Issue #15

INTEL WATCH

August 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

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #15 OF THE WATCHER

In this Issue #15 of *The Watcher*, we turn our attention to a digital world where the boundaries between cybersecurity, surveillance and everyday technology are becoming increasingly difficult to distinguish. Across Africa and beyond, governments, corporations and cybercriminals are deploying increasingly sophisticated technologies to identify, monitor, protect and exploit people. From AI-powered cybercrime and mobile banking attacks to biometric identity systems, spyware and digital borders, this edition asks a fundamental question: What happens when the technologies built to make us safer also create new ways to watch, control and exploit us?

In this Issue #15, we examine the rapidly evolving cyber threat facing South Africa and the wider continent. South Africans are confronting an expanding ecosystem of digital fraud, banking-app takeovers, ransomware, malware and social-engineering attacks, with criminals increasingly targeting people rather than simply breaking into institutions. Across Africa, artificial intelligence is accelerating this transformation, enabling criminals to automate phishing, impersonation, fraud and cyberattacks at a scale that is increasingly difficult for law-enforcement agencies to match. At the same time, the growing dependence on digital infrastructure—from data centres and cloud services to smartphones and digital identities—is creating new questions about who controls the systems on which African societies increasingly depend.

This edition also explores the expanding surveillance landscape across Africa and the world. We investigate allegations of telecom surveillance targeting journalists and activists in Nigeria, concerns over intelligence monitoring in Kenya, and the absence of adequate legal oversight for AI-powered surveillance infrastructure in Nigeria's Enugu State. From Mozambique's legal battle over government access to communications, to allegations of biometric monitoring of protesters in India and mass-surveillance technologies used against demonstrators in Argentina, these developments reveal how tools originally justified in the name of security can increasingly intersect with political dissent, journalism and civic space.

Issue #15 further examines the growing normalisation of biometric and AI-powered surveillance. South Africa's new AI-powered Electronic Travel Authorisation system promises faster and more secure border processing, while the country's proposed Digital ID system could place increasingly sensitive biometric information at the centre of everyday access to public services. Across the continent, digital identity programmes, facial recognition and biometric verification are expanding rapidly—raising an increasingly urgent question: when identity becomes data, who gets to control it? The same concern extends to the smartphones people carry every day, with research highlighting extensive data collection built into some of Africa's most popular devices.

Finally, this issue looks beyond individual technologies to the changing balance of power in the digital age. Commercial spyware such as Pegasus continues to demonstrate how smartphones can become instruments of covert surveillance, while Apple’s spyware warnings and new US reporting requirements could bring greater visibility to government hacking. Meanwhile, debates over the Five Eyes, Canada's proposed surveillance powers and China's expanding AI influence in Africa highlight a wider struggle over digital sovereignty, encryption, intelligence and technological dependence. As governments and companies gain unprecedented abilities to collect, analyse and act upon digital information, The Watchercontinues to ask who is watching the watchers—and who is protecting the people being watched.

Across this month's investigations, one message is clear: cybersecurity is no longer simply about protecting networks from hackers. It is about determining who controls our identities, our data, our devices and ultimately our digital lives. As AI and surveillance become embedded into everything from banking and border control to policing, smartphones and national security, the need for transparency, accountability and human-rights protections has never been more urgent.

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

THIS MONTH'S FOCUS

SURVEILLANCE UPDATES - pages 4-23

This section examines an increasingly aggressive cyber threat landscape in which criminals are no longer simply attacking networks, but exploiting identities, devices, trusted brands and human behaviour. In South Africa, readers will find coverage of telecom fraud costing major operators nearly R200 million, banking-app takeovers, malicious Android applications impersonating DStv, Takealot, South African Airways and SARS, rising digital-banking fraud, ransomware and AI-powered social engineering. The section also explores wider African and global developments, including Kenya's surge in QR-code phishing, the growing use of artificial intelligence in African cybercrime, cyber-espionage against African organisations, hidden tracking software embedded in popular smartphones, spyware warnings, banking trojans, malware targeting connected vehicles, browser-based malware, government ransomware attacks and the hijacking of thousands of internet-connected cameras. Together, these stories show how cybersecurity threats are moving beyond conventional hacking towards an environment in which trust, identity, connected devices and everyday digital behaviour have themselves become attack surfaces.

REPRESSION MONITOR - pages 24-29

This section tracks the growing use of surveillance technologies, digital monitoring and state security powers against political actors, protesters, journalists and civil society. It examines allegations that Kenya's National Intelligence Service sought to intercept former Deputy President Rigathi Gachagua's political address, Nigeria's reported use of telecommunications records to identify activists through their networks of contacts, and Mozambique's legal battle over government powers to monitor communications and suspend internet services. Beyond Africa, the section looks at facial recognition and AI surveillance of protesters in India, drones and biometric monitoring of demonstrations in Argentina, authoritarian uses of AI-assisted surveillance across countries including China, Russia, Iran, Turkey and Belarus, and India's controversial attempt to require a government cybersecurity application on smartphones. Commercial spyware also remains central, with renewed scrutiny of Pegasus and the broader global market in state-linked hacking tools. Collectively, these stories demonstrate how surveillance increasingly operates not only as a tool for security and investigation, but as a potential mechanism for identifying dissent, mapping political networks, restricting anonymity and influencing whether people feel safe enough to protest, organise or speak freely.

INTELLIGENCE AGENCIES - pages 30-38

This section explores how governments and intelligence institutions are expanding their capabilities through biometrics, artificial intelligence, commercial spyware, digital identity systems and communications surveillance, while exposing the growing accountability challenges that accompany these technologies. South Africa features prominently through its proposed Digital ID system, biometric verification of social-grant beneficiaries and the rollout of an AI-powered Electronic Travel Authorisation system that uses facial recognition and digital identity verification at major airports. Elsewhere in Africa, readers will encounter Senegal's efforts to strengthen protection of critical information infrastructure and Nigeria's multi-billion-naira Enugu Safe City surveillance system, which combines more than 1,000 cameras, facial recognition, automatic number-plate recognition and drones despite the absence of a dedicated oversight law. The section also examines Morocco's alleged use of Pegasus spyware, India's constitutional battle over AI-powered protest surveillance, Brazil's attempt to regulate facial recognition, the global Five Eyes intelligence network, Canada's struggle over lawful access to encrypted cloud data and new U.S. plans to publicly report government spyware use. It concludes by exploring how Chinese military-linked researchers are adapting advanced AI capabilities for cyber operations, surveillance, drones and intelligence gathering. Across these cases, the central question is not simply what intelligence agencies can now do, but whether legal safeguards, democratic oversight and public accountability are evolving quickly enough to govern the extraordinary surveillance powers emerging in the AI age.

SURVEILLANCE UPDATES

SPY TECH FOR SALE? MADLANGA COMMISSION HEARS CLAIMS OF STATE IMPERSONATION

IMAGE SOURCE: SABC

South Africa's Madlanga Commission of Inquiry has heard allegations that Katiso "KT" Molefe, the late taxi boss Mswazi Msibi and businessman Steve Motsumi presented themselves as representatives of the South African state while engaging foreign suppliers over surveillance and communications-jamming technology. Evidence leader Advocate Matthew Chaskalson told the Commission that communications extracted from Msibi's cellphone suggested the three men were involved in efforts to market or sell "grabber" technology to the government of Eswatini, although it remains unclear whether any transaction was ultimately completed. Particularly concerning is the allegation that technology providers were prepared to engage with the men and invite them to sign contracts on the basis that they represented the South African government. Chaskalson further raised the possibility that individuals with access to suppliers of sophisticated surveillance technology could potentially obtain or use such capabilities independently, rather than solely through legitimate state procurement channels. The allegations place the commercial market for interception, surveillance and communications-jamming technologies under renewed scrutiny, raising questions about who can acquire powerful surveillance capabilities, how suppliers verify the identities and authority of prospective government customers, and what safeguards exist to prevent sophisticated spy technology from ending up in private hands. SABC News

MTN, VODACOM, AND TELKOM TAKE R198.9 MILLION PAIN FROM SYNDICATES IN SOUTH AFRICA

IMAGE SOURCE: MY BROADBAND

South Africa's largest telecommunications companies lost R198.9 million to subscription fraud syndicates in the 12 months to April 2026, as reported cases surged by an extraordinary 307% year-on-year to 14,897 incidents. The figures, contained in a report from the Communications Risk and Information Centre (COMRiC), show how organised criminals are increasingly exploiting legitimate identity and financial information to defraud telecom operators. Syndicates reportedly use genuine documents and authentic bank statements when applying for expensive telecom services, sometimes purchasing bank-account information from account holders and using it to establish apparently legitimate customer profiles before obtaining services and deliberately refusing to pay. Although the average loss per incident fell by 75% to approximately R13,400, the sheer volume of cases pushed total losses to nearly R200 million, with March 2026 recording the highest monthly figure at 2,475 cases. COMRiC members—including MTN, Vodacom, Cell C, Telkom and Liquid—are responding by sharing intelligence and developing a cross-industry database of fraud syndicates and their activities, reflecting growing recognition that criminals can exploit weaknesses across multiple networks rather than targeting a single operator. The report also highlights wider cyber risks facing South Africa's telecom infrastructure: the sector is experiencing persistent ransomware attacks, while SIM-swap fraud generated a further R4.26 million in losses from 383 cases during the reporting period. COMRiC CEO Thokozani Mvelase warned that WhatsApp messages, phone calls, SMSes and increasingly sophisticated impersonation scams are becoming major gateways for fraud, meaning that the industry's vulnerability is no longer purely technical—criminals are increasingly attacking trust itself. My Broadband

CRACKED INFRASTRUCTURE, CRACKED BUDGETS: SA MINISTER ADMITS CYBER FUNDING CAN'T KEEP UP AFTER SUPERCOMPUTER HACK

IMAGE SOURCE: RESEARCH PROFESSIONAL NEWS

South Africa's science minister Blade Nzimande has conceded, in a written parliamentary response dated 19 August, that the country's national high-performance computing infrastructure is squeezed, just months after a government-owned supercomputer was compromised and used for cryptocurrency mining. The incident he's referring to is the May breach of the Lengau supercomputer, hosted by the Centre for High Performance Computer in Cape Town, which was hacked and made to run cryptocurrency-mining malware — a stark illustration of how even national research infrastructure isn't immune to opportunistic cybercriminals looking to hijack compute power. On the funding side, the Department of Science, Technology and Innovation has ring-fenced over 292 million rand in the 2026-27 financial year for the National Integrated Cyber Infrastructure System (NICIS). But that allocation is being squeezed from multiple directions: Treasury budget cuts, escalating operational costs and shifting exchange rates have placed this budget under pressure, Nzimande admitted. In his own words, "the current allocations are therefore inadequate to sustain both operations and planned expansion targets." On the response side, the department is pushing ahead with a hardware refresh: the CSIR has already acquired and taken delivery of a new four-petaflop high-performance computing system, with the first phase expected to go live by the end of November and the completed system upgrade expected by the end of March next year. The staggered rollout is deliberate — the phased deployment aims to maintain continuity of national research-computing services while the new platform is commissioned and reduce reliance on the legacy Lengau environment, effectively weaning the country off the compromised system while the replacement comes online. Research Professional News

R5 MILLION AND RISING: SOUTH AFRICA'S DATA REGULATOR SHARPENS ITS TEETH ON GOVERNMENT CYBERSECURITY FAILURES

IMAGE SOURCE: BUSINESS TECH

South Africa's Information Regulator (IR) has confirmed that two government departments — Justice and Basic Education — hold the largest fines it has ever issued under the Protection of Personal Information Act (POPIA), at R5 million each, as the regulator moves from awareness-raising into active enforcement of the country's five-year-old data protection law. The Department of Justice's fine stems directly from a 2021 cyberattack that resulted in the loss of roughly 1,200 files and the compromise of personal information. The IR's investigation found the department had failed to implement adequate cybersecurity measures to prevent the attack in the first place. When the regulator issued an enforcement notice ordering the department to review its security monitoring and antivirus software, the department missed the 31-day deadline to respond entirely — triggering the R5 million penalty, which remains in dispute amid ongoing legal proceedings between the two parties. The Department of Basic Education's matching R5 million fine is a different kind of case: it was penalised for publishing matric (Grade 12) results in newspapers using ID numbers, which the IR has repeatedly argued fails to protect personal information. Courts have sided with the department so far, currently permitting the practice to continue, and the matter remains before the courts after several rounds of appeal. Beyond these headline cases, the IR's 31 August briefing listed other enforcement actions: the Independent Electoral Commission and Lancet Laboratories were each fined roughly R100,000 (paid), and Bloubergstrand Municipality was fined R500,000, later reduced to R250,000 by a court and currently in recovery proceedings. Looking ahead, the regulator wants sharper teeth. It's proposing amendments that would replace the current 31-day compliance grace period with immediate fines for POPIA breaches, arguing the grace period currently blunts the deterrent effect. On the PAIA side — where the only enforcement option today is lodging a criminal complaint, since there's no fines regime — the IR wants power to release withheld information directly if a compliance order goes unmet for 180 days, a response to weak reporting compliance (only 417 of 853 public entities submitted required annual reports). Werksmans Attorneys' Ahmore Burger-Smidt, Armand Swart and Hlonelwa Lutuli read this as a clear signal: the regulator is shifting from education to enforcement, and organisations — public and private alike — need proper breach response plans and section 22 notification readiness in place now, since "the Regulator's express intention to seek stronger enforcement powers means that non-compliance is likely to attract consequences in the near future." Business Tech

FAKE DSTV, FAKE TAKEALOT, REAL BANK THEFT: SOUTH AFRICANS TARGETED BY MOBILE BANKING TROJANS

IMAGE SOURCE: MY BROADBAND

Cybercriminals are exploiting the trusted names of DStv, Takealot, South African Airways, SARS and other major organisations in a sophisticated campaign targeting South Africans' smartphones and bank accounts. According to MyBroadband, the campaign uses fake websites and convincing social-engineering messages sent through SMS, WhatsApp and social media, often posing as job offers, tax refunds, ID-renewal notices or pension-verification requests. Victims are directed to fraudulent websites designed to closely resemble legitimate corporate or government platforms and are then persuaded to install malicious Android applications. Once installed, the malware can operate persistently in the background and gain access to sensitive phone functions, including SMS messages, contacts, call logs, screen activity, audio and the camera. The most serious risk is its ability to intercept one-time passwords (OTPs) sent by banks, potentially allowing criminals to bypass two-factor authentication and approve transactions themselves. More than 100 domains linked to the campaign have been identified, with the operation reportedly active since at least August 2025. The fraudulent sites are also highly localised, suggesting that criminals are tailoring their deception to different countries and languages, while rapidly abandoning compromised domains and creating new ones. The campaign demonstrates how modern banking attacks increasingly combine impersonation, malware and stolen authentication data rather than attempting to break directly into a bank's systems. My Broadband

R129 MILLION GONE: SOUTH AFRICA'S BANKING FRAUD PROBLEM GOES DIGITAL

IMAGE SOURCE: FA NEWS

South Africa's rapidly expanding digital-banking ecosystem is becoming a lucrative target for increasingly sophisticated cybercriminals, with Absa and its customers losing R129 million to fraud during the first six months of 2026. According to Absa's interim results, the losses formed part of a wider rise in operational-risk losses, which climbed from R240 million to R369 million year-on-year, with the bank attributing much of the increase to digital fraud incidents affecting its Personal and Private Banking operations. The bank specifically pointed to social engineering and malicious applications targeting customers' devices, illustrating how criminals are increasingly attacking the customer rather than attempting to breach the bank's core infrastructure directly. The risk is growing alongside digital adoption: Absa's digitally active South African customer base increased by 10% to 3.77 million, expanding the number of people conducting everyday financial transactions through online and mobile platforms. In response, Absa increased its information-technology spending by 6% to R3.8 billion, with cybersecurity, cloud and data infrastructure among the priorities, while deploying measures including in-app malware detection, advanced call screening, fraud analytics and real-time customer alerts. The scale of the losses nevertheless demonstrates the difficult security equation created by digital banking: the more financial activity moves onto smartphones and online platforms, the more opportunities criminals have to manipulate users, compromise devices and exploit trusted digital channels. Business Tech

BANKING APPS TAKEN OVER BY CYBERCRIMINALS IN SOUTH AFRICA

IMAGE SOURCE: MY BROADBAND

South African bank customers are facing a growing threat from mobile-banking account takeovers, as cybercriminals increasingly target the devices and authentication systems that sit between customers and their money. The threat is particularly concerning because attackers do not necessarily need to compromise a bank's own systems: instead, they can target the customer's phone, credentials, authentication codes and mobile-banking session to gain control of an account. Once access is obtained, criminals can potentially change account settings, intercept authentication processes and initiate unauthorised transactions while appearing to operate from the legitimate customer's device. The rise of these attacks highlights a broader shift in financial cybercrime from attacking banks directly to exploiting the digital ecosystem surrounding the customer — including smartphones, SIM cards, login credentials and authentication mechanisms. For South African users, where banking is increasingly conducted through mobile applications rather than physical branches, the smartphone has effectively become a key to financial identity, making the security of the device itself inseparable from the security of the bank account. The growing sophistication of account-takeover attacks also demonstrates why traditional protections such as passwords and one-time codes cannot be treated as a complete defence: criminals are increasingly looking for ways to compromise the wider authentication chain. My Broadband

SOUTH AFRICA'S BANKS ARE FIGHTING A CYBER WAR — AND THE THREAT IS MOVING FASTER

IMAGE SOURCE: IOL

South Africa's financial sector is facing a rapidly intensifying cyber threat environment, with digital banking fraud increasing by 86% year-on-year to almost 100,000 incidents, causing losses of approximately R1.888 billion. The warning comes as financial institutions prepare for the proposed Conduct of Financial Institutions (COFI) Bill, which is intended to strengthen operational and governance requirements but could take years to fully implement, creating a gap between regulatory reform and threats that are already hitting banks and their customers. One of the biggest emerging dangers is AI-powered social engineering: Unit 42 research cited in the report found that 36% of cyber incidents over the past year originated with social engineering, as criminals exploit personal information already available through previous data breaches and public sources to convincingly impersonate legitimate customers. South Africa's financial institutions also face a complicated technology landscape in which ageing legacy banking infrastructure sits alongside rapidly evolving fintech platforms, creating multiple potential entry points for attackers. The interconnected nature of the country's financial system adds another layer of risk: a serious breach at one institution could potentially disrupt services and have consequences beyond a single organisation. The report also warns that simply meeting regulatory requirements will not be enough, particularly where banks rely on numerous disconnected cybersecurity tools that create gaps in visibility and slow down responses. The central concern is therefore not only that attacks are increasing, but that criminals are accelerating faster than institutions can adapt — making cybersecurity resilience, rather than compliance alone, increasingly critical to protecting South Africa's financial system and public trust in digital banking. IOL

BANNED IN WASHINGTON, BOOMING IN JOHANNESBURG: WHY HIKVISION AND DAHUA STILL DOMINATE SOUTH AFRICA'S CCTV MARKET

IMAGE SOURCE: MY BROADBAND

MyBroadband's Hanno Labuschagne reports that two Chinese CCTV brands facing government-level restrictions in the US and elsewhere — Hikvision and Dahua — remain the dominant camera brands in South Africa's residential and small-business security market, with virtually no local pushback despite the same data-sharing concerns that triggered bans overseas.

Fidelity Services Group, South Africa's largest private security firm, confirmed to MyBroadband that Hikvision and Dahua are its most popular brands in that segment. Corporate affairs head Charnel Hattingh was candid about why: "They both offer exceptional value for money and are widely known and trusted for their quality," citing regular technical advances and ease of configuration as key draws for installers. Hattingh acknowledged that data-sharing concerns with the Chinese government have influenced decisions in overseas government and corporate circles, but said this has had little impact on the South African market — price, features and quality simply outweigh the privacy concerns here. Her sharper point: "Alternative, more cost-effective Far Eastern options would largely carry the same privacy concerns, but battle to compete in quality and longevity" — meaning switching brands to dodge the concern often doesn't even solve it.

The international context: The US has barred federal agencies and contractors from using Hikvision or Dahua equipment under the National Defense Authorisation Act, and the FCC has banned new equipment authorisations, effectively blocking import and sale of new models in the US. India, Australia, and UK organisations have similarly stripped these devices from sensitive or government sites. None of this is enforced in South Africa, though Hattingh noted it has become "a regular topic for conversation at the distributor level." Interestingly, the pressure pushing replacements in markets where bans do apply isn't purely regulatory — tightening cyber insurance rules and a lack of ongoing firmware support are increasingly forcing hardware swaps even among private businesses with no federal ties.

The Vumacam angle: Hikvision is also among the brands used by Vumacam, South Africa's largest public CCTV operator, which runs more than 7,000 pole-mounted street cameras nationwide. This drew US congressional scrutiny back in 2023 via a House resolution urging a review of the US–South Africa relationship. Vumacam CEO Ricky Croock pushed back firmly, telling MyBroadband the system is "not designed" for unlawful surveillance and "is not capable of ongoing surveillance of individuals" — stating all data is anonymised, there's no facial recognition, and no linkage to personal data or tracking capability. He also disputed reports of a formal partnership with Hikvision, saying Vumacam uses multiple camera brands across its network. Vumacam did not respond to MyBroadband's request for an updated brand list. My Broadband

SA TELECOM SUBSCRIPTION FRAUD SURGES, AI DEEPFAKES ON THE RISE – COMRIC

IMAGE SOURCE: CONNECTING AFRICA

South African bank customers are facing a growing threat from mobile-banking account takeovers, as cybercriminals increasingly target the devices and authentication systems that sit between customers and their money. The threat is particularly concerning because attackers do not necessarily need to compromise a bank's own systems: instead, they can target the customer's phone, credentials, authentication codes and mobile-banking session to gain control of an account. Once access is obtained, criminals can potentially change account settings, intercept authentication processes and initiate unauthorised transactions while appearing to operate from the legitimate customer's device. The rise of these attacks highlights a broader shift in financial cybercrime from attacking banks directly to exploiting the digital ecosystem surrounding the customer — including smartphones, SIM cards, login credentials and authentication mechanisms. For South African users, where banking is increasingly conducted through mobile applications rather than physical branches, the smartphone has effectively become a key to financial identity, making the security of the device itself inseparable from the security of the bank account. The growing sophistication of account-takeover attacks also demonstrates why traditional protections such as passwords and one-time codes cannot be treated as a complete defence: criminals are increasingly looking for ways to compromise the wider authentication chain. Connecting Africa

77% HIT RATE: NEW KASPERSKY DATA SHOWS SOUTH AFRICAN SMBS ARE NOW GETTING THE SAME PLAYBOOK AS BIG ENTERPRISES — JUST WITHOUT THE BUDGET TO FIGHT BACK

IMAGE SOURCE: CAPE BUSINESS NEWS

A new global Kaspersky survey of IT security specialists across 18 countries — including South Africa — finds that only 23% of South African SMBs with 100-499 employees avoided a cybersecurity incident in the past year, meaning roughly 77% were hit at least once (slightly better than the 14% global avoidance rate, but still a striking figure). Kaspersky's core argument: the idea that small and mid-sized businesses can "fly under the radar" is now obsolete, since attackers are deploying the same methods against smaller companies that they use against large enterprises, driven by the falling cost of launching attacks and SMBs' accelerating digitalisation.

What's actually hitting South African SMBs: On average, organisations experienced three different types of security incidents over the past year. Locally, the leading categories were social engineering (23% of organisations), followed by phishing, weak or stolen credentials, and business email compromise (BEC) — each affecting 18% — with software vulnerability exploitation close behind at 15%. Globally, the picture was similar in shape but different in specifics: phishing (20%), software vulnerability exploitation (17%), and external remote access (16%) topped the list, while more severe attack types like zero-days and trusted-relationship attacks, though rarer, still hit 8% of organisations each. Notably, mass malware, ransomware, BEC, and AI-related vulnerability exploits skewed more toward large enterprises than SMBs.

Why South African SMBs are exposed — and it's mostly structural, not just human error: Locally, outdated software or hardware and shadow IT (unauthorised apps and services) tied as the top risk factors, each named by 30% of respondents, followed by a lack of security awareness among employees (28%). Rounding out the list: high workload on IT/security departments, insufficient security policies (like infrequent password changes or backups), and a lack of regular risk assessments — each cited by 25%. Globally, the picture skewed slightly more toward people problems: a lack of expertise among IT security staff (24%) and low security awareness among non-IT employees (23%) topped the list worldwide.

The budget response: South African organisations are already reacting — 32% have expanded their IT/security teams, 35% have funded new security awareness training for staff, and 24% have invested in advanced tools like XDR, NDR, and SIEM. Kaspersky's Ilya Markelov frames the core tension bluntly: growing companies are "held back by budget constraints and the global InfoSec talent shortage," so effective tools for this segment need to deliver more protection without demanding scarce, expensive expertise to run.

Kaspersky's practical recommendations (worth noting this is vendor guidance, paired with their own product lineup): enforce strict access controls with prompt offboarding, automate daily backups against ransomware, run continuous security-awareness training that specifically covers deepfakes and vishing, and require IT approval for any new software to curb shadow IT.
Cape Business News

RANSOMWARE'S SIX-STEP ATTACK: HOW SOUTH AFRICAN BUSINESSES GET HELD HOSTAGE

IMAGE SOURCE: LOOPHOLD

South Africa is facing the highest volume of ransomware detections in Africa, with 17,849 detections recorded in a single year, according to figures cited from INTERPOL's 2025 Africa Cyberthreat Assessment. The threat is also evolving beyond simply locking companies out of their files: attackers increasingly use "double extortion", first stealing sensitive information and then encrypting systems, allowing them to threaten both operational paralysis and the public release of customer or corporate data. According to Loophold, a typical attack unfolds over several days, beginning with phishing, stolen credentials, exposed remote-access services or unpatched internet-facing systems; attackers then establish persistence, escalate their privileges, map the victim's network, identify valuable financial and customer information, exfiltrate that data and deliberately target backups before finally triggering widespread encryption. This means the ransomware encryption itself is often the final stage of an intrusion that may already have been underway for days. The article argues that this timeline creates multiple opportunities for organisations to detect and stop attackers before the damage becomes widespread, particularly through stronger monitoring, multi-factor authentication, network segmentation, patching and properly isolated, immutable backups. The financial stakes are enormous: Loophold cites INTERPOL estimates that cybercrime caused around $3 billion in financial losses across Africa between 2019 and 2025, while South Africa's relatively digitised economy and concentration of valuable corporate and personal data make it an especially attractive target. The consequences also extend beyond business disruption because stolen personal information can trigger obligations under South Africa's Protection of Personal Information Act (POPIA), including notification requirements when personal information has been accessed or acquired without authorisation. The article's central message is therefore that ransomware is not simply a malware problem — it is a failure-of-resilience problem, where the outcome of an attack can depend on decisions made months or years earlier about backups, access controls, monitoring and incident response. Loophold

SOUTH AFRICA'S NEW CYBERCRIME WEAPON: THE ART OF PERSUASION

IMAGE SOURCE: TECH CENTRAL

South Africa's fraud problem is increasingly being driven not by criminals breaking into bank systems, but by criminals persuading legitimate users to hand over access themselves — a shift that is being accelerated by artificial intelligence. TechCentral, drawing on data from Flashpoint, Interpol and the South African Banking Risk Information Centre (Sabric), reports that cybercriminals are using AI to automate everything from identifying stolen credentials to launching highly targeted fraud campaigns. Flashpoint recorded more than 22 million posts in the first six months of 2026 involving AI tools for criminal use, alongside more than 7.4 million compromised hosts from which attackers extracted 1.7 billion credentials and identity data points. AI-powered systems can rapidly test stolen usernames, passwords and session cookies across corporate VPNs, cloud platforms and other services, meaning attackers can identify working credentials at a scale that would previously have required substantial human effort. But the most significant threat for South Africa is social engineering: Sabric recorded R2.4 billion in digital-banking fraud claims across 110,074 investigations in 2025, up 29.2% from the previous year, with banking-app fraud accounting for 88.6% of investigations and 70.5% of claim value. Crucially, Sabric says many of these incidents did not involve a breach of the bank itself; instead, criminals impersonated trusted organisations, manufactured urgency and guided victims through transactions in real time. The wider threat is compounded by South Africa's exposure to ransomware, phishing and DDoS attacks, while telecommunications fraud is estimated to cost the country R5.3 billion annually. The result is a changing cybersecurity battlefield in which criminals increasingly exploit trust, identity and human behaviour rather than technical vulnerabilities alone. Tech Central

SOUTH AFRICA'S DATA CENTRE BOOM: BUILDING THE CLOUD BEFORE WRITING THE RULES

IMAGE SOURCE: DAILY MAVERICK

South Africa is rapidly positioning itself as a major African hub for data centres and AI infrastructure, but the country's digital infrastructure expansion is moving faster than the governance systems needed to oversee it. A major warning comes from Cape Town, where two proposed hyperscale data-centre complexes would require approximately 174 megawatts of electricity — enough to power around 130,000 homes — while potentially consuming billions of litres of water annually through cooling systems. The deeper concern, however, is not simply the environmental footprint: data centres are becoming strategic digital infrastructure, controlling where enormous quantities of data are stored, processed and routed, yet South Africa currently lacks a coherent national framework that treats them as critical infrastructure rather than ordinary commercial developments. The Daily Maverick argues that existing regulations divide responsibility between environmental, water, electricity, planning and data-protection laws, meaning no single regulatory system considers the full impact of a data centre as an interconnected digital, economic and strategic asset. This governance gap is particularly significant as global technology companies expand their cloud and AI infrastructure in South Africa, potentially giving foreign firms substantial influence over the physical systems underpinning the country's digital economy. The article therefore raises a broader digital-sovereignty concern: South Africa could end up hosting increasingly important foreign-controlled computing infrastructure without having sufficient visibility into its resource consumption, strategic importance, ownership or long-term implications for national digital resilience. With data centres becoming essential to AI, cloud computing, financial services and government systems, the question is no longer simply whether South Africa needs more of them, but who controls this infrastructure, what safeguards govern it and whether the country is building digital capacity without first establishing the rules needed to protect its resources and sovereignty. Daily Maverick

THE PASSWORD ISN'T THE KEY ANYMORE: SOUTH AFRICANS FACE A COOKIE-HIJACKING THREAT

IMAGE SOURCE: BUSINESS TECH

South African internet users are being warned about a growing cybercrime technique in which criminals steal browser cookies to hijack already-authenticated online accounts without needing the victim's password. A recent NordVPN study found more than 263 million browser cookies associated with South African users in infostealer datasets circulating online, placing South Africa 30th globally for the volume of stolen cookies identified. The most valuable targets are "remember-me" cookies, which allow services to recognise a user and keep them logged in; if criminals obtain a valid session cookie, they can potentially impersonate the user and gain access to services such as Netflix, YouTube, Reddit and email accounts. The technique, known as session hijacking, is typically enabled by infostealer malware that criminals spread through social engineering, including malicious websites and phishing links that trick users into downloading infected software. The FBI has warned that stolen login cookies can allow criminals to bypass the normal authentication process, effectively turning a previously trusted browser session into a digital key. This means that even a strong password may not be enough to protect an account once an attacker has stolen an active authentication token. The threat highlights an increasingly important shift in cybersecurity: criminals are not always trying to crack passwords — they can instead steal the digital evidence that proves a user has already logged in. Business Tech

JOURNALISTS ARE BECOMING PRIME TARGETS IN GHANA'S DIGITAL BATTLEFIELD

IMAGE SOURCE: BUSINESS GHANA

Journalists in Ghana are facing a growing range of digital threats that can compromise both their work and personal security, according to a warning from a cybersecurity expert reported by BusinessGhana. The concern is particularly serious because journalists routinely handle sensitive sources, confidential documents and politically sensitive information, making their phones, computers, email accounts and social-media profiles attractive targets for attackers seeking to monitor communications or disrupt reporting. The expert warned that journalists need to treat cybersecurity as an essential part of their professional practice rather than an optional technical concern, particularly as attackers increasingly exploit weaknesses in digital accounts and communications. The warning comes as journalism across Africa becomes increasingly dependent on digital platforms, expanding the number of potential entry points through which reporters, editors and their sources can be targeted. A compromised journalist's account can do more than expose personal information: it can potentially reveal confidential contacts, compromise sensitive reporting material and place sources at risk. The Ghana warning therefore highlights a broader issue for African media organisations: protecting journalism now requires protecting the digital infrastructure behind it, from journalists' devices and accounts to the confidential information entrusted to them. Business Ghana

QR CODES BECOME KENYA'S NEW PHISHING TRAP

IMAGE SOURCE: TECH TRENDS

Kenyan organisations are facing a surge in low-tech cyberattacks that exploit familiar security weaknesses, with the latest ESET Threat Report highlighting a particularly sharp rise in QR-code phishing, or "quishing". ESET telemetry recorded a 145% increase in quishing activity in Kenya between the second half of 2025 and the first half of 2026, as attackers increasingly use QR codes to redirect victims to malicious websites—often shifting the attack onto smartphones, where the scanning process can occur outside an organisation's normal security controls. The threat is part of a broader pattern: globally, around 11% of detected phishing emails during the reporting period contained QR codes, while malicious email attachments remained a major route for delivering malware, with scripts accounting for 46.2% of malicious attachments, followed by Microsoft Office documents at 14.4%, PDFs at 11.9% and archives at 9.7%. Kenya also recorded more than a twofold increase in attempts to exploit CVE-2017-0199, an old Microsoft Office vulnerability that can allow malicious code to execute when a victim opens a specially crafted document. Meanwhile, Aotera, an infostealer and malware dropper, became Kenya's fourth most-detected malware family and has been linked to the delivery of other malware including AgentTesla, Formbook, PureLogs, PhantomStealer and Vidar. ESET also warned that some organisations have even paid suspected ransomware demands without first confirming whether their systems had actually been encrypted by genuine ransomware. The report's central warning is therefore less about sophisticated, futuristic hacking than about attackers continuing to exploit basic weaknesses that organisations already know how to fix—from unpatched software and exposed remote-access systems to weak passwords and increasingly deceptive phishing techniques. Tech Trends

AI IS SUPERCHARGING AFRICA'S CYBERCRIME ECONOMY

IMAGE SOURCE: STREAMLINE FEED

Artificial intelligence is rapidly transforming cybercrime across Africa from a largely manual operation into a faster, more automated and increasingly industrialised criminal economy, according to Streamline Feed's report drawing on the 2026 African Cyberthreat Assessment Report. The report says 55% of reported cybercrimes across the continent now involve some form of AI, while estimated cybercrime losses have risen from $192 million in 2024 to about $484 million in early 2026. Criminal groups are using generative AI to produce highly personalised phishing messages, clone voices, generate synthetic identities and modify malicious code, allowing relatively decentralised networks to conduct attacks at a scale that can overwhelm traditional investigations. The report highlights the emergence of AI-assisted ransomware capable of adapting its code during deployment, alongside synthetic documents and biometric profiles being used to bypass Know Your Customer (KYC) checks and create fraudulent accounts for money laundering. It also identifies regional patterns: West African groups are heavily involved in business-email compromise and corporate fraud, Southern African actors increasingly target government and healthcare infrastructure with ransomware, while East African criminals exploit the region's widespread mobile-money ecosystem using AI-generated voice impersonation. The problem is compounded by a widening institutional gap: cybercriminal networks can access inexpensive cloud-based AI tools and operate across borders, while many African law-enforcement agencies remain constrained by fragmented legal systems, limited cyber-forensics capacity and jurisdictional barriers. The report warns that this imbalance could damage confidence in Africa's rapidly growing fintech and technology sectors, particularly if investors conclude that governments cannot adequately protect digital infrastructure. Streamline feed

AI IS OUTRUNNING AFRICA'S CYBER DEFENDERS

IMAGE SOURCE: BUSINESS INSIDER

Artificial intelligence has become a major force in Africa's cybercrime economy, but the continent's law-enforcement agencies are struggling to develop the skills and infrastructure needed to keep pace: according to INTERPOL's African Cyberthreat Assessment Report 2026, AI was involved in 55% of cybercrime cases observed across Africa in 2025, yet only 8% of intelligence analysts had advanced expertise in investigating AI-driven attacks. The assessment, based on responses from 36 African countries, found that AI was used frequently in 8% of cases and occasionally in another 47%, enabling criminals to automate phishing, imitate corporate executives, generate convincing fake voices and videos, create synthetic identities and develop malicious software. Deepfake incidents reportedly increased sevenfold between the second and fourth quarters of 2024, while reported cybercrime losses more than doubled from $192 million in 2024 to $484 million in 2025; INTERPOL estimates the broader economic damage was at least $5 billion. The defensive gap is equally striking: only 22% of digital-forensics units surveyed had working knowledge of AI-driven threats, just 33% of agencies used AI for threat detection, and approximately 94% lacked adequate digital-forensics tools. The problem extends beyond technology to the structure of cybercrime itself: 72% of surveyed countries reported organised scam centres, while 89% identified cross-border cooperation as a major obstacle to investigations. With criminals able to deploy AI across borders almost instantly while investigators remain constrained by shortages of specialist personnel, forensic equipment and slow information-sharing mechanisms, INTERPOL warns that cybercrime is increasingly becoming an industrialised, borderless ecosystem operating at machine speed. Business Insider

YOUR DIGITAL IDENTITY IS BECOMING YOUR NEW PASSPORT — BUT WHO CONTROLS IT?

IMAGE SOURCE: THE GUARDIAN

Across Africa, the rapid shift from physical identification to digital identities and biometric systems is creating new opportunities for governments, banks and businesses to deliver services, but it is also creating a growing privacy and cybersecurity challenge: the more everyday activities become tied to a single digital identity, the more valuable that identity becomes to both legitimate institutions and malicious actors. The Guardian Nigeria argues that digital identity is increasingly being used to access banking, healthcare, government services, telecommunications and other essential systems, meaning identity databases can contain highly sensitive information about an individual and become attractive targets for cybercriminals, fraudsters and unauthorised surveillance. Unlike a password, biometric information such as fingerprints or facial characteristics cannot simply be changed after a breach, making the protection of identity databases particularly important. The article highlights the need for African countries to develop strong safeguards around how identity data is collected, stored, shared and accessed, particularly as governments expand national digital-ID programmes and integrate databases across public and private services. Without effective data-protection laws, independent oversight and robust cybersecurity controls, systems designed to make identification easier could instead create centralised repositories of personal information that are vulnerable to misuse or mass exposure. The issue is therefore bigger than convenience: digital identity is becoming part of the infrastructure through which people participate in modern African economies, and weaknesses in that infrastructure could expose citizens to identity theft, fraud, profiling or loss of privacy on a much larger scale. The Guardian

AFRICA'S CYBER-ESPIONAGE SURGE: SPIES ARE COMING FOR CORPORATE NETWORKS

IMAGE SOURCE: OMNY FM

Cyber-espionage is intensifying across Africa, with new Kaspersky research showing sharp increases in the malware commonly used to steal corporate information, establish persistent access to networks and prepare the ground for further targeted attacks. Over the past year, spyware detections targeting African organisations increased by 16%, while password-stealer attacks surged by 51% and backdoor detections rose by 23%, according to Kaspersky. The significance is that these are not simply opportunistic malware infections: spyware can be used to monitor activity and gather sensitive information, password stealers can provide attackers with credentials that open the door to corporate accounts and systems, while backdoors can give attackers continued access after an initial compromise. Kaspersky researchers say these tools are increasingly being used as part of broader intrusion campaigns against businesses, making compromised credentials and infected devices potential entry points into larger organisational networks. The trend comes as African businesses and institutions rapidly digitise their operations, expanding the amount of commercially and strategically valuable information stored online while creating more opportunities for attackers to establish a foothold. Kaspersky's findings therefore point to a shift in the African threat landscape in which cyber-espionage is not only about stealing data after an attack, but about quietly gaining and maintaining access to organisations for future operations. Omny.FM

YOUR PHONE IS WATCHING YOU: AFRICA'S MOST POPULAR SMARTPHONES UNDER THE MICROSCOPE

IMAGE SOURCE: TECH CENTRAL

Research has uncovered a hidden tracking system built into millions of Tecno, Infinix and Itel smartphones — brands owned by Chinese manufacturer Transsion that accounted for roughly 48% of smartphone shipments in Africa in 2025, representing more than 40 million devices. An independent security researcher working with NowSecure decrypted the data transmitted by a Tecno Spark 40 and found that Transsion's built-in Athena data-collection system and oneID cross-app tracker can report a user's precise GPS location, nearby mobile masts and signal strength, which applications are being used, how much data individual apps consume and even when an application activates the phone's camera — although the system does not appear to capture what the camera actually records. The collected information is linked to around 14 permanent device identifiers that users cannot reset, allowing activity to be associated with the same handset throughout its lifespan. Unlike ordinary Android applications, which are restricted by the operating system's sandbox, this tracking software operates as a privileged system component connected to core functions including Settings, the system interface and camera services, meaning users cannot simply uninstall or disable it without potentially making the device unusable. The research also found that the software can read the clipboard, identify installed applications and interfere with other apps. The findings raise an additional privacy concern because the tracking traffic is transmitted automatically over the phone's internet connection, potentially consuming users' prepaid mobile data without their knowledge. While the research found the data reaching Alibaba Cloud infrastructure in Frankfurt rather than directly observing transfers to servers in China, the system's ownership, references to external analytics platforms and the scale of information being collected have intensified questions about who ultimately controls African users' smartphone data — and how much surveillance is happening inside devices that millions of people simply assume are private. Techcentral

YOUR EXPIRED VISA CARD COULD BE 'ZOMBIFIED' TO MAKE CONTACTLESS PAYMENTS

IMAGE SOURCE: WIRED

An expired Visa card may not be as useless as consumers think: researchers from the University of Massachusetts Amherst have demonstrated a technique that can potentially "reanimate" expired cards and use them for unauthorised contactless payments. Presented at the USENIX Security Conference, the research found a weakness in the authentication chain used for contactless transactions that can allow an expired Visa card's payment data to be relayed through a man-in-the-middle setup involving two phones. The problem stems from the way expiry checks are handled: rather than the card network uniformly rejecting an expired card, authentication can ultimately depend on how individual banks implement the relevant cryptographic checks. Researchers found that Visa's system could allow some expired cards to pass this stage, with the issuing bank then deciding whether to block the transaction. While some banks rejected the fraudulent transactions, others could allow them to proceed, meaning an old card that has been discarded could potentially remain linked to an active bank account and be abused at contactless payment terminals. The discovery exposes an unexpected weakness in the increasingly complex chain connecting physical cards, mobile devices, payment networks and banks, showing that even a card that has technically expired can retain security significance if it is not properly deactivated. Wired

APPLE'S SPYWARE WARNING: THE NOTIFICATION THAT COULD EXPOSE A HIDDEN ATTACK

IMAGE SOURCE: TECH CENTRAL

Apple has issued a new wave of spyware threat notifications to users in 110 countries, warning that their iPhones, iPads or Macs may have been deliberately targeted by sophisticated "mercenary spyware" typically associated with government surveillance operations. Apple says it has now notified users in more than 150 countries since beginning the alerts, with the latest warnings appearing directly on users' lock screens as well as through email and Apple account notifications. The alerts are significant because receiving one does not necessarily mean the device was successfully compromised, but it indicates that Apple has detected activity suggesting the person may have been specifically targeted and should take the warning seriously. Apple now directs recipients towards security guidance and its Lockdown Mode, a protection designed to restrict certain device functions and make highly sophisticated spyware attacks harder to execute; the company says it has not seen a confirmed case of a device being successfully hacked while Lockdown Mode was enabled. Researchers at Citizen Lab describe the notifications as an important early-warning mechanism because a single alert can trigger investigations that uncover much wider surveillance campaigns, including cases where journalists, activists, civil-society figures or political actors have been targeted. According to researcher John Scott-Railton, Apple's alerts have previously helped expose major spyware-abuse scandals, including investigations into surveillance during Poland's election period. The development highlights a growing reality of commercial spyware: some of the most dangerous cyberattacks are not random attacks aimed at stealing money, but highly targeted operations designed to secretly compromise the devices of specific people. TechCrunch

YOUR BANKING APP ISN'T SAFE: ANDROID MALWARE LEARNS TO CONTROL THE PHONE

IMAGE SOURCE: THE HACKER NEWS

Two Android banking trojans are expanding their ability to take over victims' devices and perform fraudulent transactions from inside legitimate banking applications, highlighting a growing shift from stealing banking credentials to directly manipulating the device itself. The updated ToxicPanda 2.0 now contains 167 remote commandsand has expanded its targeting from 16 banking applications to 349 financial institutions across 16 countries, while using Android accessibility features to extract information displayed on-screen, capture PINs through fake overlays and manipulate device settings. Researchers also found that the malware can abuse accessibility controls to activate Developer Options and wireless debugging, potentially giving attackers deeper access to compromised devices, while fake full-screen "system update" screens can conceal malicious activity from the victim. At the same time, the GoldDigger banking trojan has been observed in a major campaign affecting South Africa and the United Kingdom, with attackers disguising malicious applications as airline companies and shopping retailers. Once installed, GoldDigger can abuse Android accessibility permissions to simulate legitimate user interactions inside banking apps — including entering information, clicking buttons and performing gestures — while also providing attackers with real-time screen access and the ability to capture credentials. Researchers say the malware can additionally collect SMS messages and contacts, access location information, record audio and video, and communicate with its operators through persistent WebSocket connections. The significance of these campaigns is that attackers are increasingly bypassing the traditional model of stealing a username and password: instead, they are attempting to make the victim's own smartphone perform the banking activity on their behalf. The Hacker News

HACKERS HAVE FOUND A NEW DASHBOARD: YOUR CAR

IMAGE SOURCE: TECH CENTRAL

Cybersecurity researchers have identified what Kaspersky describes as the first documented malware infection chain specifically designed to compromise Android-based vehicle infotainment systems, signalling that the attack surface of connected cars is expanding beyond traditional computers and smartphones. The campaign targets Android head units manufactured by DoFun, whose systems use a legitimate application called TWCore to manage software updates. Attackers appear to have abused this trusted update mechanism to install JarService, a malicious dropper that secretly decrypts and launches additional malware without requiring any interaction from the driver. The subsequent malware can collect technical information including the vehicle's model, screen resolution, MAC address and connected Wi-Fi network, communicate with an attacker-controlled server and download additional malicious components. One component, a "clicker", is designed to generate fraudulent advertising activity, while another known as zhima can turn infected head units into nodes in a proxy botnet, allowing third parties to route internet traffic through compromised vehicles. Kaspersky links the activity to the MoYu Group, a threat actor associated with the wider BadBox ecosystem, which has previously compromised Android-based devices such as streaming boxes. The campaign is particularly significant because modern vehicle head units are often permanently connected to the internet through SIM cards or other connectivity, while manufacturers frequently use Android because of its flexibility and extensive app ecosystem. Although the malware identified in this campaign is focused on fraud and botnet activity rather than demonstrated control of steering, braking or other critical driving functions, the discovery shows how vehicles are becoming another category of connected computing device that criminals can recruit into their infrastructure. DoFun was notified of the issue and has addressed the vulnerability across most affected devices. Digitalshield

META FINED $567 MILLION: WHEN SOCIAL MEDIA BECOMES A CHILD-SAFETY THREAT

IMAGE SOURCE: THE HACKER NEWS

Meta has been ordered by a New Mexico judge to pay an additional $567 million over allegations that its platforms exposed children to harmful content and dangerous contacts, bringing the total penalties in the case to $942 million and marking the largest child-safety fine imposed on the company. The ruling goes beyond simply penalising individual pieces of harmful content: Judge Bryan Biedscheid classified Meta as a "public nuisance", comparing its platforms to a factory whose advertising and content are the products while the psychological harm and sexual exploitation of children are the resulting "pollution". At the centre of the case were Meta's recommendation algorithms, which the court found had repeatedly steered young users towards harmful content and contacts, raising questions about whether the systems designed to maximise engagement can themselves become mechanisms for exposing children to risk. The court has ordered Meta to establish a fund, with $420 million earmarked for clinical and behavioural-health programmes, alongside measures requiring that adults cannot message underage users, accounts belonging to under-18s cannot be recommended to adults, minors cannot send or receive nudity, and adult users involved in child sexual exploitation face a one-strike policy. Meta must also remove "like" counts for users under 18, restrict overnight and school-hour push notifications, and impose a 90-hour monthly usage limit across Instagram and Facebook. The case is part of a much wider legal reckoning: Meta faces thousands of similar lawsuits in the US, while governments in the UK and EU are pursuing stronger protections for children online. BBC

THE MALWARE THAT BUILDS ITSELF: SOURTRADE TURNS YOUR BROWSER INTO AN ATTACK MACHINE

IMAGE SOURCE: CYBER SECURITY NEWS

A sophisticated malvertising campaign known as SourTrade is turning victims' web browsers into an unexpected part of the malware delivery system, targeting cryptocurrency users across Asia-Pacific, Latin America, Africa, Australia and Great Britain with fake advertisements and convincing copies of platforms including TradingView, Solana and Luno. Active since late 2024, the campaign uses a technique that makes it particularly difficult for conventional security tools to detect: rather than downloading a completed malicious Windows executable, SourTrade sends the victim's browser the individual components and instructions needed to assemble the malware locally. Its malicious webpages use browser technologies including ServiceWorkers and SharedWorkers, alongside a legitimate Bun runtime, encrypted data and session-specific values, to construct a new executable for each victim or session. This means that two people exposed to the same campaign can receive files with different cryptographic hashes, undermining one of the most common ways security systems identify known malware. The campaign also uses cloaking, screening visitors and presenting harmless or blank pages to researchers and automated security systems while showing selected targets the fraudulent trading pages. The result is a significant evolution in malvertising: the browser is no longer merely the place where a victim encounters a malicious advertisement — it becomes part of the machinery that creates the malware itself. For cryptocurrency users, the campaign demonstrates why sponsored search results and advertisements can become a dangerous entry point, particularly when they imitate trusted financial and trading brands. Cyber Security News

GOVERNMENTS UNDER SIEGE: RANSOMWARE HITS 187 PUBLIC-SECTOR TARGETS IN SIX MONTHS

IMAGE SOURCE: INDUSTRIAL CYBER

Government agencies around the world faced a sharp rise in ransomware attacks during the first half of 2026, with 187 incidents recorded between January and June — a 13% increase from the 165 attacks reported in the second half of 2025. Of those incidents, 89 were confirmed by the affected organisations, exposing at least 179,000 records, meaning governments were targeted by roughly one ransomware attack every day. The United States recorded the highest number of attacks with 58, followed by Germany with nine, France with eight and South Africa with six, highlighting the continued vulnerability of public institutions across the continent. The ransomware landscape is also shifting: the relatively new Gentlemen group emerged as the most active threat against government organisations, claiming 22 attacks in six months — a dramatic increase from just one reported attack in the previous six-month period — followed by Qilin with 21 and LockBit with 14. The financial demands varied considerably, with the median ransom falling from $500,000 in late 2025 to $100,000 in the first half of 2026, although some demands reached millions: South Africa's Land and Agricultural Development Bank refused a $3.1 million ransom following a January attack and restored its systems by April. Other incidents demonstrate the potentially devastating operational consequences, including a German municipal transport company that needed 11 weeks to recover, while a US government breach resulted in nearly 158,000 people being notified that their data may have been compromised. Researchers warn that governments remain particularly attractive targets because ransomware can simultaneously disrupt essential public services and threaten vast stores of sensitive citizen information, with basic weaknesses such as unpatched systems continuing to provide attackers with opportunities to penetrate government networks. Industrial Cyber

THE MAC SECURITY MYTH IS CRACKING: MORE THREATS, LESS PROTECTION

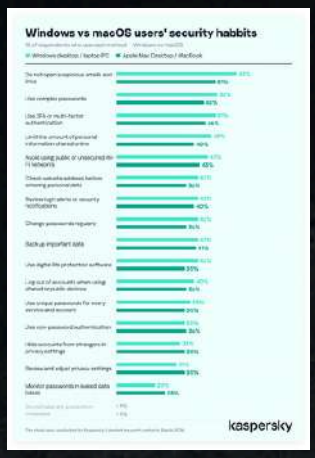


IMAGE SOURCE: KASPERSKY

The long-standing perception that Macs are inherently safer than Windows PCs is becoming increasingly difficult to defend, according to a 2026 Kaspersky survey of 7,200 people across 18 countries, including South Africa. The survey found that 12% of macOS users reported experiencing malware infections during the previous year, compared with 9% of Windows users, while macOS users also reported higher rates of phishing (12% vs 9%), scams and investment fraud (16% vs 13%), privacy violations (11% vs 8%) and personal-data theft (12% vs 7%). Yet despite reporting more incidents across several categories, Mac users were less likely to use dedicated security software: only 35% said they had installed digital-life-protection software, compared with 42% of Windows users. The behavioural gap extends further: only 51% of macOS users said they avoid opening suspicious emails or links, compared with 62% of Windows users. Kaspersky argues that the idea of macOS being a low-value target because of its smaller user base is increasingly outdated, as attackers can exploit users through phishing, supply-chain attacks and malware specifically designed for Apple systems. The survey does not establish that macOS is objectively less secure than Windows, but it exposes a more important cybersecurity problem: confidence in the platform's security may itself be encouraging weaker security behaviour, leaving users less prepared as attackers increasingly target people rather than simply targeting operating systems. Kaspersky

STARLAND RAT: TRUSTED SOFTWARE TURNS INTO A BACKDOOR

IMAGE SOURCE: CYBER MAGAZINE

A newly uncovered malware campaign is disguising Starland RAT, a Python-based remote access trojan, inside trojanised copies of legitimate software including MobaXterm, Cisco WebEx, Zoom, FACEIT and DBeaver Community Edition, allowing attackers to exploit the trust users place in familiar applications. Cisco Talos attributes the campaign to UAT-11795, a Russian-speaking, financially motivated threat actor active since at least June 2025, with infections concentrated in the United States and additional cases reported in Germany, Romania and Venezuela. Once installed, Starland RAT can maintain long-term access to compromised computers while stealing credentials and cryptocurrency-wallet information. The malware is paired with a second component called the WLDR agent, a PowerShell-based command-and-control implant that operates in memory rather than writing files to disk, making conventional detection more difficult. The attackers have also built resilience into their infrastructure: they use multiple domains, Telegram bots to receive information from infected machines, and a fallback command-and-control mechanism hidden inside a Polygon blockchain smart contract, allowing the malware to retrieve alternative server information if its main infrastructure is disrupted. Particularly concerning is the campaign's use of apparently legitimate software and deceptive social-engineering techniques, demonstrating how attackers can bypass traditional security assumptions without exploiting a software vulnerability at all — instead, they exploit the victim's trust in the software they are installing. Cyber Magazine

BEFORE THE ENCRYPTION: THE GENTLEMEN RANSOMWARE GANG IS TAKING CONTROL FIRST

IMAGE SOURCE: DIGITAL SHIELD

The Gentlemen ransomware group is evolving beyond the traditional "break in, encrypt files and demand a ransom" model, with researchers from Kaspersky's Global Research and Analysis Team identifying a previously unknown Go-based backdoor that attackers deploy before launching the ransomware itself. The malware gives the attackers a foothold inside compromised networks from which they can collect information about devices and networks, communicate with their command-and-control infrastructure and remotely execute commands, allowing them to study and prepare the environment before beginning the destructive phase of the attack. Researchers also found evidence that some compromised systems had been accessed long before the ransomware infection, raising the possibility that Gentlemen affiliates are purchasing access from Initial Access Brokers rather than gaining entry themselves. The group, believed to have emerged in mid-2025 and operating under a Ransomware-as-a-Service (RaaS) model, has targeted organisations across manufacturing, technology, healthcare, finance, construction and logistics, while continuing to develop its toolkit. Researchers have additionally identified a new C-based Windows ransomware variant, suggesting the group is actively refining its malware, and observed an attempt to remove security software from a compromised system — an effort that was detected and blocked. The significance of the campaign is that ransomware is increasingly becoming a multi-stage intrusion rather than a single attack: by gaining control, gathering intelligence and positioning themselves inside a network before encryption begins, attackers can better understand their target and potentially make the eventual ransomware operation more effective. Digital shield

FAKE CLAUDE, REAL MALWARE: HOW A SEARCH AD TURNED AI HYPE INTO A CYBER TRAP

IMAGE SOURCE: INTERNATIONAL BUSINESS TIMES

A sophisticated malvertising campaign dubbed "FakeAgent" has weaponised the popularity of AI assistants, using sponsored Bing search results to trick users into downloading a fake desktop version of Anthropic's Claude that instead installed the SectopRAT remote-access trojan. According to researchers at Huntress, the campaign compromised at least 29 organisations between 21 and 22 July 2026, while a malicious Claude Artifact hosted on the legitimate Claude.ai domain was downloaded approximately 7,100 times before being removed. Victims who followed the fraudulent download chain were directed to an installer called "ClaudeDesktop.exe", which abused a legitimate JetBrains Chromium component to sideload a malicious DLL and deploy SectopRAT; a separate executable, "DockerDesktop.exe," then created a scheduled task to maintain persistence on the infected machine. SectopRAT can steal passwords, browser credentials, cookies, credit-card information, files, FTP credentials and data from messaging applications such as Discord and Telegram, while its hidden virtual-network-computing capability gives attackers the ability to interact remotely with compromised systems. The campaign also incorporated multiple anti-analysis techniques, including virtual-machine detection and hardware checks, making the malware harder for researchers to examine. What makes the operation particularly striking is that the attackers did not need to compromise a victim by exploiting Claude itself: they exploited trust in the Claude brand, trust in search advertising and even a legitimate Claude.ai domain to construct a convincing delivery chain. The incident is another warning that a familiar logo or a top search result is no guarantee that the software behind the download is legitimate — particularly as cybercriminals increasingly use the explosive popularity of AI tools as bait. International Business Times

CYBERCRIMINALS AREN'T HACKING SYSTEMS — THEY'RE HACKING TRUST

IMAGE SOURCE: TECH CENTRAL

Cybercriminals are increasingly abandoning the obvious signs of cyberattacks — suspicious emails, malicious files and unfamiliar websites — and instead hijacking the digital experiences people already trust. A Gen Digital threat report highlighted by TechCentral recorded 114.2 million e-commerce scam attacks blocked in the first half of 2026, alongside 20.3 million tech-support scam attacks, while government-impersonation scams surged by 387% and family-impersonation scams by more than 454%. The report also identified more than 304 million scam-related advertising impressions across the EU and UK in less than one month and approximately 1.9 billion tracking attempts blocked globally during the first six months of the year. The shift is significant because attackers are increasingly embedding themselves in legitimate-looking environments: fake online shops mimic trusted retailers, fraudulent support requests imitate familiar companies, compromised accounts communicate through legitimate messaging platforms, and AI-generated text, images and videos can make impersonation considerably more convincing. Rather than attempting to defeat security software head-on, criminals are manipulating the context surrounding the user so that a malicious interaction appears ordinary. For African businesses, the implication is particularly important: cybersecurity can no longer focus solely on detecting malware at the endpoint. Organisations increasingly need protection spanning devices, applications, identities, data, software updates, online interactions and user behaviour, because the next attack may not look like an attack at all — it may look exactly like something the victim already knows and trusts. TechCentral

GOODBYE PASSWORDS? GOOGLE WANTS YOUR FACE TO BE THE KEY

IMAGE SOURCE: MY BROADBAND

Google is pushing the passwordless future a step further with a new selfie-video login feature that allows users to authenticate their Google Accounts by scanning their face instead of entering a password. Users enrol by recording a short video while following guided head movements, creating a reference that Google can later compare against a new selfie when they need to regain access to their account. The system is designed to check that the person is physically present by requiring movement and uses additional security measures, including technology intended to detect deepfake images and videos, to make impersonation more difficult. Google says the selfie video is encrypted while stored, collected with the user's consent, used specifically for sign-in unless the user chooses otherwise, and can be deleted from their account. The move is part of Google's broader shift towards passkeys and other passwordless authentication methods, driven by the weakness of passwords, which can be guessed, reused or exposed through data breaches. But replacing passwords with facial biometrics creates a new cybersecurity dilemma: while a password can be changed after compromise, your face cannot be replaced. That makes the security of the systems storing and processing biometric information especially important. Google's introduction of selfie authentication therefore represents both a major convenience and a significant privacy question — as digital identity moves away from something you know, like a password, towards something you are. My Broadband

4.7 MILLION FAKE WORK TOOLS: HACKERS ARE HIDING IN THE OFFICE

IMAGE SOURCE: PORTAL ERP

Cybercriminals are increasingly disguising malicious software as the everyday workplace tools employees rely on, with Kaspersky detecting 4,781,846 attempted attacks between July 2025 and June 2026 involving content associated with legitimate business platforms. The most frequently abused brand was Zoom, which accounted for 2,658,283 attempted attacks, followed by Outlook with 1,546,122, while attackers also used the names of OneDrive (197,030), Microsoft Excel (151,948) and Microsoft Teams (111,402) to make malicious content appear legitimate. The campaign exploits a simple but powerful weakness: employees are accustomed to downloading, opening or interacting with software and files associated with familiar workplace platforms, making a fake business tool a more convincing lure than an obviously suspicious file. Kaspersky warns that as businesses return to more active working routines, attackers are likely to exploit this familiarity by disguising malware and other malicious content as productivity, communication and collaboration software. The threat is particularly significant because these platforms often sit at the centre of corporate operations, meaning a compromised employee device could provide attackers with a pathway into sensitive company systems, credentials and data. The scale of the detections shows that cybercriminals are not merely impersonating obscure software — they are hiding behind the names employees see every day. Portal ERP

14,000 CAMERAS HIJACKED: THE INTERNET OF THINGS BECOMES A SURVEILLANCE NETWORK

IMAGE SOURCE: SECURITY WEEK

More than 14,000 internet-connected Dahua security cameras in Ukraine and Russia were compromised during a 35-day hacking campaign dubbed “Operation CameraSwarm,” exposing the security risks created by poorly protected Internet of Things (IoT) devices. According to research by Hunt.io cited by SecurityWeek, the campaign ran from 17 June to 22 July 2026, initially scanning IP addresses across several countries before concentrating on Russian and other Commonwealth of Independent States (CIS) telecommunications networks. Investigators identified 14,530 compromised devices, while the attackers used automated credential attacks against more than 12,000 unique addresses and established a persistent backdoor account on 1,923 cameras. Particularly concerning was the persistence of that access: the attackers’ backdoor account could survive a password change and, on most affected firmware, even a factory reset. In some cases, the attackers also exploited Dahua’s cloud infrastructure to reach cameras located behind network address translation (NAT), meaning cameras did not necessarily have to be directly exposed to the public internet. Hunt.io discovered that the attackers had established their infrastructure at least a year before launching the campaign and used a toolkit combining their own code with modified tools developed by other actors. The incident demonstrates how thousands of ordinary connected devices can be quietly transformed into a distributed network under an attacker’s control, creating risks that extend far beyond the individual camera owner. Security Week

META REMOVES DOZENS OF ADS AFTER INDIA FLAGS MALWARE SCAM ON FACEBOOK, INSTAGRAM

IMAGE SOURCE: THE INDIAN EXPRESS

Meta on Monday removed dozens of advertisements after India flagged a pattern of Facebook and Instagram ads using sexually explicit content to lure users into downloading malware that could steal banking credentials and drain bank accounts. India recorded nearly $2.4 billion in cyber-fraud losses in 2025, government data shows, as scam operators increasingly target the country's digital-payments boom. The government said ads on Facebook and Instagram operating under names such as "Night Play" and "Kyss" directed users to phishing websites. It said it had observed a rise in financial fraud involving what it described as "malicious Android applications masquerading as pornography apps". Reuters found at least 39 such ads still active after the government advisory was issued on Monday, with many of them using sexually explicit video thumbnails to attract clicks. Meta took down all of the ads shortly after Reuters flagged them to the company, seeking comment on the advisory

The Indian Express

REPRESSIVE MONITOR

SURVEILLANCE BY PROXY: HOW NIGERIAN POLICE USE PHONE RECORDS TO TRAP CIVIC ACTORS

IMAGE SOURCE: ICIR

A new investigation by The ICIR reveals how Nigerian police and security agencies are allegedly using telecommunications data not simply to track suspected individuals, but to map their entire networks of friends, colleagues and associates — turning ordinary phone records into a tool for locating activists, journalists and other civic actors. The investigation documents cases in which authorities reportedly identified people who communicated frequently with their targets, labelled them "soft targets", and then used those relationships to locate or pressure the person they were seeking. Activist Juwon Sanyaolu, for example, said police located him ahead of the June 2024 #EndBadGovernance protests by tracing the phone number he contacted most frequently and first detaining a friend who knew his whereabouts. Journalist Friday Alefia described a similar operation in which repeated calls, including purported job offers and an alleged emergency involving a family member, appeared designed to establish his location; investigators later allegedly told him they had mapped his frequent contacts, arrested the caretaker of his residence and used him to locate Alefia. The investigation places these cases within Nigeria's broader surveillance infrastructure: the Institute for Development Studies reportedly estimates that Nigeria spent at least $2.7 billion on surveillance technologies over the previous decade, making it Africa's largest customer for such systems. Digital-rights advocates say Nigerian security agencies are increasingly relying on telecom surveillance to identify and monitor activists and journalists, while lawyers interviewed by The ICIR stressed that phone tracking and access to communications are legally constrained and generally require judicial authorisation. The result is a disturbing shift in how surveillance can operate: you do not necessarily have to be directly monitored to become part of an investigation — your phone calls, your contacts and the people around you can become the pathway used to find you. ICIR

KENYA'S SPY GAME: GACHAGUA CLAIMS THE NIS TRIED TO INTERCEPT HIS SPEECH

IMAGE SOURCE: CIPESA

Former Kenyan Deputy President and Democracy for Citizens Party leader Rigathi Gachagua has accused Kenya's National Intelligence Service (NIS) of attempting to obtain the contents of his "Ruto@4" address before he delivered it, claiming the operation failed because his team deliberately avoided conventional digital communication and secretarial channels. According to Gachagua, he personally prepared the statement and had his wife, Pastor Dorcas Rigathi, type it, saying this prevented government operatives from accessing the speech electronically. The allegation offers a striking illustration of how concerns over state surveillance are influencing political activity in Kenya, where a senior opposition figure reportedly resorted to keeping sensitive political material outside ordinary digital systemsbecause he believed it could be intercepted. The speech itself was a detailed attack on President William Ruto's four-year record and included allegations of political intimidation, abductions, extrajudicial killings and the use of state security structures against opponents. While the NIS surveillance allegation remains an allegation made by Gachagua rather than an independently established finding, it raises significant questions about the potential use of intelligence capabilities against political actors and the safeguards governing state surveillance. The incident is particularly significant ahead of Kenya's 2027 general election, as growing political tensions increase scrutiny of how intelligence, policing and digital surveillance capabilities could be used in an electoral environment. For The Watcher, the most revealing detail is perhaps the simplest: a senior politician reportedly trusted a handwritten or manually prepared political statement more than digital communications because he feared the state could access it. That points to a broader cybersecurity concern — when political figures believe ordinary phones, computers and communication channels may be vulnerable to government interception, digital security becomes inseparable from political freedom, privacy and the ability of opposition actors to organise independently. Streamline Feed

MOZAMBIQUE'S CYBERSECURITY PUSH COLLIDES WITH A BATTLE OVER INTERNET CONTROL

IMAGE SOURCE: DEVELOPING TELECOMS

Mozambique is simultaneously strengthening its cybersecurity defences and confronting a major legal dispute over how far the government should be allowed to go in controlling digital communications. The country has recently advanced efforts to improve public awareness of cybercrime through a UN-supported cybersecurity awareness initiative, while its broader cybersecurity framework has also been strengthened through the adoption of new Cybersecurity and Cybercrime laws designed to protect networks, information systems and critical infrastructure. At the same time, Mozambique's Constitutional Council has struck down provisions of a government decree that would have given authorities powers to monitor communications, collect users' data, suspend internet services and technically intervene in telecommunications operators' networks. The court ruled that the government had exceeded its authority because such powers required parliamentary legislation rather than being created through a government regulation. The clash exposes a critical tension at the heart of Mozambique's digital-security agenda: the same state seeking stronger powers to combat cybercrime and protect national networks is also being challenged over whether those powers could undermine privacy, communications rights and internet freedom. For The Watcher, the story is significant because cybersecurity legislation is not only about defending citizens from hackers and cybercriminals; it also determines what governments themselves are legally permitted to see, collect and control in cyberspace. Mozambique's court intervention therefore provides an important example of the growing struggle across Africa to build stronger cyber defences without allowing cybersecurity to become a justification for unchecked government surveillance or internet control. Developing Telecoms

ARGENTINA'S SURVEILLANCE STATE: WHEN PROTESTERS BECOME DATA

IMAGE SOURCE: SECURITY WEEK

Argentina is becoming a striking example of how mass-surveillance technology can move from a security tool into an instrument of social and political control, with Amnesty International warning that the government's expanding use of surveillance is threatening privacy, freedom of expression and the right to peaceful protest. According to Amnesty's August 2026 report, Argentina acquired at least US$1.2 million worth of mass-surveillance technology during 2024–2025, including social-media monitoring systems, aerial drones and facial-recognition software, some supplied by companies with records of large-scale surveillance. The technology is increasingly being deployed in both physical and digital spaces, with Amnesty documenting how protesters, journalists, young people and human-rights activists can be monitored or identified. The chilling effect is already visible: pensioners participating in weekly demonstrations against pension cuts in Buenos Aires reported being followed by drones and said that protesters had been identified, while some people were becoming reluctant to attend demonstrations because they feared being tracked or targeted. Amnesty argues that this creates a dangerous feedback loop in which surveillance does not merely observe protest—it can discourage people from protesting in the first place, weakening freedom of assembly without authorities needing to physically stop a demonstration. The organisation is calling for bans on the development, sale and use of remote biometric-recognition systems for mass or discriminatory surveillance, alongside stronger controls over the procurement and trade of surveillance technologies. For The Watcher, Argentina offers a powerful warning of what happens when governments combine facial recognition, drones, social-media monitoring and AI-driven surveillance: the threat is no longer simply that authorities can see a protest, but that people may begin to censor themselves because they know they can be seen. Amnesty International

DELHI'S PROTEST ZONE BECOMES A SURVEILLANCE ZONE

IMAGE SOURCE: BUSINESS & HUMAN RIGHTS CENTRE

A protest site in New Delhi has become the centre of a growing controversy over AI-powered policing, facial recognition and biometric surveillance, after demonstrators alleged that Delhi Police subjected protesters at Jantar Mantar to continuous technological monitoring. According to the Business & Human Rights Resource Centre, protesters reported the use of AI surveillance systems, facial-recognition technology, surveillance cameras and Meta smart glasses, raising concerns that police could identify, track and monitor people participating in peaceful political activity. A key piece of technology reportedly deployed around the protest was "Ikshana," a police surveillance system equipped with high-resolution cameras capable of monitoring people in the surrounding area, while reports indicate that facial-recognition systems were positioned around protest entry and exit points. Delhi Police has defended the surveillance, arguing that photography and videography are routine policing measures and, more recently, telling India's Supreme Court that facial recognition at the protest was intended to identify known criminals rather than indiscriminately monitor demonstrators. Nevertheless, the allegations have triggered a broader legal and civil-liberties debate because protesters argue that biometric identification in a political gathering can transform ordinary attendance into a permanent digital record of participation. The controversy is particularly significant because facial recognition removes much of the anonymity traditionally associated with public protest: cameras can capture faces at a distance, algorithms can compare them against databases, and surveillance can potentially link an individual's physical presence to their identity. Meta has also been asked to respond to allegations concerning the use of its smart-glasses technology, adding another layer to concerns about the growing involvement of private technology in state surveillance. The case has now reached India's courts, with a Supreme Court petition challenging the use of facial-recognition surveillance at the protest. For The Watcher, Jantar Mantar demonstrates the increasingly blurred boundary between public security and biometric monitoring of dissent: when showing up to a protest can mean being digitally identified, recorded and potentially matched against government databases, surveillance itself can become a deterrent to exercising the right to peaceful assembly. Business and Human Rights Centre

AI'S IRON GRIP: HOW DICTATORSHIPS ARE TURNING ALGORITHMS INTO SURVEILLANCE WEAPONS

IMAGE SOURCE: SECURITY WEEK

Artificial intelligence is rapidly changing the machinery of authoritarian control, giving governments new ways to identify, monitor, predict and suppress dissent at a scale that would have been difficult with human surveillance alone, according to The Insider. The investigation examines China, Russia, Iran, North Korea, Turkey and Belarus, showing how AI is being integrated into existing systems of facial recognition, telecommunications monitoring, censorship, biometric databases and mass video surveillance. China represents the most advanced example: authorities are increasingly combining biometric, geolocation and financial data with AI systems capable of processing enormous datasets in real time, while a surveillance network of more than 600 million cameras can use facial and even gait recognition to identify people, detect unusual gatherings and flag behaviour associated with potential protests. AI is also reducing the human labour traditionally required for censorship by allowing systems to interpret context, sarcasm, images and voice messages rather than simply searching for banned words. In Russia, authorities are developing centralised video-surveillance systems and AI tools for monitoring political content, while Kremlin-linked actors are also using generative AI to automate disinformation and cyber operations. Iran is deploying facial recognition to enforce rules governing women's dress, while Turkey has used biometric analysis of street-camera footage alongside social-media information to identify protesters. Belarus has reportedly used AI to analyse huge archives of protest footage, allowing authorities to identify people years after demonstrations occurred. The investigation also highlights a broader geopolitical danger: authoritarian governments are increasingly sharing surveillance expertise, hardware and software, with China emerging as a potential supplier of technologies that could allow other regimes to build sophisticated digital-control systems without relying on Western technology. The result is a new model of surveillance in which governments do not simply collect information about citizens — AI allows them to connect disparate digital traces, identify patterns of behaviour and potentially intervene before dissent develops into organised action. The Insider

THE GOVERNMENT APP YOU COULDN'T DELETE: INDIA'S SMARTPHONE SURVEILLANCE CONTROVERSY

IMAGE SOURCE: TECH REPUBLIC

India's attempt to turn every smartphone into a potential frontline of cyber defence sparked a major privacy controversy after the government ordered manufacturers to pre-install its Sanchar Saathi cybersecurity app on all new phones, with existing devices also to receive the app through software updates. The November 2025 directive gave companies including Apple, Samsung, Xiaomi, Vivo and Oppo 90 days to comply, and required the app to remain readily accessible rather than allowing users to disable or remove it. Sanchar Saathi was designed to combat mobile fraud by helping users identify fraudulent connections, verify device identities through IMEI numbers, and block or trace lost and stolen phones; the government said the system had already helped block millions of compromised devices and terminate fraudulent mobile connections. But privacy advocates argued that making a state-controlled application effectively unavoidable on privately owned devices crossed an important line by removing meaningful user consent and creating concerns about data governance, potential scope expansion and state access to the digital environment of hundreds of millions of citizens. The controversy was particularly significant because India has more than 1.2 billion mobile subscribers, meaning a mandatory pre-installed application could have placed a government-controlled cybersecurity tool on an enormous portion of the country's digital infrastructure. Apple reportedly resisted the requirement because it conflicted with its policies around third-party pre-installed software, while the broader backlash forced the Indian government to reconsider the mandate. The order was ultimately withdrawn days later, with authorities saying Sanchar Saathi would remain voluntary. The episode nevertheless highlights a much bigger cybersecurity dilemma: when governments use cybersecurity as the justification for putting state-controlled software directly onto personal devices, where does protection end and digital intrusion begin? Tech Republic

PEGASUS STRIKES AGAIN: HOW SPYWARE TURNS A PHONE INTO A SURVEILLANCE DEVICE

IMAGE SOURCE: MALLORY

NSO Group's Pegasus spyware continues to demonstrate how commercial surveillance technology can be used to secretly target journalists, activists and human-rights defenders, with recent investigations documenting infections and attempted compromises across Jordan and other countries. According to Mallory's synthesis of research from Citizen Lab, Google, Amnesty International and technical researchers, New York Times journalist Ben Hubbard had his iPhone compromised more than once through sophisticated zero-click iMessage exploit chains, meaning the attacks could infect the device without requiring the target to click a malicious link. In Jordan, Citizen Lab documented repeated Pegasus targeting of human-rights defenders, lawyers and journalists between 2019 and 2021, and assessed that suspected Pegasus operators MANSAF and BLACKIRIS were likely connected to Jordanian government agencies. The technical capabilities exposed by analysis of Pegasus and its Android variant Chrysaor are particularly alarming: once deployed, the spyware can provide access to messages, contacts, call records, emails and application data, while enabling functions such as keylogging, screenshots, camera access, microphone recording and covert data extraction. Researchers also found that Pegasus can communicate with its command-and-control infrastructure while disguising activity and can contain mechanisms designed to remove traces of the spyware from an infected device. The documented targeting demonstrates why Pegasus represents more than conventional malware: it is a state-linked surveillance capability designed for highly specific individuals, potentially allowing governments or their operators to turn a journalist's or activist's personal smartphone into a covert intelligence-gathering platform. The case also highlights the importance of forensic investigation, with Amnesty International developing methodologies for identifying Pegasus infections and Citizen Lab repeatedly using device evidence to establish who was targeted and how. Mallory

WHEN SPYWARE BECOMES EVERYONE'S PROBLEM: THE GLOBAL REACH OF GOVERNMENT HACKING

IMAGE SOURCE: TECH REPUBLIC

Nation-state spyware is no longer simply a tool used by governments to pursue suspected criminals or security threats; its growing commercialisation has created a global surveillance problem in which journalists, activists, political figures, businesses and ordinary citizens can all become potential targets. The proliferation of sophisticated commercial spyware means governments can purchase capabilities that exploit vulnerabilities in smartphones and other connected devices, allowing operators to gain access to highly sensitive information and, in some cases, monitor communications and activity without the victim's knowledge. What makes this particularly concerning is the lack of transparency surrounding who is targeted, what legal authority is used and what happens to information collected during an operation. Spyware can also cross national borders, creating diplomatic and security consequences when governments target individuals located in other countries or use surveillance against foreign officials and journalists. The growing market has therefore blurred the traditional distinction between state intelligence operations and commercial cybercrime, because companies develop and sell the capabilities while governments deploy them against real-world targets. As commercial spyware becomes more advanced and increasingly difficult to detect, the central challenge is no longer simply whether governments should have sophisticated surveillance capabilities, but whether democratic institutions can establish meaningful limits on technologies that can secretly turn a person's own phone into an intelligence-gathering device. The issue ultimately affects everyone because vulnerabilities created or exploited for state surveillance can become part of a wider ecosystem of cyber risk, potentially weakening the security and privacy of the broader digital environment. Homeland Security

THE FBI'S PEGASUS PROBLEM: AMERICA'S SPYWARE OVERSIGHT HAS A BLIND SPOT

IMAGE SOURCE: TECH REPUBLIC

Newly disclosed records reveal that the FBI went considerably further than simply testing Pegasus, the powerful phone-hacking spyware developed by Israeli surveillance company NSO Group, exposing a gap between the government's expanding use of commercial spyware and the transparency mechanisms designed to monitor it. The records show that the FBI acquired Pegasus and explored how it could be incorporated into criminal investigations, including developing proposed guidelines for its potential use, before ultimately deciding not to deploy the NSO tools operationally. The FBI's interest is significant because Pegasus can enable investigators to obtain information directly from targeted devices, making it fundamentally different from conventional surveillance methods that intercept communications as they travel across networks. The revelations also come as U.S. courts prepare to introduce a new "spyware/hacking" category in their annual wiretap statistics, beginning with activity in 2028 and producing the first public figures in 2029. However, the Pegasus records demonstrate why those numbers will remain incomplete: government agencies can spend years testing spyware, negotiating its use, developing operational guidelines and assessing potential applications before a judge ever authorises a reportable hacking-based wiretap. In other words, the official statistics could eventually show how often courts approve certain spyware operations while still concealing the much larger ecosystem of government experimentation and preparation surrounding commercial hacking tools. Tech Republic

HOW MASS SURVEILLANCE FROM ONLINE ADVERTISING PUTS JOURNALISTS AT RISK

IMAGE SOURCE: CPJ

A special report from CPJ's Jonathan Rozen, produced with the Harvard Kennedy School's Carr-Ryan Center, lays out in granular detail how the online advertising ecosystem — worth nearly $1 trillion — has quietly become one of the most effective tools for tracking journalists worldwide, often without any hacking involved at all.

The opening hook: Belgian journalist Nicolas Baudoux was able to locate a colleague using a free two-week sample from a US data broker covering roughly a million devices and 100 million locations. German journalist Ingo Dachwitz found his own movements in a similar free sample, despite knowing a weather app was tracking him — "it's very spooky," he told CPJ, even for someone who studies this for a living.

How the tracking actually works — six interlocking pieces:

- SDKs (software development kits) embedded in ordinary apps quietly harvest location data, which developers have a direct financial incentive to sell since it raises ad bid prices.
- Real-time bidding (RTB) auctions broadcast a user's data profile — location, political affiliation, employment, even health and mental health status — to unregulated bidders every time an ad-carrying page or app loads. Crucially, you don't even need to win the auction to harvest the data.
- Advertising IDs, though nominally anonymous, provide "no anonymity" according to the US FTC, and AI is making it steadily easier to re-identify individuals from them.
- Data brokers package and resell this information — a 2021 Xandr (Microsoft) marketplace dataset reportedly included literal targeting segments like "uk_femalejournalists" and people interested in "Committee to Protect Journalists."
- ADINT (advertising intelligence) firms sell purpose-built surveillance tools. Citizen Lab's investigation into Nebraska-based Penlink's "Webloc" product found it's been used by Hungarian intelligence, El Salvador's police, and US agencies, with signs of tracking activity in at least eight countries.
- Ad-delivered spyware is the newest frontier: firms like Intellexa (maker of Predator spyware) have developed "half-click" infection methods where simply having an infected ad served to your device — no click required — can trigger a compromise, a technique researchers say emerged as phone security improved and zero-day exploits got pricier.

Real-world cases: Exiled Egyptian journalist Basma Mostafa's full "pattern of life" — home address and regular haunts — turned up in a commercial dataset obtained as a free sample, raising fears Egyptian authorities used it to track her in Berlin. A Hungarian reporter and a Salvadoran outlet have separately documented Webloc-style tools being used in contexts where journalist surveillance is already well established. In the US, journalist Byron Tau confirmed to CPJ that an attempt was made to track a White House reporter using commercial data during Trump's first term.

The regulatory picture is thin. A June 2026 legal study found "significant legal gaps and ambiguities" across US and European law governing commercial data. The FTC has taken some enforcement action (banning Kochava's subsidiary from selling sensitive location data) and a 2025 complaint against Google's RTB system — alleging data flowed to entities in China and Russia — remains stalled with no substantive movement as of August 2026. UN Special Rapporteur Gina Romero put it bluntly: private tech built the surveillance infrastructure that states are now exploiting.

INTELLIGENCE AGENCIES

SOUTH AFRICA'S DIGITAL ID: CONVENIENCE AT THE COST OF A BIGGER PRIVACY RISK?

IMAGE SOURCE: MY BROADBAND

South Africa's planned Digital ID system could fundamentally change how citizens prove who they are, replacing reliance on physical identity documents with a digital identity linked to biometric information such as fingerprints and facial recognition and capable of storing or providing access to records including IDs, driving licences, marriage certificates and social-grant information. The government's MyMzansi roadmap presents the system as a way to make public services faster and more accessible, allowing people to verify their identities remotely through devices, QR codes or other secure methods. But the central cybersecurity concern is that concentrating such a large volume of highly sensitive personal information into a digital identity infrastructure could create an extremely valuable target for cybercriminals: unlike a password, biometric data cannot simply be changed after it is stolen. Critics have also raised concerns about the potential for surveillance or misuse if a centralised identity system is poorly secured or accessed without adequate safeguards. The debate is particularly significant given South Africa's existing identity-fraud problem and the government's ambition to make the Digital ID a foundation for broader digital public services. The proposed system therefore presents a fundamental cybersecurity trade-off: putting identity documents, biometrics and access to essential government services into one interconnected digital ecosystem could make life considerably easier for citizens, but it could also make a successful breach far more consequential. The government says the system is intended to improve security and convenience, but questions around data protection, access controls, oversight and what happens when biometric information is compromised will be crucial to determining whether South Africa's digital-ID revolution strengthens identity security or creates a new single point of failure. My Broadband

WHEN YOUR FACE BECOMES THE GATEKEEPER: SASSA'S DIGITAL CRACKDOWN RAISES PRIVACY QUESTIONS

IMAGE SOURCE: POST

South Africa's crackdown on social-grant fraud is increasingly relying on digital identity, biometric verification and data-sharing, but an opinion piece in The Post argues that the technology intended to protect the grant system could also create new barriers for vulnerable beneficiaries. Social Development Minister Dina Pule has confirmed that more than 350,000 grants will be reviewed during the 2026/27 financial year, with the department expecting to save approximately R1.5 billion, while SASSA is using bank and credit-bureau information, Home Affairs-linked biometric verification and its e-Life Certification system to determine whether beneficiaries still qualify. The scale of the data-driven checks is significant: SASSA reportedly flagged more than 420,000 beneficiaries for review in the previous financial year, completed 240,000 checks and found 160,000 people who failed to comply, while a separate analysis of six million bank accounts and eight million credit records resulted in 291,000 grants being flagged and more than 34,000 cancelled. But the technology is producing its own problems: although 88% of roughly 15,500 people using the online portal in mid-April were successfully verified, facial-recognition verification generated nearly 7,800 complaints, compared with almost none involving fingerprints. Beneficiaries who fail facial verification can consequently be pushed back into already overcrowded SASSA offices, while organisations such as Black Sash have warned that the review process could potentially exclude more than 200,000 people who remain eligible for assistance. The article therefore exposes a wider digital-governance dilemma: when governments use interconnected databases, biometrics and automated verification to fight fraud, a failure in the technology can become a failure in access to essential services. For elderly or poor beneficiaries who may lack reliable internet access, airtime or the money to travel long distances to a SASSA office, a digital verification system designed to make administration more efficient can instead become another obstacle between citizens and the support they depend on. Post

GOODBYE PASSPORT STAMPS: SOUTH AFRICA'S AI BORDER IS WATCHING

IMAGE SOURCE: PRESS READER

South Africa is replacing an old symbol of international travel—the passport stamp—with an AI-powered digital border system that combines machine learning, biometric verification and facial recognition, raising both security benefits and significant questions about privacy and data protection. Launched by President Cyril Ramaphosa at OR Tambo International Airport, the Electronic Travel Authorisation (ETA) has already processed 216,204 applications during its pilot phase and rejected 6,126 fraudulent submissions, including fake passports and manipulated documents. The system is currently operating at OR Tambo, Cape Town International, King Shaka and Lanseria airports, with plans to expand to land and sea ports and eventually cover study, work and spousal visas. While Home Affairs Minister Leon Schreiber says the technology will make legitimate travel faster while strengthening border security and reducing visa fraud, the shift means that travellers' identities are increasingly being verified through facial data and digital records rather than physical documents. That creates a new cybersecurity and privacy challenge: biometric information is highly sensitive, and unlike a compromised password, a person's face cannot simply be changed if their biometric data is stolen or misused. South Africa's move mirrors a wider international shift, including the European Union's Entry/Exit System, which records facial scans and fingerprints and automatically tracks when non-EU travellers enter and leave the Schengen Area. The experience of other countries also shows that digital border systems can suffer technical failures and delays, meaning that security, reliability and public trust must develop alongside the technology. Press Reader

CONTINUOUS FACIAL SECURITY GOES LIVE IN SA

IMAGE SOURCE: GADGET

A new system designed to continuously verify an authorised user's presence throughout a digital session has been launched in South Africa. Continuous Facial Recognition with Liveness is being offered locally by Flownamix Group. The launch includes Secure Enterprise Messaging, which protects communications through verified identities and end-to-end encryption. Both products use patented technology from YEO Messaging. "The introduction comes at a time when organisations are re-evaluating how they establish trust in digital environments," say the companies. "The rise of identity fraud, AI-enabled impersonation and increasingly sophisticated cybercrime is driving demand for technology that provides stronger identity assurance beyond the point of login." According to the South African Banking Risk Information Centre (SABRIC), digital banking fraud incidents increased by 86% in 2024, while associated losses rose by 74% to nearly R1.9-billion. Continuous Facial Recognition with Liveness and Secure Enterprise Messaging can provide identity verification and secure communications across the digital journey. Leon van der Merwe, Flownamix Group CEO, says: "Our partnership with YEO Messaging, combined with Continuous Facial Recognition (CFR) technology, represents an important step towards secure, identity-assured communication where the person receiving, viewing or acting on sensitive information can be continuously and confidently verified. "For Flownamix Group, this partnership is not simply about adding another layer of authentication. We believe this approach will become increasingly important for regulated industries, enterprises and service providers that need to protect confidential information, reduce impersonation risk and strengthen accountability across digital interactions."
In SA, Continuous Facial Recognition with Liveness and Secure Enterprise Messaging are distributed through Datanamix, SigniFlow and SMSFlow, with local support from Flownamix Group and YEO Messaging. Gadget

SOMALIA'S INTELLIGENCE AGENCIES ARE BECOMING THE COUNTRY'S NEW CENSORS

IMAGE SOURCE: INDEX ON CENSORSHIP

This article reports that journalists in Somalia are being arrested without warrant, questioned over their reporting and forced into exile . "Do you know that we can kill you? To us, your life is worth less than a cigarette." These are the words with which operatives from Somalia's National Intelligence and Security Agency (NISA) threatened freelance journalist Mohamed Bulbul, days after he co-authored a news report for UK news outlet The Guardian about the prosecution of activist Sadia Moalim Ali. Two days after the article ran in June 2026, Bulbul was having dinner with two fellow journalists at a restaurant in Mogadishu's Zoobe area when armed men wearing black masks entered the establishment. "They walked straight towards our table [shouting] 'Stand up! Stand up!'" Bulbul told Index. The masked men beat all three journalists before they dragged him outside, placed a bag over his head and forced him into a vehicle. After being moved between two police stations and the offices of the regional police commissioner, Bulbul was interrogated by NISA officers about the article. "They asked me why I had published it." He was then, he said, given three choices: "Work with us and take money, leave the country, or if you refuse both, we will kill you." Bulbul fled Somalia and is now in an undisclosed safe location. "Saving my own life become my priority," he said. "I can no longer spend time with my parents or my children." Bulbul's experience is not unique. Across Somalia, journalists and press freedom advocates say that intelligence and security agencies are intimidating, detaining and otherwise silencing reporters. Recent cases in Mogadishu and Puntland state indicate the state's growing reliance on intelligence agencies and extra-legal actions, rather than the police and the courts, to deal with critical journalism. Index on Censorship

CYBERSECURITY OR CENSORSHIP? ZAMBIA AND SOUTH SUDAN TIGHTEN THEIR GRIP ON THE INTERNET

IMAGE SOURCE: DEVELOPING TELECOMS

Zambia and South Sudan have begun enforcing new cybercrime laws that authorities say are necessary to combat online crime and strengthen national cybersecurity, but critics warn that the legislation could also expand state control over digital speech and create new risks for journalists, activists and political opponents. In Zambia, the government has activated the Cyber Crimes Act No. 4 of 2025, warning that the unauthorised recording, publication or distribution of private communications can result in criminal penalties; the Act operates alongside the country's Cyber Security and Data Protection laws, creating a broader regulatory framework covering online communications, personal data and digital services including banking, mobile money and e-commerce. In South Sudan, authorities have likewise begun implementing the Cybercrime and Computer Misuse Act 2026, presenting it as a tool to strengthen cybersecurity and tackle online criminal activity. However, critics argue that some provisions in both countries are too broadly worded, particularly offences concerning "undesirable" online content and the publication of "false or misleading information", because the legislation does not always clearly define what constitutes prohibited material. This ambiguity creates the possibility of selective enforcement against legitimate criticism, independent journalism or political dissent. Zambia's Law Association has previously raised concerns that its cybersecurity legislation could facilitate increased state surveillance, while digital-rights and media organisations have voiced similar fears over South Sudan's new law. The developments highlight a growing tension across Africa: governments are responding to genuine cybercrime threats with stronger digital laws, but legislation designed to secure cyberspace can also become a mechanism for controlling what citizens can say, record and share online. Developing Telecoms

SENEGAL ADOPTS CRITICAL INFRASTRUCTURE BILL AS CALLS GROW FOR STRONGER CYBERSECURITY FRAMEWORK

IMAGE SOURCE: TECH REVIEW AFRICA

Senegal has taken a significant step towards strengthening its cyber defences after the National Assembly adopted Bill No. 25/2026 on the protection of critical information infrastructure, creating a new legal framework for securing the digital systems that underpin essential national services. The legislation is intended to protect Senegal's strategic information infrastructure, strengthen the state's ability to anticipate, prevent and respond to cyber threats, and establish common security standards for government institutions, individuals and private organisations. The move forms part of a broader overhaul of Senegal's cybersecurity architecture, with proposals including a National Cybersecurity Authority, a National CERT, sector-specific CERTs and Cybersecurity Operations Centres (SOCs), alongside requirements for certain organisations to report cyber incidents and vulnerabilities. The framework also addresses the growing security risks created by outsourced digital services and cloud infrastructure, including rules governing the outsourcing of digital systems and the local hosting of public-sector data. The legislation comes as Senegal accelerates its digital transformation under its broader New Deal Technologique agenda, which includes sovereign cloud infrastructure, data centres and expanded digital connectivity—making the protection of those systems increasingly important as more essential services become digitally dependent. Tech Review Africa

ENUGU'S MULTI-BILLION-NAIRA SURVEILLANCE CENTRE WITH NO OVERSIGHT LAW

IMAGE SOURCE: ICIR

Nigeria's Enugu State has built a multi-billion-naira AI-powered surveillance network capable of watching streets, identifying vehicles and faces, tracking incidents and deploying security teams in real time—but the system is operating without a dedicated law governing how its surveillance powers and data should be used. An investigation by The ICIR found that Governor Peter Mbah's Safe City initiative links more than 1,000 CCTV cameras across Enugu to a central Command-and-Control Centre inside Government House, with operators able to zoom in on vehicles and faces, while drones equipped with thermal and zoom cameras provide aerial surveillance across urban and rural areas. The technology includes AI-powered CCTV, automatic number-plate recognition (ANPR), facial recognition, drones, forensic databases and encrypted communications equipment. The scale of the investment is substantial: Enugu's 2024 budget contained about ₦4.657 billion in security-technology allocations, including ₦940 million for surveillance and monitoring, while the 2025 budget allocated ₦10 billion for high-tech CCTV, AI cameras, drones and facial recognition. The government says the system has helped reduce violent crime by 80%, although the police did not provide comparative crime statistics to substantiate the claim. The investigation, however, found a major accountability gap: Enugu currently has no specific law governing the Safe City surveillance centre, no independent oversight board and no clear publicly available rules establishing who can access footage, how long data is retained, when facial recognition or tracking may be used, or how citizens can challenge surveillance or request information about their data. The state Attorney General confirmed that legislation is still being drafted and argued that the Nigeria Data Protection Act 2023 currently provides the necessary legal framework. Meanwhile, journalists, activists and opposition figures have alleged that surveillance infrastructure has contributed to monitoring and intimidation, with some journalists telling ICIR they now hesitate to publish critical reporting because they fear being watched or tracked. The state government strongly denies using Safe City for political surveillance and insists that its purpose is crime prevention and emergency response. ICIR

PEGASUS RETURNS TO MOROCCO: INSIDE A SPYWARE MACHINE THAT "SPIES ON EVERYONE"

IMAGE SOURCE: PPSA

Morocco's alleged use of Pegasus spyware is back under scrutiny after a whistleblower who previously worked within the country's internal security services provided new evidence to a collaborative investigation involving The Guardian, Forbidden Stories and Amnesty International's Security Lab. The investigation alleges that Moroccan intelligence used Pegasus — a highly invasive spyware capable of remotely compromising smartphones and accessing emails, text messages and photographs, while potentially activating a device's microphone and camera — against journalists, human-rights defenders and political figures, despite NSO Group's stated position that its technology is sold to governments to investigate serious criminals and terrorists. Morocco has denied having a relationship with NSO Group, but investigators say they found evidence indicating otherwise. The alleged surveillance also extended beyond Morocco's borders: investigators identified approximately 200 Spanish mobile numbers that were reportedly targeted, including those belonging to Spain's prime minister and ministers responsible for defence, interior and agriculture, demonstrating how commercial spyware can turn a smartphone into a remote intelligence-gathering device without requiring physical access to the phone. The investigation further alleges that Moroccan intelligence expanded its targeting after acquiring Pegasus, moving from purported security-related uses toward journalists and human-rights defenders. Most strikingly, a former Moroccan intelligence officer reportedly described the approach as "We spy on everyone… just in case," capturing the central concern surrounding Pegasus: technology marketed as a tool for targeted investigations can become far more powerful — and far more intrusive — when deployed without effective legal, judicial and democratic oversight. PPSA

INDIA'S AI SURVEILLANCE FACES THE COURTS: CAN SECURITY JUSTIFY WATCHING CITIZENS?

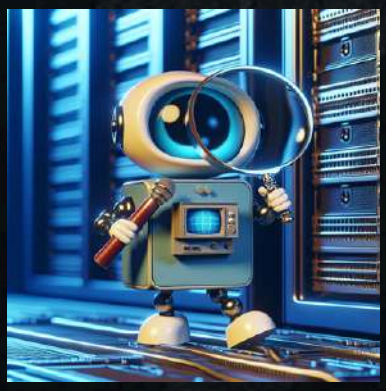


IMAGE SOURCE: DEV DISCOURSE

India's expanding use of AI-powered surveillance is now facing a constitutional challenge, after student activist Aishe Ghosh went to court alleging that police used facial-recognition technology and a 360-degree surveillance van to monitor participants during a major youth protest without adequate legal safeguards. The case centres on a fundamental conflict: Indian authorities argue that advanced surveillance tools can strengthen public security and help identify potential threats, while civil-liberties advocates contend that deploying facial recognition and other AI systems without clear limits, transparency or judicial oversight can undermine citizens' constitutional right to privacy. The petition reportedly seeks not only scrutiny of the surveillance operation but also the destruction of data collected through it, highlighting concerns over what happens to biometric information once it has been captured. The dispute comes amid India's wider expansion of AI-assisted policing and facial-recognition systems, raising questions about whether existing legal frameworks are capable of controlling technologies that can identify and monitor people at scale. The case could therefore have implications far beyond the individual protest: if governments can use AI to identify, track and analyse people in public spaces without sufficiently clear safeguards, mass surveillance could become increasingly normalised before democratic institutions have established where the boundaries should lie. At its heart, the legal battle asks whether the promise of greater security gives the state enough justification to deploy technologies capable of turning ordinary public gatherings into sources of biometric intelligence. Dev Discourse

BRAZIL WANTS FACIAL RECOGNITION EVERYWHERE — BUT WHO GETS TO WATCH THE WATCHERS?

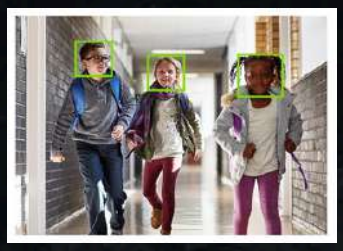


IMAGE SOURCE: BIOMETRIC UPDATE

Brazil is moving toward establishing clearer legal rules for the rapidly expanding use of facial-recognition technology, with lawmakers considering legislation that could govern deployments ranging from schools and public transport to roads and public buildings. One proposed measure, Bill 1225/2026, specifically addresses facial recognition in schools after reports highlighted the technology's rapid spread across Brazil's education system, including more than 1,700 schools in Paraná. The bill would not ban facial recognition outright, but would require safeguards including a clear legal basis, appropriate consent, transparency, security measures, proven accuracy and human review rather than fully automated decision-making. It would also treat practices such as automated attendance without human oversight, collecting students' biometric data without parental consent, using inaccurate or unaudited systems and automatically linking biometric information to social-benefit accounts as examples of irresponsible deployment. At the same time, another bill, 1828/2023, is being considered as a legal basis for facial-recognition systems across public transport, including vehicles, roads and public buildings. The debate is particularly significant because facial recognition has already expanded faster than Brazil's specific regulatory framework, leaving authorities, companies and citizens grappling with questions about when biometric surveillance is justified and what limits should apply. The urgency of those questions was underscored in August when Brazil's data-protection authority ordered Paraná's education system to stop collecting students' facial biometrics for attendance, saying the state had failed to demonstrate an adequate legal basis and sufficient security and governance protections. Brazil's emerging regulatory battle therefore raises a much larger surveillance question: when facial recognition moves from exceptional security measure to everyday infrastructure — scanning commuters, drivers, students and people in public buildings — who controls the biometric database, and who is accountable when the system gets it wrong? Biometric Update

CHINA'S AI IS WINNING AFRICA — BUT AT WHAT COST TO DIGITAL INDEPENDENCE?

IMAGE SOURCE: THE NEW YORK TIMES

China's artificial intelligence industry is rapidly gaining ground across Africa, not necessarily because its models are the most powerful, but because they are cheaper, downloadable, customisable and easier for African developers to deploy on limited infrastructure. The New York Times reports that Chinese models now account for roughly half of AI use on OpenRouter, up from less than 25% a year earlier, while 19 of the 25 most-downloaded open-source models on Hugging Face are Chinese. African developers are increasingly building on these systems: in Uganda, Ernest Mwebaze developed Sunflower, an AI tool using an Alibaba model that can understand dozens of Ugandan languages and provide farmers with weather and agricultural advice in local dialects; in Kenya, developers are using Chinese models for banking, government services and legal technology, with one legal-document platform costing around $25,000 to build compared with an estimated $1 million-plus using Anthropic's Claude. China is also leveraging its existing technological footprint: Huawei has built infrastructure at Kenya's Konza Technopolis, Chinese technology already underpins major telecommunications and mobile-money systems, and Chinese companies are offering African developers incentives such as free computing, technical assistance and subsidised access. But the growing dependence raises a deeper cybersecurity and digital-sovereignty concern: African organisations are increasingly building critical services on AI technologies developed and controlled by foreign companies, meaning models can potentially be altered, withdrawn, restricted or influenced by geopolitical decisions beyond African governments' control. Sunflower illustrates the risk particularly clearly: after being questioned about China, the Ugandan chatbot reportedly described China as a democracy and avoided questions about its economic and environmental impact in Uganda, prompting its developer to reconsider the technology behind the system. The competition is therefore about more than AI performance; it is becoming a contest for Africa's digital infrastructure, data, developers and technological loyalties, with the United States and China offering very different models of access and control. For African countries, the attraction of inexpensive Chinese AI is obvious, but the strategic question is whether adopting these systems will expand technological opportunity or create a new form of digital dependency in which essential AI capabilities are ultimately shaped outside the continent. The New York Times

FIVE EYES UNDER WATCH: THE GLOBAL FIGHT AGAINST MASS SURVEILLANCE

IMAGE SOURCE: FPIF

The intelligence alliance known as the Five Eyes — Australia, Britain, Canada, New Zealand and the United States — has built an extensive system for sharing signals intelligence, but growing international opposition is challenging the surveillance powers that underpin it. The alliance expanded significantly after the September 11 attacks, and the 2013 Snowden disclosures revealed how information collected under national surveillance laws could circulate between member states, raising concerns about the ability of governments to bypass domestic safeguards through intelligence cooperation. The latest battleground is encrypted communications, where governments increasingly seek technical access to data that providers themselves cannot read. Britain's reported demands to Apple over its encrypted iCloud service illustrate the problem: forcing a provider to create government access to end-to-end encrypted data could weaken protections not only for the intended target but potentially for other users and create vulnerabilities exploitable by criminals or foreign governments. The controversy has triggered resistance from technology companies, privacy organisations and civil-society groups, with Apple challenging British surveillance orders and international coalitions organising opposition through courts, legislatures and public campaigns. The article also highlights resistance beyond the Five Eyes countries, including southern African campaigns against surveillance powers: in Botswana, public opposition helped force changes to legislation requiring High Court approval for interception; in Mauritius, activists challenged the creation of a central fingerprint database; and in South Africa, the Right2Know Campaign has opposed laws threatening journalists and whistleblowers who expose classified information. In the United States, civil-society groups are similarly pushing for stronger safeguards around Section 702, the controversial surveillance authority that permits the collection of communications involving foreigners abroad and can incidentally capture communications involving U.S. persons. The broader message is that resistance to state surveillance is becoming increasingly international: as intelligence agencies collaborate across borders and governments seek greater access to encrypted data, privacy advocates, technology companies, courts and ordinary citizens are also building cross-border networks to challenge those powers. FPIF

CANADA'S SURVEILLANCE GAMBLE COULD COST IT ACCESS TO U.S. CLOUD EVIDENCE

IMAGE SOURCE: LAWFARE

Canada's push to expand government surveillance powers could jeopardise the very tool its law-enforcement and intelligence agencies need to access digital evidence held by U.S. technology companies. The Lawfare analysis focuses on Bill C-22, Canada's proposed "lawful access" legislation, arguing that some of its surveillance provisions could undermine negotiations for a Canada-U.S. CLOUD Act agreement. Canadian investigators currently face major delays when seeking evidence stored by U.S.-based providers, with requests through traditional diplomatic channels reportedly taking around three to six months; a bilateral CLOUD Act agreement would instead create a faster, direct route for obtaining electronic evidence in serious criminal investigations, subject to legal safeguards and independent oversight. The U.K. provides an indication of the potential scale: by October 2024, British authorities had submitted 20,142 ordersto U.S. providers under its CLOUD Act agreement, supporting investigations involving arrests, financial recovery, weapons seizures and threats to life. The problem is that Bill C-22 could require technology providers to implement surveillance capabilities or otherwise weaken security features, including measures that raise concerns about encryption and the possibility of creating vulnerabilities that could be exploited by governments or malicious actors. That is particularly problematic for Washington because U.S. law requires countries seeking CLOUD Act agreements to meet standards concerning privacy, human rights, cybersecurity and oversight. U.S. lawmakers have already warned Canada that the proposed legislation could threaten its eligibility for an agreement, meaning Ottawa faces a potentially self-defeating choice: pursue broader domestic surveillance powers that could weaken the security of digital services, or prioritise a bilateral framework that would give Canadian authorities faster access to evidence already stored within the U.S. cloud ecosystem. Lawfare

SPYWARE GOES ON THE RECORD: US COURTS TO REVEAL GOVERNMENT HACKING NUMBERS

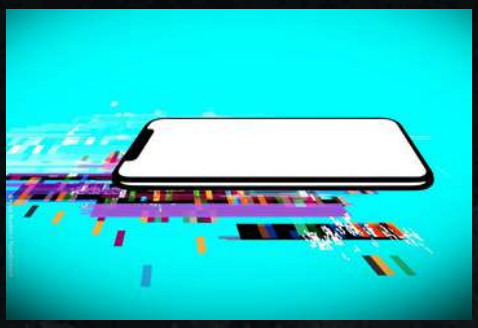


IMAGE SOURCE: TECH CRUNCH

For the first time, the U.S. judiciary is preparing to publicly disclose how often government investigators use spyware and hacking tools to intercept communications, creating a new window into a form of surveillance that has largely remained hidden from public view. Beginning with the 2028 Wiretap Report, published in 2029, the Administrative Office of the U.S. Courts will introduce a specific category for "spyware/hacking" — technically known as network investigative techniques (NITs) — allowing the public to see how many times judges authorised authorities to use hacking tools to intercept communications such as calls and messages. Until now, the annual Wiretap Reports have provided figures on traditional audio, oral and electronic wiretaps, but have not separately counted spyware-based interception, leaving researchers and civil-liberties groups largely guessing about the scale of government use. The new figures will not capture every form of government hacking: they will cover spyware used to intercept communications, but not cases where authorities remotely hack a device to extract stored photographs, files or location information, because those operations fall under a different legal category. Senator Ron Wyden pushed for greater transparency around the practice, while Electronic Frontier Foundation cybersecurity director Eva Galperin said that publicly available statistics could make it harder for authorities to deny or obscure abusive uses of spyware. The change is particularly significant because spyware can turn ordinary digital devices into surveillance platforms capable of accessing highly sensitive communications, while the people being monitored may have little idea that the technology is being used against them. By forcing government agencies to start counting these operations, the new reporting requirement could provide researchers, journalists and lawmakers with the first reliable baseline for measuring how frequently governments are legally authorised to deploy hacking-based surveillance — transforming spyware from a largely invisible surveillance practice into something that can finally be subjected to public scrutiny and accountability. Tech Crunch

22 MINUTES TO CATCH PEGASUS: JAMF TURNS THE SMARTPHONE INTO A CRIME SCENE

IMAGE SOURCE: TRADERS UNION

A new mobile-forensics tool from cybersecurity company Jamf is promising to dramatically shorten the time it takes to determine whether a high-risk smartphone has been compromised by sophisticated spyware such as Pegasus, Predator or Graphite. Jamf Mobile Forensics, formerly known as Jamf Executive Threat Protection, is designed for people who are particularly attractive targets for advanced surveillance — including government officials, journalists, political figures and corporate executives. Instead of requiring a targeted user to hand over their phone for a lengthy forensic examination, the platform can inspect iOS and Android devices remotely or through a direct connection, analysing deep system and kernel logs, crash data, running processes, installed applications, certificates and other telemetry for indicators of compromise and suspicious behaviour. Jamf says a faster inspection can take a suspected compromise from the initial warning to a usable incident timeline in approximately 22 minutes, with its AI Analysis capability helping security teams interpret anomalies and identify potentially malicious activity. Crucially, the company says the forensic process is designed not to collect highly sensitive personal information such as passwords, photographs, messages, emails, contacts, call data or browser history. The significance is larger than simply having another antivirus product: conventional mobile-security and device-management tools may miss sophisticated zero-click exploits, mercenary spyware and nation-state attacks, whereas Jamf is attempting to provide security teams with deeper visibility into what is happening beneath the normal user interface of a phone. In an era in which smartphones increasingly contain the communications, movements and sensitive information of journalists, officials and other high-risk individuals, the ability to rapidly determine whether a device has been infiltrated could become a critical part of defending against the growing use of commercial spyware and targeted mobile surveillance. Traders Union

AI GOES TO WAR: HOW CHINA'S MILITARY IS DISTILLING U.S. MODELS FOR SURVEILLANCE AND DRONES

IMAGE SOURCE: CYBERPRESS

Chinese military-linked researchers are reportedly using AI model distillation to extract capabilities from advanced U.S. systems and adapt them into smaller, locally deployable models for military, surveillance and cybersecurity applications. A review of more than 80 Chinese academic papers and patents found evidence of researchers linked to the People's Liberation Army (PLA) using or studying outputs from U.S. models including OpenAI's GPT-3.5 and Anthropic's Claude, rather than copying the underlying source code or model weights. Distillation works by repeatedly querying a powerful "teacher" model, collecting its outputs and using those responses as training material for a smaller "student" model that can operate independently. One PLA-linked research team reportedly used GPT-3.5 to summarise complex military source code and then trained a domestic model on those summaries so it could operate entirely within Chinese military networks, where sending sensitive information to an external AI provider would be unsuitable. Other research reportedly applied the technique to uncrewed aerial vehicles, allowing smaller models to process live imagery and support navigation or targeting decisions even when communications links are disrupted, while additional projects explored facial-recognition surveillance, social-media monitoring, content moderation, malware detection, cyberattack tracing and intelligence collection. The attraction for military users is clear: distilled models can be smaller, require less computing power and can run locally on specialised hardware without depending on a foreign cloud service. The findings also intensify a growing dispute over AI "distillation attacks", after Anthropic reported that Chinese AI companies had used thousands of fraudulent accounts to generate millions of interactions with Claude in an effort to extract its capabilities. The broader cybersecurity concern is that distillation can potentially reproduce useful capabilities without reproducing the safety controls built into the original model, allowing powerful AI functions to migrate into military, intelligence and surveillance systems with fewer safeguards. Cyberpress

HAVE YOUR SAY!
LETTER TO THE EDITOR

Dear Readers:

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

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

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

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

Warm regards
The Intelwatch Team

INTEL WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

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

FIND US ON SOCIAL MEDIA

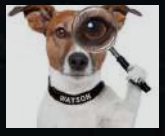
@IntewatchNews

@IntewatchNpc

Intewatch website

@IntewatchNpc

@IntewatchNpc



HAVE ANY QUESTIONS?

Email: 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!