gradually adopt surveillance and censorship practices that resemble those of authoritarian states, especially through the use and export of advanced digital tools. In Israel, state-regulated spyware exports—particularly NSO Group's Pegasus—have been marketed for counterterrorism and crime prevention but have repeatedly been linked to the surveillance of journalists, activists, lawyers, and political opponents across multiple countries. In India, similar technologies have allegedly been used domestically against journalists and opposition figures, alongside broader practices such as internet shutdowns, content takedowns, online harassment, and increased regulatory pressure on critical voices. These developments are presented as part of a wider global pattern in which democratic governments normalise digital surveillance under security justifications, gradually narrowing civic space and weakening accountability. The broader concern is that such "digital authoritarianism" evolves slowly through legal and administrative measures, making it harder to detect but steadily eroding privacy, free expression, and democratic oversight (10 June 2026). Scroll.in

SPYWARE AS A TOOL OF COERCIVE CONTROL: HOW SURVEILLANCE TECHNOLOGY ENABLES HIDDEN ABUSE

IMAGE SOURCE: OPEN FORUM

Spyware and monitoring apps are increasingly being used as instruments of coercive control in abusive relationships, allowing perpetrators to secretly track, monitor, and manipulate victims over long periods of time. These tools can operate invisibly on smartphones and other devices, enabling access to messages, calls, photos, location data, and even microphones or cameras without the victim's awareness. Because the surveillance is continuous and often undetectable, it creates a persistent sense of being watched, which can erode autonomy, increase fear, and isolate victims from friends, family, or support networks. Experts warn that this form of technology-facilitated abuse is especially harmful because it extends control beyond physical presence, making escape more difficult and reinforcing dependence. The broader concern is that commercial spyware tools—originally marketed for legitimate purposes like parental control or device security—are being repurposed for intimate partner surveillance, highlighting major gaps in regulation, detection, and digital safety protections (15 June 2026). Open forum

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI AS TERRORISTS' NEW WEAPON: FROM PROPAGANDA TO POSSIBLE ATTACKS

IMAGE SOURCE: ADF

Terrorist groups like Islamic State and al-Qaida are aggressively leveraging AI to supercharge propaganda, recruitment, and potentially attacks—using voice cloning, video/photo manipulation, and generative text to produce slick, viral content rapidly with minimal resources, creating AI-generated news anchors (e.g., IS's News Harvest), fake celebrity/politician statements, and AI chatbots that continuously engage users across platforms, adapt to vulnerabilities, and passively recruit by analyzing ideology. AI enables media spawning (thousands of malicious variants from one image), automated multilingual translation, fully synthetic propaganda, variant recycling, personalized targeting, and subverting moderation—expanding reach exponentially while evading detection. Though currently accelerating existing activities rather than revolutionizing operations, experts warn AI could soon enable organizing uprisings, building WMD, and developing drones/self-driving car bombs, prompting calls for industry standards, government-industry collaboration, AU AI security laws, digital forensics training, and intelligence sharing as African nations face expensive but critical investment decisions to lead versus be led (5 February 2026). ADF

AFRICAN DATA PROTECTION LAWS: FROM PRIVACY SHIELD TO POLITICAL LEVER

IMAGE SOURCE: LAWFARE

African data protection laws, initially framed as shields guarding privacy rights, are increasingly being weaponized as levers for cybersecurity control and political authority, with regimes transforming GDPR-inspired frameworks into tools for surveillance, data localization, and tech sovereignty. While 36/55 African countries now have data protection laws (e.g., South Africa's POPIA, Nigeria's DPA, Kenya's DPA), many governments exploit these laws not just to protect citizens' rights but to enforce data sovereignty—mandating local data storage, restricting cross-border transfers, and leveraging compliance requirements to control foreign tech firms and monitor domestic dissent. The shift from protectionist intent to authoritarian leverage reflects a broader trend where data laws serve dual purposes: empowering citizens against misuse while enabling states to consolidate power, restrict digital freedom, and assert control over Africa's rapidly digitizing economy (1 June 2026). Lawfare

REPORT CLAIMS IRAN'S IRGC USES SOCCER STADIUMS FOR STATE SURVEILLANCE

IMAGE SOURCE: STREAMLINE

A report alleges that Iran's Islamic Revolutionary Guard Corps (IRGC) is using the country's football infrastructure—especially stadiums, clubs, and fan systems—as part of a wider surveillance and security network to monitor citizens. It claims IRGC-linked officials are embedded in football governance and club management, allowing them to influence stadium security operations and fan oversight. The report also suggests that technologies such as facial recognition cameras, ID-linked ticketing systems, and detailed seat-mapping in major stadiums are being used to identify and track spectators. Critics argue this system could enable the monitoring of political dissent under the guise of sporting event security, raising concerns about privacy, civil liberties, and the politicisation of football infrastructure (10 June 2026). Streamline .

INTELLIGENCE AGENCIES

SOUTH AFRICA'S HOME AFFAIRS TO ROLL OUT FACIAL RECOGNITION AT AIRPORTS AND BORDERS

IMAGE SOURCE: MY BROADBAND

South Africa's Department of Home Affairs is set to introduce facial biometric verification at all major ports of entry, including airports and land borders, as part of a broader upgrade to its Electronic Traveller Authorisation (ETA) and Enhanced Movement Control System (EMCS 2.0). The system, already piloted successfully at OR Tambo, Cape Town International, and Lanseria airports, uses facial recognition to automate identity checks for travellers entering and leaving the country. Authorities say the rollout—expected to be completed by March 2027—will speed up immigration processing, reduce queues, and strengthen border security by replacing manual passport checks with real-time biometric matching. The initiative forms part of South Africa's wider shift toward digital identity systems and integrated border management, aimed at modernising immigration services while improving fraud detection and operational efficiency (24 May 2026). My Broadband

GAUTENG MOVES TOWARD AI SURVEILLANCE IN CLASSROOMS AS SCHOOL SAFETY PUSH INTENSIFIES

IMAGE SOURCE: ST THE SOUTH AFRICAN

Gauteng's education authorities are proposing the rollout of AI-powered surveillance cameras in classrooms as part of a broader plan to tackle rising levels of violence and misconduct in schools across the province. The system would upgrade existing CCTV infrastructure to include artificial intelligence capabilities such as facial and behavioural recognition, allowing real-time detection of incidents like fights, weapon possession, or unauthorised access, with alerts sent to school officials or security responders. Officials argue that the technology could improve safety, deter criminal behaviour, and help restore order in learning environments that have experienced thousands of reported violent incidents in recent years. The proposal also includes wider biometric access controls and integration with other security systems. However, it has sparked concerns about student privacy, data protection, and the risks of normalising continuous surveillance in educational spaces, especially given uncertainties around how long data would be stored and who would have access to it (17 June 2026). The South African

INTEL WATCH

Watching the watchers. Guarding the guardians.

KENYA'S PARLIAMENT APPROVES NEW NATIONAL CYBERSECURITY AGENCY

IMAGE SOURCE: THE STAR KENYA

Kenya's Parliament has approved the creation of the National Cybersecurity Agency (NCSA), an autonomous body that will coordinate the country's cybersecurity efforts and strengthen the protection of critical digital infrastructure. The agency will oversee national cybersecurity operations, monitor cyber threats, conduct security audits, coordinate incident response, and establish a Cybersecurity Centre of Excellence to promote research, innovation, and skills development. The move aims to improve Kenya's resilience against growing cyber threats while supporting the country's expanding digital economy and protecting essential government and private sector systems (25 June 2026). Africa Business Communities

---

KENYA CONSIDERS LINKING NATIONAL ID DATABASE TO CCTV FACIAL RECOGNITION NETWORK

IMAGE SOURCE: BIOMETRIC UPDATE

The article reports that Kenya is considering linking its National Registration Bureau database with a facial recognition CCTV network across six major cities to help law enforcement identify crime suspects more quickly. The proposed system would match images captured by surveillance cameras with photographs stored in the national ID database, strengthening criminal investigations and public security. While the government says the initiative will improve policing and crime detection, privacy advocates have raised concerns about increased surveillance, data protection, and the need for strong legal safeguards to prevent misuse of citizens' biometric information (26 June 2026). Biometric Update

INTEL WATCH

Watching the watchers. Guarding the guardians.

NAMIBIA'S CYBERCRIME BILL SPARKS PRESS FREEDOM AND SURVEILLANCE CONCERNS

IMAGE SOURCE: THE AFRICA REPORT

Namibia's proposed Cybercrime Bill is facing criticism from journalists, digital rights advocates, and civil society groups who argue that some of its provisions could threaten press freedom, whistleblower protections, and privacy rights. Critics are particularly concerned about broad powers related to online content moderation, real-time data collection, communication interception, and surveillance, as well as clauses that could allow the law to override other legislation in cyber-related matters. While supporters say the bill is necessary to combat cybercrime, online abuse, fraud, and attacks on critical infrastructure, opponents warn that vague definitions and expansive investigative powers could be used to suppress reporting, discourage whistleblowing, and increase state monitoring without sufficient safeguards or oversight. The debate highlights the challenge of balancing cybersecurity objectives with constitutional rights such as freedom of expression, access to information, and privacy (14 June 2026). The Namibian

STARLINK IN AFRICA: DIGITAL BREAKTHROUGH OR SOVEREIGNTY RISK?

IMAGE SOURCE: MAIL & GUARDIAN

The expansion of Starlink across Africa is framed as both a major connectivity breakthrough and a potential geopolitical and data sovereignty concern. On one hand, satellite internet offers a fast way to close the digital divide in remote and underserved areas where traditional fibre and mobile infrastructure are limited, improving access to education, business services, and emergency communications. On the other hand, the growing reliance on a foreign-owned satellite network raises questions about regulatory control, data governance, and national security, particularly around who can access user data and how much oversight African governments actually have over the infrastructure. The debate highlights a broader tension between accelerating digital inclusion and maintaining control over critical communications infrastructure, with concerns that dependency on external providers could shape the continent's digital future in ways that are not fully governed by local institutions (10 June 2026). Mail&Guardian

GACHAGUA EXPOSES ALLEGED STATE SURVEILLANCE OF STANDARD MEDIA JOURNALIST OVER CRITICAL REPORTING

IMAGE SOURCE: STREAMLINE

The article reports that former Deputy President Rigathi Gachagua has accused the Kenyan government of engaging in surveillance and intimidation targeting journalists, particularly those working with the Standard Media Group. He claims that a journalist was being trailed by security operatives following the publication of critical reports about the administration, and links this to a broader pattern of pressure against the media, including alleged attacks, abduction attempts, and harassment of reporters covering corruption and governance issues. Gachagua argues that these actions amount to a deliberate effort to suppress press freedom ahead of the 2027 elections, and he has called on media organisations and rights groups to defend journalists and resist state intimidation (30 June 2026). Streamline

DIGITAL PRIVACY RIGHTS IN EGYPT: BALANCING NATIONAL SECURITY AND DATA PROTECTION IN THE DIGITAL AGE

IMAGE SOURCE: RECORD OF LAW

The article discusses how Egypt's approach to digital privacy is shaped by a constant tension between protecting citizens' data and prioritising national security. It explains that while Egypt has introduced laws like the Personal Data Protection Law (2020), these frameworks are still weak in practice because security agencies often have broad access to communications data and are exempt from many privacy safeguards. The piece highlights that surveillance powers under cybercrime and telecommunications laws allow state authorities to monitor online activity, sometimes without strong judicial oversight, raising concerns about mass surveillance and limited transparency. At the same time, the government justifies these measures as necessary for counter-terrorism and maintaining stability. Overall, the article argues that Egypt's digital privacy system is uneven: legal protections exist on paper, but in practice national security priorities often override individual data protection rights, leaving citizens with limited control over their personal information (30 June 2026). Record of Law

INTEL WATCH

Watching the watchers. Guarding the guardians.

HOW ENCRYPTED SIGNAL CHATS BECAME CENTRAL TO MINNEAPOLIS ICE PROTEST INVESTIGATIONS

IMAGE SOURCE: THE INTERCEPT

A federal investigation into protests against Immigration and Customs Enforcement (ICE) operations in Minneapolis has highlighted how encrypted messaging apps like Signal were allegedly used to coordinate activist activity. Prosecutors say some individuals involved in the protests used private group chats to organise surveillance of ICE agents, share real-time location information, and plan actions aimed at disrupting enforcement operations during a large federal immigration crackdown known as Operation Metro Surge. The case has led to multiple indictments, with authorities arguing the communications show coordination beyond peaceful protest, while critics raise concerns about the use of digital surveillance and encrypted chat analysis in building cases against activists. The situation has intensified debate in the US over the boundaries between protest rights, digital privacy, and law enforcement monitoring of encrypted platforms (17 June 2026). The Intercept

BULGARIA LICENSED SURVEILLANCE EXPORTS TO RIGHTS VIOLATORS

IMAGE SOURCE: HUMAN RIGHTS WATCH

Between 2018 and 2023, Bulgaria issued export licences for surveillance technologies, including interception systems and spyware tools, to countries with documented histories of human rights violations and political repression. According to a Human Rights Watch investigation, these tools can enable governments to monitor communications, track individuals, and conduct intrusive digital surveillance that has been used against journalists, activists, and opposition figures. The report argues that such exports highlight major weaknesses in European Union oversight of “dual-use” technologies, where surveillance tools marketed for security or law enforcement purposes can also be used for abuse. It calls for stronger EU-level controls, greater transparency in licensing decisions, and stricter human rights due diligence to prevent surveillance technology from being supplied to regimes likely to misuse it (18 June 2026). Human Rights Watch

INTEL WATCH

Watching the watchers. Guarding the guardians.

HOW CHINA IS QUIETLY EXPORTING ITS SURVEILLANCE MODEL TO OTHER COUNTRIES

IMAGE SOURCE: MONEY CONTROL

China is exporting its surveillance model beyond borders, with a recent New York Times investigation revealing Beijing's growing security footprint in the Solomon Islands where Chinese police proposed community surveillance measures—including household registration cards, fingerprint/palm print collection, and neighborhood monitoring inspired by the Mao-era "Fengqiao Experience"—alarming observers that Beijing is expanding not just geopolitical influence but its state security model itself; this differs from America's military alliance-focused approach, as China emphasizes internal security, surveillance infrastructure, and regime stability, a pitch attractive to authoritarian governments and fragile democracies concerned about unrest, while China's 2022 security pact with the Solomon Islands (after 2021 riots), $1.5M riot-control equipment donations, embedded police officers, and 138-country police training programs since 2000 signal a shift from exporting infrastructure/trade to governance models and security philosophy, though local backlash suspended the Fighter One pilot program, revealing limits to China's approach and highlighting an emerging global contest over future security and governance models (28 June 2026). Money control

---

KEY US SPY PROGRAM FACES UNCERTAIN FUTURE AS SURVEILLANCE POWERS EXPIRE

IMAGE SOURCE: CW 39

A major US surveillance authority known as Section 702 of the Foreign Intelligence Surveillance Act (FISA) has entered a period of uncertainty after Congress failed to approve an extension before its deadline. The program allows US intelligence agencies to collect communications from foreign targets located outside the United States without obtaining individual warrants, but it has long been controversial because Americans' communications can also be incidentally collected and searched. Supporters argue the tool is critical for counterterrorism, cybersecurity, and foreign intelligence operations, while critics say it enables warrantless surveillance and lacks sufficient privacy protections. Although the legal authority has lapsed, a court certification issued earlier this year means existing surveillance activities can largely continue in the short term, leaving lawmakers to continue debating the balance between national security and civil liberties (12 June 2026). CW 39

INTEL WATCH

Watching the watchers. Guarding the guardians.

US SECRET SERVICE TESTS FACE-SCANNING APP AS AI SURVEILLANCE EXPANDS IN LAW ENFORCEMENT

IMAGE SOURCE: THE STAR

The US Secret Service has begun piloting a mobile facial-recognition app called "Sentry" that allows officers to scan a person's face or fingerprints using a smartphone and compare the data against government biometric databases to help identify individuals and assess potential threats. The system is currently being tested by a small group of about 25 uniformed officers in Washington, D.C., and is part of a broader move by US federal agencies to integrate AI-driven identification tools into frontline policing and protective operations. Officials say the goal is to improve the ability to detect and respond to potential security risks more quickly, especially amid rising concerns about threats against public officials. However, the rollout has also raised privacy and civil liberties concerns, with critics warning that expanding facial recognition into everyday encounters could normalise constant identification checks and increase the risk of overreach or misidentification (16 June 2026). The Star

HOW GOVERNMENT SURVEILLANCE TOOLS ARE EXPANDING IN THE UNITED STATES THROUGH DATA MARKETS AND AI

IMAGE SOURCE: LAP PROGRESSIVE

In the United States, government surveillance capabilities are increasingly expanding through the purchase of commercially collected personal data and the deployment of AI-powered monitoring tools. Rather than relying solely on traditional warrants, US agencies can access vast datasets—such as location histories, online activity patterns, and behavioural profiles—sourced from data brokers that aggregate information from apps, devices, and digital services. The analysis highlights concerns that this creates a largely unregulated "surveillance marketplace," where sensitive personal information can be bought and used for law enforcement or intelligence purposes with limited transparency. It also raises questions about accountability and oversight, as the growing use of facial recognition, spyware, and predictive analytics blurs the line between targeted investigation and broader population-level monitoring (9 June 2026). LAP Progressive

INTEL WATCH

Watching the watchers. Guarding the guardians.

SMART CITIES, SILENT SURVEILLANCE: THE RISE OF AI-DRIVEN CONTROL IN THE GULF

IMAGE SOURCE: ARAB CENTER WASHINGTON DC

Gulf states such as Saudi Arabia and the UAE are embedding advanced surveillance technologies into their smart city projects, turning urban infrastructure into highly data-driven environments where daily life is continuously monitored and analysed. Systems such as facial recognition, biometric databases, predictive analytics, and large-scale sensor networks are being integrated into transport, public services, and urban planning, enabling real-time tracking and behavioural profiling of residents. While these initiatives are often framed as innovation and efficiency projects supported by "ethical AI" guidelines, concerns remain that weak oversight and broad security exemptions allow extensive surveillance with limited transparency or public accountability. Critics warn that these developments risk normalising digital monitoring as a core feature of governance, raising serious implications for privacy, civil liberties, and the long-term balance between technological progress and state control (3 June 2026). Arab Center Washington DC

AUSTRIA'S SPYWARE LAW UNDER FIRE AS KEY DEBATE FOCUSES ON WHO CONTROLS THE EXPLOIT SUPPLY CHAIN

IMAGE SOURCE: DIGITAL INTELLIGENCE

Austria's proposed spyware legislation is facing renewed legal and constitutional scrutiny, with critics arguing that the most critical unresolved issue is not just whether the state should be allowed to hack devices, but who develops, supplies, and potentially exploits the vulnerabilities used to do so. The debate centres on the use of so-called "state trojan" tools that allow authorities to infiltrate encrypted communications on phones and computers, raising concerns about privacy, proportionality, and the risk of intentionally preserving software vulnerabilities for surveillance purposes. Opponents warn that building legal frameworks around hacking tools effectively creates a market for exploits, which could be abused or leak into criminal hands. Supporters argue the law is necessary for serious investigations in a digital environment dominated by end-to-end encryption. The case reflects a broader European tension between expanding investigative powers and protecting cybersecurity integrity and fundamental rights (12 June 2026). Digital Intelligence

INTEL WATCH

Watching the watchers. Guarding the guardians.

UK PLANS AI FACE SCANS TO ESTIMATE AGE OF MIGRANT CHILDREN

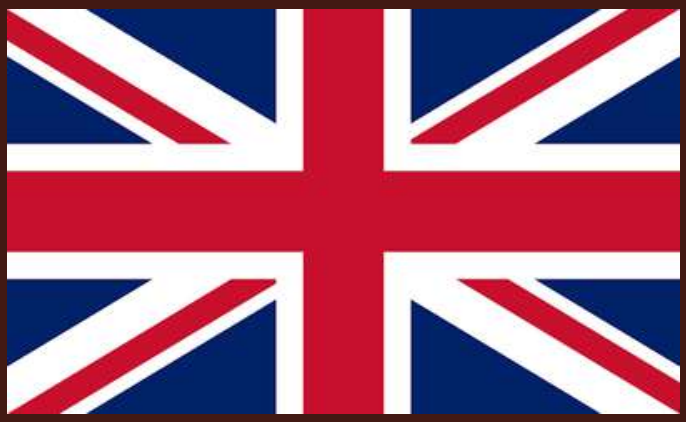


IMAGE SOURCE: RESULT SENSE

The UK Home Office plans to trial AI facial recognition tools to estimate the age of asylum seekers who claim to be children, using machine learning to assess facial features when official documentation is missing or disputed. Officials say the system could help improve consistency in age verification and reduce errors in placing adults into child protection systems. However, the proposal has drawn criticism from rights groups and child protection advocates, who warn that AI age estimation can be inaccurate, biased across different ethnic groups, and risky if used to make legal or safeguarding decisions affecting vulnerable migrants (18 June 2026). Result Sense

---

U.K. SOCIAL MEDIA BAN STOKES FEARS OF GOVERNMENT SURVEILLANCE

IMAGE SOURCE: DIGITAL INTELLIGENCE

The UK government has announced plans to ban social media access for users under 16 as part of a major online safety overhaul aimed at reducing children's exposure to harmful and addictive online content. The policy would restrict under-16s from platforms such as TikTok, Instagram, Snapchat, Facebook, YouTube, and X, while still allowing access to messaging services like WhatsApp and Signal. Officials say the move is designed to protect young people's mental health and reduce risks linked to excessive screen time, online harassment, and harmful content, and it is expected to be enforced from 2027 with mandatory age verification requirements for tech companies. The decision has sparked debate, with supporters calling it a strong protective measure for children, while critics warn it could be difficult to enforce and may push young users toward less regulated online spaces (16 June 2026). AOL

INTEL WATCH

Watching the watchers. Guarding the guardians.

FROM OVERSIGHT TO COERCION: HOW GOVERNMENTS ARE RESHAPING AI SAFETY INTO POLITICAL CONTROL

IMAGE SOURCE: THE CONVERSATION

Authoritarian-style governments are increasingly using "AI safety" rules and regulation frameworks not just to oversee technology companies, but to pressure them into aligning with political and security goals. Instead of treating safety standards as neutral protections for users, these governments can redefine what counts as "safe" in ways that favour state surveillance priorities or restrict companies that refuse to remove safeguards against things like surveillance or autonomous weapons. This creates a situation where compliance becomes tied to access to major government contracts, forcing companies to choose between maintaining ethical safeguards or staying competitive in lucrative state markets. Over time, this can shift AI development away from public-interest protections and toward systems designed to be controllable by governments, raising concerns about reduced transparency, weaker safeguards, and growing political influence over how AI is built and deployed (4 June 2026). The Conversation

31 COUNTRIES POSE HIGH DIGITAL SURVEILLANCE RISKS AS GOVERNMENTS EXPAND MONITORING POWERS

IMAGE SOURCE: RECORDED FUTURE

A new global assessment of state digital surveillance warns that governments are increasingly using a combination of telecom interception, commercial spyware, AI-powered monitoring systems, biometric databases, and large-scale data aggregation to track individuals, businesses, and foreign visitors. The report identifies 31 countries as presenting high or very high surveillance risks due to advanced monitoring capabilities, weak oversight, and a history of targeting critics, journalists, activists, and foreign entities. Researchers highlight five key surveillance methods—network interception, device compromise, platform-level access, public-space surveillance, and data aggregation—arguing that the growing availability of commercial spyware and AI tools is making state surveillance more powerful and accessible. The report warns that inadequate oversight can lead to privacy violations, intellectual property theft, reputational harm, and broader human rights concerns, while urging organisations and travellers to assess surveillance risks before operating in higher-risk jurisdictions (17 June 2026). Recorded Future

RIGHTS GROUPS CONDEMN CANADA'S RUSH TO EXPAND STATE SURVEILLANCE POWERS

IMAGE SOURCE: THE CONVERSATION

Civil liberties organisations, privacy advocates, and technology experts have criticised the Canadian government for cutting short parliamentary debate on Bill C-22, a controversial surveillance proposal that would expand law enforcement access to personal data and potentially require technology companies to facilitate government access to digital communications. Critics argue the bill could weaken encryption, increase data retention requirements, expand information-sharing powers, and create significant privacy and cybersecurity risks, while limiting public scrutiny of measures they describe as some of the most far-reaching surveillance powers proposed in Canada in decades. They have called for greater transparency, stronger safeguards, and a full public debate before any such powers are enacted (18 June 2026). Ifex

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

INTEL WATCH

Watching the watchers. Guarding the guardians.

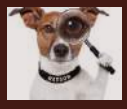
GET INVOLED!

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!