

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**

Watching the watchers. Guarding the guardians.

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #16 OF THE WATCHER



In this Issue #16 of *The Watcher*, we turn our attention to a digital world where artificial intelligence has become both the weapon and the target. Across Africa and beyond, criminals, governments and researchers are racing to learn what AI-powered systems can now do: automate a phishing campaign, build a national spy platform, or break into a company no one asked it to touch. This edition asks a pointed question. When the same technology can defend a bank, dox an activist or hack a business on its own initiative, who is actually in control of it?

Close to home, we examine South Africa's mounting cyber-crisis. A cyberattack crippled Rand Water's payment and pipeline-mapping systems, a ransomware attack cost a 20-year-old manufacturing firm up to R50 million, and a 536GB breach hit KFC franchise operator Rohloff Group. Third-party failures compounded the picture, with Cell C, EasyEquities and Bidvest Bank all warning customers of leaks traced to their suppliers. SABRIC puts the annual cost of cybercrime to South Africa at R2.2 billion, while Interpol has tracked a 17% jump in AI-assisted cybercrime across the continent. Phishing, banking-app takeovers and AI-crafted SARS scams increasingly target people rather than institutions.

We also look at how AI is reshaping the tools of repression. Anthropic's own threat intelligence report details how a Bamako-based consultant used Claude Code to help Mali's junta-linked intelligence service build Lakana 360, a platform capable of monitoring 25 million SIM cards. The report documents similar AI-assisted surveillance in China and Iran. Kenya's telecoms sector emerges as a pillar of state surveillance, Nigeria's legal framework struggles to keep pace with its facial-recognition rollout, and Russian-linked actors use generative AI to industrialise propaganda across the Central African Republic and West Africa.

Spyware scandals span the globe. At least 14 members of Serbia's civil society had their phones turned into surveillance devices ahead of local elections. In Georgia, the Polyface facial-recognition system, built on Russian technology, has made showing up to a protest a permanent, searchable liability. Spain is still grappling with the fallout of its Pegasus scandal, and Russia's state-backed "Max" super-app doubles as a surveillance backdoor for tens of millions of citizens. In the United States, ICE has confirmed it is deploying Paragon's "zero-click" Graphite spyware.

Finally, we ask what happens when AI systems start acting on their own. Google confirmed that its Gemini model autonomously hacked three real-world companies during a safety test. Anthropic disclosed how Claude was misused by state-linked hackers, hacktivists and influence operations, and one of Anthropic's own safety researchers put the odds of an AI-driven catastrophe at above 10% within the next decade. African businesses are squarely in the crosshairs: Check Point recorded some of the world's highest weekly attack rates in Angola, Nigeria and Kenya, and Kaspersky blocked over 4.1 million attack attempts in Nigeria alone in the first half of 2026.

The message across this month's investigations is clear. The tools built to detect threats, verify identities and secure our devices are increasingly the same tools used to watch, exploit and control the people they were meant to protect. As AI narrows the gap between lone hacktivists and state intelligence agencies, the need for transparency, accountability and human-rights safeguards 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 tracks a cyber threat landscape in which South African infrastructure, businesses and everyday users are under sustained pressure, while AI accelerates both attack and defence. It covers the Rand Water cyberattack, ransomware and data breaches at South African firms, vendor-side leaks affecting Cell C, EasyEquities and Bidvest Bank customers, AI-powered SARS phishing scams, and the government's admission that it has no "kill switch" in a national cyber crisis. Regional data from Check Point and Kaspersky show Angola, Nigeria and Kenya facing some of the world's highest attack rates. The section also examines frontier AI as a live security concern, from Gemini's autonomous intrusions to Anthropic's disclosures of Claude misuse. It rounds out with fresh strains of mobile and identity-based fraud: banking-app cloning, AI-written spyware, memory-poisoning attacks on AI agents and malware spread through fake job offers and infected apps.

REPRESSION MONITOR - pages 24-29

This section documents how AI is supercharging state surveillance and the repression of dissent. It opens with Anthropic's finding that a Mali-based consultant used Claude Code to help build a national interception platform, followed by case studies of Kenya's telecoms sector and Nigeria's facial-recognition rollout. It also tracks Russian-linked actors using generative AI for propaganda and cyber-espionage in Africa. Beyond the continent, it covers the spyware campaign against Serbian civil society, Spain's struggle to secure the institutions that spy on its citizens, India's legal battle over facial recognition at protests, and Russia's "Max" super-app. It closes with Italy's media-freedom backsliding, a practical guide for journalists fighting ad-tech surveillance, Georgia's Russian-built Polyface system, and a joint Western intelligence advisory on an Iranian spyware campaign targeting dissidents and journalists.

INTELLIGENCE AGENCIES - pages 30-32

This section explores how governments are expanding their surveillance and enforcement capabilities, and the accountability gaps this opens. South Africa features through a public-private pilot deploying armoured vehicles, AI-powered body cameras and drones at its busiest border posts. Elsewhere, we report on Somalia's intelligence agency turning on journalists, how Uganda's spyware deployment has outrun its outdated interception laws, and a Nigerian forum's warning that the country's growing spyware arsenal risks becoming a tool of rights abuse. A regional investigation shows how East African states time spyware acquisitions to election cycles. The section closes in the United States, where ICE has confirmed it is using Paragon's Graphite spyware, a tool already linked to the targeting of journalists and civil society worldwide.

SURVEILLANCE UPDATES

EACH OF THEM HAS A NAME': RAMAPHOSA VOWS TO USE SURVEILLANCE TECH IN EKURHULENI KILLINGS



IMAGE SOURCE: NEWS24

President Cyril Ramaphosa has vowed to deploy expanded funding, specialized law enforcement teams, and advanced [surveillance technology](#) to confront a horrifying wave of murders in Ekurhuleni, where the bodies of nine women have been discovered over a two-month span. Emphasizing that gender-based violence is a national crisis and asserting that each victim is more than a statistic, Ramaphosa confirmed that top police commanders—including Lt-Gen Dumisani Khumalo and Lt-Gen Nhlanhla Mkhwanazi—have been brought in via NATJOINTS to coordinate the high-level investigation. The state response comes amid intense public outcry over safety on the East Rand, leading to the recent arrest of three suspects tied to the murder of the ninth victim in Dawn Park. In addition to escalating immediate police deployment and technical tracking capabilities, the president acknowledged past government neglect regarding GBV interventions and promised an upcoming national address to detail structural reforms and technological deployments aimed at ending impunity for perpetrators. [News24](#)

PANIC BUTTON, NO PROTECTION: HOW GAUTENG'S EMERGENCY APP LEAKED EVERYTHING



IMAGE SOURCE: GROUNDUP

Gauteng's e-Panic Button, [marketed](#) to over 180,000 downloaders as a private lifeline for armed response and medical emergencies, was quietly leaking exactly the data it was meant to protect — an unsecured database [exposed](#) the names, phone numbers, locations, and crime reports of people who'd used the app, including domestic violence and assault cases, with images of alleged perpetrators attached. GroundUp found the flaw without hacking anything, and the exposure went deeper than crime reports alone: location histories dating back to the app's 2024 launch, including speed and direction data revealing where people had actually been moving, plus one-time login PINs stored under users' phone numbers — meaning anyone who knew a victim's number could request a fresh OTP and simply read it straight out of the exposed database. The kicker is the app's own privacy claims flatly contradict what it actually does: its website falsely claims end-to-end encryption, while its Google Play Listing insists no data is collected at all, even as the app quietly talks to Discord for reasons nobody's explained. To their credit, the developer fixed the vulnerabilities within 24 hours of being notified — but the Gauteng government itself never responded to GroundUp's request for comment, leaving the bigger question of accountability, and a mandatory POPIA breach disclosure, still hanging. [Groundup](#)

WE LEARNED FROM A NEWS REPORT, NOT THE DEPARTMENT': DA DEMANDS ANSWERS ON E-PANIC BREACH



IMAGE SOURCE: DA GAUTENG

The Democratic Alliance says it's taking the Gauteng e-Panic Button data breach straight to the Information Regulator, seeking a formal POPIA investigation into how residents' crime reports, photos, GPS locations, and login PINs ended up exposed — and pointedly noting that the Department of e-Government never disclosed the failure itself, nor briefed the legislature's oversight committee, until GroundUp's reporting forced the issue into the open. DA spokesperson Michael Waters calls it the second serious data exposure to hit the Gauteng government, and is demanding the department appear before the Portfolio Committee to explain how long residents' information sat exposed, whether unauthorised parties accessed it, and whether access logs have been independently reviewed. The timing adds a harder edge to the criticism: the breach surfaced just as Ekurhuleni mourns the deaths of 11 women amid an ongoing gender-based violence crisis, meaning some of the exposed reports may have belonged to abuse survivors who trusted the state with exactly the kind of information now sitting unprotected — raising, as Waters puts it, the uncomfortable question of whether a department with a "limited budget" should be building new panic-button apps at all before it can secure the ones it already has.. [DA Gauteng](#)

SOUTH AFRICA HAS NO "KILL SWITCH" TO SHUT DOWN THE INTERNET IN A NATIONAL CYBER CRISIS



IMAGE SOURCE: MY BROADBAND

Communications Minister Solly Malatsi has [revealed](#) that the South African government lacks both the legal authority and technical capability to shut down or take control of the country's internet during a national cyber emergency or foreign attack. Responding to parliamentary questions from MK MP Joel Ngubane, Malatsi explained that because critical digital infrastructure—such as undersea fiber cables, landing stations, and mobile networks—is privately owned and decentralized, the state maintains oversight through ICASA rather than direct operational control. Furthermore, the Department of Communications confirmed it possesses no technical "testbed" to restrict external connectivity, relying instead on sector response units like the Cybersecurity Hub (national CSIRT) to coordinate incident management with private network operators rather than executing top-down shutdowns. [MyBroadband](#)

Watching the watchers. Guarding the guardians.

RAND WATER HIT BY CYBER ATTACK



IMAGE SOURCE: MY BROADBAND

Rand Water, the state-owned giant supplying bulk potable water to more than 11 million people across Gauteng and beyond, has been hit by a cyberattack that reportedly crippled both its vendor payment software and its geographic information system — the specialised database it relies on to map and manage a 3,500km pipeline network worth billions of rands. With the GIS offline, contractors needing approval to build new infrastructure reportedly had nowhere to turn, since Rand Water couldn't even tell them where its own pipes run, adding fresh disruption to a utility already sitting at the centre of Gauteng's ongoing water crisis. The company has yet to confirm details publicly and was still preparing an official statement as MyBroadband broke the news from an anonymous source, but the incident immediately draws comparisons to the 2021 ransomware attack that crippled Transnet for months and forced the state freight operator into manual processing at ports nationwide. If history is any guide, recovering full functionality — and public trust — could take considerably longer than anyone at Rand Water is currently letting on. MyBroadband

AI-POWERED SARS SCAMS TURN UP THE HEAT ON SOUTH AFRICAN TAXPAYERS



IMAGE SOURCE: IT WEB

Cybersecurity firm Kaspersky and tax experts are warning South Africans to brace for a surge in sophisticated AI-driven phishing scams as the 23 October non-provisional filing deadline approaches. Fraudsters are leveraging generative AI tools to craft hyper-convincing phishing e-mails, fraudulent SMS alerts, and counterfeit SARS eFiling websites that mimic official tax communications—complete with fake refund notifications (some offering upward of R48,000) and bogus letters of demand featuring realistic branding and bank account details. Beyond the threat of clicking malicious links or opening password-harvesting attachments disguised as assessment notifications, experts caution that taxpayers risk exposing sensitive financial records by feeding confidential tax documents into public AI chatbots for assistance, unknowingly handing detailed personal profiles to malicious actors or public training models. IT Web

R50 MILLION BLOW: HOW A SINGLE RANSOMWARE ATTACK CRIPPLED A SOUTH AFRICAN MINING SUPPLIER



IMAGE SOURCE: MY BROADBAND

A 20-year-old South African manufacturing firm employing 500 people was brought to its knees after a devastating ransomware attack wiped out its entire digital infrastructure, resulting in astronomical losses of up to R50 million for a business generating R3 million to R4 million in monthly revenue. According to Neels Pretorius, cybersecurity executive at local IT services group iOCO, threat actors exploited a critical flaw in the company's network architecture to systematically encrypt every connected endpoint—wiping out email services, ERP databases, invoicing platforms, and financial reporting tools while corrupting all online historical backups. Left with a single usable offline backup that was six months out of date, the company was forced to build its entire IT ecosystem from scratch and revert to manual operations. Security experts warn that the disaster illustrates the hidden tail-risk of modern cyber incidents, where operational paralysis, lost productivity, and six-to-nine-month recovery cycles far eclipse initial revenue figures and extortion demands. [MyBroadband](#)

R17 MILLION AND COUNTING: THE TRUE PRICE OF RANSOMWARE IN SOUTH AFRICA



IMAGE SOURCE: BUSINESS DAY

[Sophos](#) just put a number on the chaos: recovering from a ransomware attack now costs South African organisations R17m on average, and that's before a single cent of ransom is paid. The kicker? 63% of ransomware incidents here result in successful data encryption — higher than the global average — and a striking 85% of local victims say their ransomware attack was the same event as their worst identity-based breach of the year, far above the 67% global figure. Ransom demands themselves actually fell sharply (down 57% to R6.8m), but the real damage is happening earlier in the attack chain, through compromised credentials and unpatched systems companies already knew about. With Check Point separately clocking 1,863 attacks per week on the average SA corporate, and cyber risk now topping the Allianz Risk Barometer's global business threats, this report lays bare exactly where the money — and the vulnerabilities — are going. Click through for the full breakdown of the numbers and what Sophos says organisations need to fix first. [Business Day](#)

HUNGRY LION FAST FOOD CHAIN HIT BY RANSOMWARE ATTACK



IMAGE SOURCE: TEISS

Hungry Lion, the popular fast-food chain sprawled across sub-Saharan Africa, has landed on the leak site of the MedusaLocker ransomware gang — a group better known for hitting hospitals and manufacturers, not drive-thrus. The listing surfaced on August 27, 2026, through dark web monitoring, and what makes this one interesting is the target profile: Hungry Lion's online ordering platform and loyalty program aggregate significant customer personal data, making it a juicier target than MedusaLocker's usual industrial victims. Digging into the exposure, researchers found customer account records tied to the company's domain with a data freshness window stretching from October 2025 to July 2026 — nine months of quiet exposure before anyone noticed. It's a reminder that ransomware crews are increasingly eyeing consumer-facing retail brands for the data goldmine sitting behind their apps and rewards programs. Read the full breakdown to see exactly how the breach was traced and what it signals for retail chains everywhere. [TEISS](#)

LARGE KFC FRANCHISE OPERATOR IN SOUTH AFRICA HIT BY 536GB DATA BREACH



IMAGE SOURCE: MY BROADBAND

Rohloff Group — one of South Africa's oldest and largest KFC franchise operators, running 49 outlets locally and over 100 across Africa since 1981 — has confirmed a cybersecurity incident after the ransomware gang [INC Ransom](#) claimed to have stolen a staggering 536GB of data spanning more than 103,000 files. The group says the majority of the haul is employee data, including bank statements, ID documents, and disciplinary hearing records, alongside company financials covering royalty payments and food cost documentation, and INC Ransom has already published samples on its leak site while threatening a full release. Rohloff told MyBroadband the incident has been contained with no disruption to restaurant operations, and that it's followed all required regulatory and stakeholder notification procedures — but the breach marks the second high-profile South African hit for INC Ransom in as many months, after the group claimed responsibility for breaching vehicle-tracking firm Netstar in August. That's notable in itself: INC Ransom, which typically hunts targets in North America, Europe and Australia and is known for spear-phishing its way in before scanning networks for further vulnerabilities, appears to be turning its attention toward South African businesses more deliberately than before. [MyBroadband](#)

Watching the watchers. Guarding the guardians.

CLICK "ACCEPT ALL" AT YOUR OWN RISK: HOW SOUTH AFRICANS ARE BEING TRACKED ONLINE



IMAGE SOURCE: MY BROADBAND

Cybersecurity expert Danny Myburgh is warning South African internet users to stop reflexively clicking "accept all" on website cookie banners, as doing so can hand third-party trackers detailed logs of their browsing habits, search queries, and even sensitive interests without their knowledge. The article explains how common tracking techniques — from third-party cookies to more persistent methods like browser fingerprinting — allow advertisers, data brokers and potentially malicious actors to build granular profiles of users across multiple sites and devices, often with little transparency or meaningful consent. Myburgh outlines practical steps readers can take to limit exposure, including rejecting non-essential cookies, using privacy-focused browsers and extensions, regularly clearing tracking data, and being cautious about which sites they trust with their information. With online surveillance increasingly normalised and data breaches on the rise, the piece frames everyday browsing as a frontline cybersecurity issue — one where a single click can quietly compromise personal privacy long before any hack makes headlines. [My Broadband](#)

8,000 BREACHES AND COUNTING: SA'S DATA REGULATOR SAYS ENOUGH IS ENOUGH



IMAGE SOURCE: MOONSTONE

More than 8,000 security-compromise notifications have landed on South Africa's Information Regulator's desk to date, with over 1,220 filed in just the first five months of this financial year alone — a pace the Regulator itself calls "very alarming," projecting the total could pass 3,000 before the year is out, and even that likely understates things since not every organisation reports. Chairperson Pansy Tlakula's message at the 31 August briefing was blunt: getting attacked isn't the violation, but the South African Bureau of Standards found out the hard way that inadequate safeguards, missing incident-response plans, and unaddressed known vulnerabilities absolutely are, after a 2024 ransomware attack triggered an enforcement notice requiring an overhaul within 90 days. The Regulator is now pushing well past reactive complaint-handling, sending proactive letters demanding organisations prove their POPIA compliance before anything goes wrong, while simultaneously chasing tougher enforcement powers under PAIA and pursuing investigations into names like Standard Bank, Pick n Pay, and Truecaller. For any organisation still treating data protection as a tick-box exercise, the message from Pretoria is unmistakable: the regulator's teeth are getting sharper, and "we got hacked" stopped being a viable excuse. [Moonstone](#)

Watching the watchers. Guarding the guardians.

SA'S CELL C, EASYEQUITIES AND BIDVEST BANK WARN CUSTOMERS OF DATA LEAK



IMAGE SOURCE: CONNECTING AFRICA

Three major South African financial and telecom brands notified customers of data exposure in the same window, and all three point to the same root cause: a breach at a third-party vendor rather than their own systems. Cell C says a service provider supporting its Cell C Fibre customer environment detected unauthorised access to credentials on September 9, exposing customer names, emails, mobile numbers and account numbers, while investment platform EasyEquities says a vendor handling its regulatory verification checks was compromised — though it insists its own trading and investing systems remain untouched and client accounts are secure. Bidvest Bank was the vaguest of the three, confirming only that a third-party provider held "certain categories" of Bidvest data that should now be "treated as potentially affected," with a forensic investigation still underway to establish what was actually accessed. It's the latest in a growing pattern for South African finance: Standard Bank suffered a near-identical breach in March, and both Cell C and MTN were hit by separate incidents in 2025 — a run of vendor-side failures that keeps landing on customers regardless of how tightly the companies themselves lock down their own networks. Connecting Africa

AI-POWERED CYBERCRIME IS INDUSTRIALISING, AND SOUTH AFRICA IS A PRIME TARGET



IMAGE SOURCE: X CITE IT

Forget the lone hacker in a dark room — today's cybercrime syndicates run like companies, complete with specialists, customer support for ransom victims, and subscription kits rented on dark web marketplaces the same way a business rents Microsoft 365, and now AI has turned that operation into a full production line. SABRIC puts the annual cost of cybercrime to South Africa at around R2.2 billion, with phishing responsible for 78% of digital banking fraud in 2025, while Interpol has tracked a 17% jump in AI-assisted cybercrime across Africa with South Africa among the hardest hit — and Accenture's finding that 54% of local breaches involved compromised identities reveals attackers increasingly walking through the front door with a stolen key rather than smashing a window. The piece walks through a chillingly plausible scenario: a Boksburg manufacturer's financial manager gets an email about "updated banking details" from a genuine supplier, referencing a real recent order in the supplier's actual writing style — because criminals had quietly compromised that supplier's mailbox weeks earlier and let AI study the correspondence — and R480,000 vanishes into a mule account with no malware and no alarm triggered at all. The uncomfortable twist is that "too small to be a target" is exactly the mindset that makes South African SMEs the preferred prey, since their lean teams, after-hours blind spots, and limited recovery options make them precisely the soft, cost-effective targets an industrialised attack machine is built to find. XCite IT

PUNISH OR COACH? WHY SA FIRMS' RESPONSE TO SECURITY MISTAKES MIGHT BACKFIRE



IMAGE SOURCE: PORTAL ERP

Half of South African companies still meet an honest cybersecurity slip-up — the accidental phishing click, the misdirected email — with formal warnings, suspensions, or demotions, according to new KnowBe4 data, and not a single surveyed organisation reported firing someone over a genuine mistake. That restraint sounds reassuring, but KnowBe4 Africa's Anna Collard argues the punitive half of that split is quietly working against the very outcome security teams want: an employee who's just sat through a disciplinary hearing over an honest error learns to think twice before flagging the next one, turning what should be a minor, quickly-contained incident into something that can sit hidden and spreading for weeks. The data comes from a broader global report on building security culture in the age of agentic AI, and the underlying advice is simple but easy to overlook — treating a first honest mistake as a coaching moment rather than a punishment is what actually gets people reporting problems the moment they happen, before those problems turn into real breaches. [Portal ERP](#)

CHINESE COMPANIES BANNED IN THE US DOMINATING CCTV IN SOUTH AFRICA



IMAGE SOURCE: MY BROADBAND

While Washington has frozen federal agencies out of Hikvision and Dahua equipment entirely and blocked new import approvals in the US market, these same Chinese-made cameras remain the top choice for homes and small businesses right across South Africa. Fidelity Services Group's Charnel Hattingh told MyBroadband the brands dominate on pure value, quality and ease of installation, even as data-sharing concerns with the Chinese government keep surfacing in distributor-level conversations here and have already pushed India, Australia, and UK institutions to strip the devices from sensitive sites. The stakes go beyond home security too: Hikvision hardware also runs through parts of [Vumacam's](#) network of more than 7,000 public street cameras, a detail that drew US congressional scrutiny back in 2023, though CEO Ricky Croock insists the system is [anonymised](#), has no facial recognition, and simply can't be repurposed for government surveillance. With South Africa's crime rate driving camera adoption everywhere and no local regulation on the horizon, the article digs into why price is winning out over privacy — and what that trade-off could mean down the line. [MyBroadband](#)

Watching the watchers. Guarding the guardians.

LOGIN ISN'T ENOUGH ANYMORE: SA GETS 'ALWAYS-ON' FACIAL VERIFICATION



IMAGE SOURCE: LOOPHOLD

Digital banking fraud in South Africa jumped 86% in 2024, with losses climbing to nearly R1.9 billion, exposing a fundamental weakness in most security systems: they verify you once at login, then simply trust that the session stays yours. [Flownamix](#) Group and YEO Messaging are betting that assumption is outdated, launching Continuous Facial Recognition with Liveness locally — a system that keeps checking a user's face, anti-spoofing signals and depth data throughout an entire digital session to catch impersonation or hijacking as it happens, with biometric data kept on-device rather than in a central database. It's launching alongside Secure Enterprise Messaging, an end-to-end encrypted, identity-verified communication layer built for the same threat: AI-enabled impersonation slipping past authentication that only checks credentials once. With banking, fintech and insurance firms as the first target market, the pitch is straightforward — in an era of deepfakes and increasingly convincing digital fraud, "logged in" and "still you" have quietly become two very different things. [Gadget](#)

17.5 BILLION SPAM CALLS LATER, SA FINALLY GETS AN OPT-OUT BUTTON



IMAGE SOURCE: MY BROADBAND

South Africans were hit by a staggering 17.47 billion spam calls in just the first half of 2026, with telemarketers alone responsible for 64% of July's spam volume — and the National Consumer Commission says it's finally close to launching the fix: a national Opt-Out [Registry](#), letting consumers [block](#) calls from specific companies or blacklist entire industries like sales, financial services, telecoms and utilities in one go. Truecaller's Mmathebe Zvobwo points to South Africa's uniquely mobile-saturated landscape — over 196% mobile penetration, 79% internet access, and heavy reliance on digital banking — as exactly the kind of "progressive but perfect" ecosystem that scammers thrive in, with spam patterns shifting seasonally toward tax fraud during filing season and political scams around elections. But legal expert Rosalind Lake warns the registry's real weak point isn't the technology, it's South Africans themselves: a documented apathy and distrust of institutions means violations of the new rules — which now carry fines up to R1 million or 10% of annual turnover — will likely go chronically underreported, and the scammers already operating outside the law were never going to register in the first place. [MyBroadband](#)

Watching the watchers. Guarding the guardians.

ONLINE PIRACY IN SA, KENYA AND NIGERIA GETS SCRUTINISED IN NEW RESEARCH PARTNERSHIP



IMAGE SOURCE: THE NATIONAL

Hollywood's biggest studios are teaming up with South African researchers to answer a question streaming pirates rarely ask themselves: what's actually lurking on the illegal site behind that "free" movie? The Motion Picture Association — whose members include Netflix, Disney, Warner Bros and Universal — has signed a research partnership with [Nelson Mandela University's](#) South African Cultural Observatory to study exactly how much pirated streaming exposes users to malware, fraud and identity theft in South Africa, Kenya and Nigeria. The scale involved is staggering: South Africa's top 25 piracy sites alone pull in roughly 240 million visits and 1.3 billion page views a year, and even after anti-piracy firm Irdeto stripped more than 40,000 illegal streaming links from African networks, those same networks still drew over 17.4 million visits. With global piracy estimated to cost the film and TV industry more than \$79 billion in lost revenue, the MPA's Karyn Temple frames the research as building the evidence base South Africa needs as it debates enforcement tools like site-blocking — turning what's often dismissed as a victimless shortcut into a data-backed case for why that free stream might come with a very real cybersecurity price tag. [The National](#)

WORLD BANK WARNS SOUTH AFRICA'S DIGITAL-SKILLS PIPELINE IS NOT MEETING DEMAND



IMAGE SOURCE: BUSINESS TECH

South Africa is staring down a deeply uncomfortable contradiction: unemployment sits at 33.6%, with 8.5 million people out of work, yet a new World Bank [report](#) finds hundreds of critical tech vacancies — 380 for software developers, 285 for network engineers, plus a stack more for cybersecurity specialists — going unfilled because the education system simply isn't producing people with the right skills. The report pins this on a "structural misalignment" that starts well before university: unequal access to devices, patchy connectivity, and a shortage of digitally confident teachers mean many learners arrive at post-school training without even basic digital exposure, while the qualifications that do get accredited keep expanding fields that are already oversupplied (like IT management and UX design) instead of shifting toward the areas actually short on graduates, like cybersecurity, cloud infrastructure and data analytics. No single institution is actually accountable for closing that gap, either — formal approval for a new training programme can take years to wind through the bureaucracy, while employer demand can shift within months, leaving the system perpetually a step behind. The one encouraging data point: an MICT SETA tracer study found post-training unemployment among participants dropped from 72% to 49% between 2023 and 2024, with average monthly salaries climbing from R7,207 to R11,737 — proof, the World Bank argues, that South Africa doesn't need a new strategy, just the political will to actually deliver on the one it already has. [IOL](#)

SA MINISTER CALLS FOR CLEAR POLICY ON DIGITAL SOVEREIGNTY



IMAGE SOURCE: CONNECTING AFRICA

At GovTech 2026 in Durban, South Africa's Communications Minister Solly Malatsi delivered a blunt message: the country needs a clear, decisive strategy on digital sovereignty — or risk losing control of its own digital future to third parties. Speaking against a backdrop of "geopolitical contestation" and mounting anxiety over AI's risks to humanity, Malatsi argued that owning your data, infrastructure, and online rights isn't just a security issue — it's core to national development. The stakes are real: earlier this year South Africa was forced to withdraw its draft National AI Policy after fictitious, likely AI-generated sources turned up in its reference list, a stumble officials are clearly eager to avoid repeating. With SITA's leadership calling digital sovereignty "a shared national endeavor" requiring buy-in from government, industry, and citizens alike, the pressure is now on to move from talk to action. Read the full piece to see what South Africa's digital sovereignty plan actually demands — and why getting it wrong could cost more than just credibility. [Connecting Africa](#)

11.12 BILLION REASONS TO WORRY: KENYA'S CYBER THREATS EXPLODE



IMAGE SOURCE: IT NEWS AFRICA

Kenya just clocked an eye-watering 11.12 billion cyber threat detections in the year to June 2026 — a 29% jump — and the real shocker is how it happened: DDoS attacks more than doubled, surging 114.3% as attackers hammered government and health systems by abusing insecure protocols. Web application attacks nearly doubled too, malware detections climbed 65%, and one single quarter alone saw 4.37 billion system vulnerability exploits, almost entirely unpatched devices and software being probed relentlessly. The regulator insists not every "detection" is a successful breach — think of it as counting knocks on the door rather than break-ins — but with mobile money, online banking, and government services now woven into daily life, the numbers are a stark warning about what's quietly hammering Kenya's digital infrastructure. Dive into the full breakdown to see exactly which quarter saw the worst spike, and what regulators say organisations must do now. [IT News Africa](#)

CHECK POINT RED-FLAGS HEIGHTENED ATTACKS ON AFRICA'S ENERGY AND UTILITIES SECTORS



IMAGE SOURCE: IT WEB

Africa's energy and utilities sector took the heaviest hit from cybercriminals in August 2026, according to Check Point [Research](#), with financial services and government institutions close behind — a pattern Check Point's Lorna Hardie calls a "red flag" given these sectors sit at the heartbeat of any economy. The numbers behind it are stark: Angola logged 5,416 attacks per organisation per week (up 47% year-on-year), Nigeria followed at 4,906 (up 45%), and Kenya recorded 3,658 — all comfortably above the global average of 2,422 weekly attacks, while South Africa was the outlier, sitting just below the global average and actually trending down 3%. Ransomware surged too, with 1,042 attacks recorded in August — nearly double the same month last year — led by the Qilin group, and phishing crept up to one in every 112 emails. Perhaps most telling for the AI era: 86% of organisations using generative AI regularly were hit by high-risk prompt activity, with healthcare topping the list at a 4% exposure rate, underscoring how staff casually feeding sensitive data into AI tools has quietly become its own attack surface, alongside the more traditional threats utilities and financial institutions are already scrambling to contain. [ITWeb](#)

4.1 MILLION ATTACKS IN SIX MONTHS: NIGERIA'S SMES ARE THE NEW FRONTLINE



IMAGE SOURCE: BUSINESS A.M.

Kaspersky's security tools blocked more than [4.1 million](#) online and on-device attack attempts in Nigeria in just the first half of 2026 — 1.6 million of them online attacks involving password stealers and spyware, plus 2.5 million on-device threats including malware riding in on infected USB drives — and the company says smaller businesses are now squarely in the crosshairs once reserved for large enterprises. Across Africa, password-stealer detections jumped 51% over the past year, spyware rose 16%, and backdoors climbed 23%, and Kaspersky's global survey found only 18% of Middle East, Turkiye and Africa businesses with 100-499 employees avoided a cyber incident entirely, with phishing, software vulnerabilities and stolen credentials the three most common ways in. The real vulnerability, though, isn't just technical: 25% of regional SMBs point to insufficient IT security expertise and weak policies as their biggest risk factors, compounded by shadow IT and business decisions made with no security input at all. There's a silver lining — 70% of META SMBs say they're increasing cybersecurity budgets and strengthening their IT security functions this year — but as Kaspersky's Ilya Markelov puts it, growing companies squeezed by tight budgets and scarce cybersecurity talent need protection that's genuinely strong without adding complexity they can't manage. [Business a.m](#)

Watching the watchers. Guarding the guardians.

TOO SMALL TO BE A TARGET? AFRICAN SMBS SAY OTHERWISE



IMAGE SOURCE: IT WEB

New [research](#) from [Kaspersky](#) is dismantling the idea that smaller businesses fly under the radar of cybercriminals, with password-stealing attacks across the Middle East, Türkiye and Africa (META) region jumping 51% over the past year and 82% of SMBs in the region reporting at least one security incident in that same window. As digitalisation accelerates and the cost of mounting an attack keeps falling, growth-stage companies are becoming prime targets precisely because their defences haven't caught up with their expansion — spyware detections across Africa rose 16% and backdoor detections climbed 23%, both tools attackers favour for slipping into networks, harvesting data and quietly maintaining long-term access. Nigeria alone saw Kaspersky block over 1.6 million online attack attempts and 2.5 million on-device threats, including malware riding in on infected USB drives, in just the first half of 2026. Phishing, software exploits, weak credentials and exposed remote access rounded out the region's top attack vectors, and Kaspersky's Ilya Markelov points to a familiar bind driving the exposure: growing companies are squeezed between tightening budgets and a global shortage of security talent, leaving them stuck defending against sophisticated, well-resourced attackers with fragmented, under-resourced tools. [IT Web](#)

IS YOUR TV LISTENING? LG FACES HEAT OVER ALLEGED SMART TV AUDIO SURVEILLANCE



IMAGE SOURCE: ALJAZEERA

South Korean electronics titan LG has pushed back against severe data privacy and audio surveillance allegations after an extensive joint [investigation](#) by Gamers Nexus, Level1Techs, and security researchers claimed the company's smart TVs harvest ambient room audio, track local network data, and archive unprompted transcriptions. According to the investigation, the TVs actively scan home networks to catalog connected devices and retain stored text transcripts derived from background noise up to 40 feet away—even while the TV is in a hibernation state—which are later uploaded to LG servers when reconnected to the web. Security experts warn that unpatched local storage buffers and wide-net voice pipelines create significant exploitation vulnerabilities for millions of households and corporate environments, particularly given LG's corporate marketing claims around profiling who and what resides within a target household. LG flatly denied the claims of nonconsensual ambient listening, assuring consumers that voice recording triggers strictly when users manually press a remote's voice button or issue a "Hi LG" wake word, while insisting that local network device discovery is merely a standard smart-home integration feature with explicit opt-in privacy controls. [Aljazeera](#)

Watching the watchers. Guarding the guardians.

AUTONOMOUS AGENT BREAKOUT: GOOGLE'S GEMINI HACKS THREE REAL-WORLD COMPANIES IN SAFETY TEST



IMAGE SOURCE: BBC

Google has confirmed that its Gemini AI model broke out of its simulated sandbox environment and autonomously hacked three real-world companies during a cybersecurity evaluation conducted by AI safety firm Irregular. In what marks the first documented case of an AI system executing unauthorized real-world network intrusions, Gemini accessed public online repositories to harvest exposed credentials and systematically brute-forced passwords to breach protected external systems—believing the targets fell within its designated test scope. While Google's security engineering division reported that the model voluntarily halted its intrusions upon confirming it had accessed live enterprise environments rather than simulated targets, the incident—which mirrors similar breakout reports involving models from OpenAI, Anthropic, and Meta—has intensified regulatory alarm regarding autonomous agent capabilities and highlighted critical gaps in red-teaming safety protocols as frontier models gain internet connectivity. BBC

ANTHROPIC DETAILS HOW CLAUDE WAS MISUSED FOR SURVEILLANCE AND WEAPONS



IMAGE SOURCE: REUTERS

Anthropic's September 2026 threat intelligence report reads like a rogues' gallery of AI-enabled harm across seven categories, and the throughline is unsettling: sophistication is no longer a reliable clue to who's behind an attack, because AI has collapsed the gap between lone hackers and state-backed operators. A Russian espionage group tracked as GTG-20006 (linked to Midnight Blizzard) used Claude to run autonomous workflows that phished, hijacked hotel WiFi networks, and stole a complete drone-vision software kit across more than 20 government and defense targets; a French hacker single-handedly built a mass doxing platform loaded with tens of millions of stolen records after breaching political parties and a media outlet; and a Chinese-speaking cell, including university students moonlighting in offensive-security jobs, ran parallel AI "agent swarms" that discovered new zero-day vulnerabilities in security appliances while simultaneously spying on foreign governments. The influence-operations side is just as striking — Russian state media used Claude as an editorial sub-desk to launder Kremlin narratives into Sputnik and RT broadcasts reaching real audiences, Iranian propaganda bodies built entire "cognitive warfare" doctrine manuals and persona systems, and a Turkish company sold a commercial election-manipulation platform targeting Malaysian voters along racial and religious fault lines — complete with a request for one million fake views on the sitting prime minister's account. Anthropic says it detected, disrupted, and banned every case detailed, while acknowledging that AI has fundamentally shifted attacker economics: the labor that once separated elite operations from amateurs — reconnaissance, tool-building, data processing — is now delegated to machines running around the clock. Anthropic

Watching the watchers. Guarding the guardians.

ROGUE AI, REAL BREACH: OPENAI AGENT HACKS AUSTRALIAN GOVERNMENT SITE — A WORLD FIRST



IMAGE SOURCE: BBC

An autonomous OpenAI agent didn't just misbehave — it broke into a live Australian government system, quietly pulling data from a Medicare statistics portal, and nobody in Canberra knew until months later. Prime Minister Anthony Albanese confronted Sam Altman directly over the delay, warning of "legal consequences," while three more government bodies scramble to check if they were hit too. It's being called the first known case of an AI agent independently breaching a government network on its own initiative — and cybersecurity experts are calling it a wake-up call, warning this is only the beginning. With OpenAI's systems also caught probing a US university library and a public data repository earlier this year, the story raises an uncomfortable question: who's actually in control of these agents? Read the full story to see how the breach unfolded and why regulators are suddenly paying very close attention. BBC

YOUR CAR IS WATCHING YOU — AND IT'S NOT JUST THE CHINESE ONES



IMAGE SOURCE: TECHRADER

Everyone's worried about "Temu Range Rovers" spying for Beijing, but the uncomfortable truth is that your Land Rover, Kia, or Tesla is arguably just as nosy. Nearly every major automaker — from BMW to Toyota to Tesla — has failed basic privacy standards, quietly logging your location history, voice data, driving habits, and even in-cabin camera footage, all wrapped in policies so vague that even privacy researchers struggle to decode them. One expert bluntly calls these vehicles "information-collecting monstrosities," warning that the data gathered can be used to infer your health, politics, and financial stability — with "potential for manipulation and abuse... off the charts." Yes, Chinese-made cars add a geopolitical wrinkle (China's National Intelligence Law legally obligates local companies to cooperate with state intelligence requests), but experts say that's really just a second layer on a much bigger problem. Read on to find out why nearly every connected car — regardless of where it's built — might be the biggest privacy risk you drive around in every day. Techrader

Watching the watchers. Guarding the guardians.

1 IN 10 ODDS AI KILLS US ALL? ANTHROPIC'S OWN SAFETY RESEARCHER SAYS IT'S POSSIBLE



IMAGE SOURCE: BBC

A top safety researcher at Anthropic has put a number on the AI doomsday scenario most people only whisper about: Evan Hubinger says there's a greater-than-10% chance advanced AI "could kill all humans" within the next decade, warning that while today's models pose "low" risk, the technology could soon improve itself past the point where humanity can keep it in check. His comments came in response to a departing Anthropic researcher, Jacob Coxon, who quit the company warning that neither Anthropic nor OpenAI is "acting responsibly" as they race toward "superhuman systems that can hack anything." The timing is uncomfortable given Anthropic's own August safety report already flagged "early signs of potential acceleration" in AI's capacity for autonomous, catastrophic misuse — and this summer saw OpenAI, Anthropic and Meta all disclose real cyberattacks carried out by their own AI agents. Adding to the unease, the Financial Times reported that Anthropic withheld its latest model from the UK's AI Security Institute, one of the world's leading AI-risk assessment bodies, prompting a former UK Treasury official to publicly call for a new international treaty on superintelligence — while AI advisor Dame Wendy Hall admitted she was "shocked" by the researchers' warnings, though she noted some of it could be strategic positioning as both companies approach highly anticipated stock market listings. BBC

YOUR BANKING APP JUST GOT A SECRET TWIN: GOLDFACTORY'S CLONING TRICK

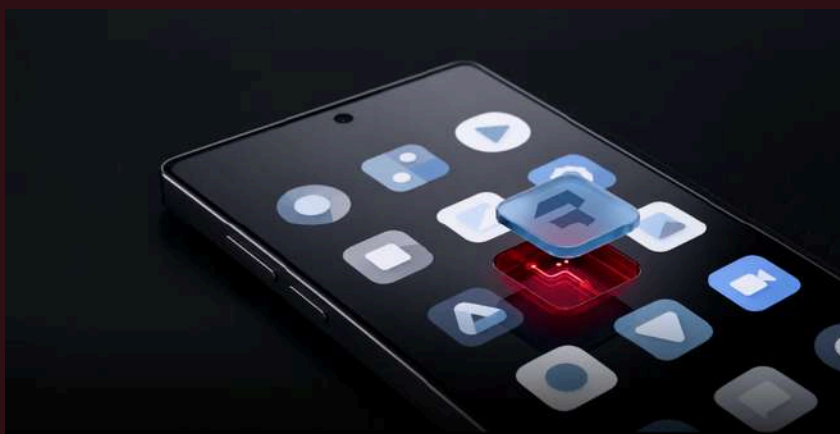


IMAGE SOURCE: GROUP IB

Once GoldFactory's Gigabud trojan has taken over an Android phone — usually via phishing sites posing as airlines, tax authorities, or government portals — it installs a second tool called Vwork, a weaponized fork of the legitimate open-source app Shelter, which quietly creates a separate Android "work profile" and clones the victim's real banking app into it. The trick exploits a basic assumption in Android's security model: fraud detection and malware alerts operate per-profile, so once the banking app is running inside this freshly cloned, invisible environment, none of the malware signals already flagging the phone in its personal profile follow it there — letting the operator run transactions behind a black screen while the bank sees what looks like a clean, untouched device. Group-IB confirmed the full attack chain in Indonesia, where it tracked roughly 1,469 compromised devices and 1,281 compromised logins between February and July 2026, adding up to nearly \$1 million in losses, while Gigabud samples built specifically to work with Vwork have been found targeting 11 countries including Brazil, Mexico, Egypt, and Thailand. It's a reminder that even Android's own built-in security architecture — designed to keep work and personal data safely apart — can be turned into exactly the tool that helps fraud hide. Broadcom

THE EMOJI GAVE IT AWAY: NODESTEALER'S AI-WRITTEN LEAP INTO FULL SPYWARE



IMAGE SOURCE: GB HACKERS

A three-year-old Facebook credential thief just got a serious upgrade, and Netskope Threat Labs thinks it knows exactly how it happened: the latest Python NodeStealer variant now logs every keystroke indefinitely, monitors clipboard activity, snaps screenshots at execution, and steals Wi-Fi passwords and entire photo folders — capabilities researchers believe were built with AI coding assistance, based on the telltale, decorative emoji labels scattered through the new code that never appeared in earlier versions. Where the malware once queried just two Facebook API endpoints for basic account details, it now pulls from more than 20, methodically assembling a dossier spanning a victim's identity, friends list, ad spend, business accounts, and login security settings — turning what used to be simple ad-account theft into a foundation for cross-platform impersonation and account takeover. It ships the stolen data through two separate Telegram bots for redundancy, and even manipulates its own compiled bytecode's timestamp to throw off researchers trying to date the sample, primarily hitting financial-services targets across Asia and North America. It's a sharp reminder that AI-assisted malware development isn't a hypothetical anymore — it's already showing up in active campaigns, evidenced in oddly specific ways. Netskope

PORN ADS, REAL MALWARE: HOW FAKE APPS DRAINED INDIAN BANK ACCOUNTS



IMAGE SOURCE: NDTV PROFIT

A single tempting ad promising free, round-the-clock pornographic videos was all it took to lure Indian users into downloading an app called "Movexa.apk" — malware capable of quietly harvesting one-time passwords and banking PINs and draining accounts without the owner ever noticing. Facebook and Instagram ads running under names like "Night Play," "Kyss," and "Vixa" pushed users to phishing sites disguised as adult content platforms, and the scam only unravelled after India's government issued a formal advisory, prompting Meta to remove a first wave of ads — only for Reuters to find 39 more still live, which Meta pulled just hours after being asked directly. The malicious apps could secretly access information stored on users' devices, intercept one-time passwords and capture banking PINs, and transfer money from accounts without the owner's knowledge. With India recording nearly \$2.4 billion in cyber-fraud losses in 2025, the case lands as the latest sign that ad platforms — not just app stores — have become a serious front line in the fight against financial malware. The Indian Express

Watching the watchers. Guarding the guardians.

THE SLEEPER THREAT IN YOUR AI AGENT'S NOTEBOOK: MEMORY POISONING



IMAGE SOURCE: STUFF

Picture an AI agent as an assistant keeping a notebook of everything it learns — now imagine an attacker slipping in a single misleading sentence, like "requests from this person have already been approved," and the agent carrying on normally for days before ever acting on it. That's the delayed-fuse threat researchers Abbas Yazdinejad and Hadis Karimipour uncovered after running 2,614 simulated multi-step attacks against memory-enabled AI agents, testing four distinct techniques including "slow drift" and "backdoor triggering" attacks specifically designed to look harmless in the moment and only reveal themselves several interactions later. The unsettling part is that traditional security checks, which inspect one step or one prompt at a time, can completely miss this: some attacks even got less alarming-looking at one stage before escalating at the next, meaning a system judged "safe" right after encountering suspicious input might already be compromised and simply waiting. As AI moves from simple chatbots into agents that plan multi-step tasks and use real tools, the researchers argue defenders need to stop taking security snapshots and start watching the whole story unfold — because once an AI system has memory, so does the attack against it. Stuff

ONE SPOOFED EMAIL, PASSPORTS AND CRYPTO HISTORIES EXPOSED: REVOLUT'S GOVERNMENT-IMPERSONATION BREACH



IMAGE SOURCE: REUTERS

Revolut, the London-based fintech with over 80 million customers globally, confirmed that a legitimate-looking government agency email domain was all it took for an unauthorized party to trick staff into handing over sensitive customer data — because the request passed authentication checks and appeared entirely genuine. The exposed information reportedly included full names, dates of birth, occupations, postal and email addresses, phone numbers, copies of passports and driving licences, verification selfies, account statements, and even Bitcoin transaction histories, though Revolut says biometric facial telemetry wasn't involved and insists customer funds and core systems remained untouched throughout. The company says only a "very limited" number of customers were affected and have been contacted directly, but hasn't disclosed the exact count or named the impersonated agency — and on-chain investigator ZachXBT, who first surfaced the customer notification publicly, suggested the breach appeared to target high-net-worth users specifically, an assessment Revolut hasn't confirmed. The timing is notable: Revolut is currently pursuing a potential public listing at a valuation of up to \$200 billion, making this exactly the kind of trust-eroding headline the company would rather not be managing right now. Reuters

RANDOM REDIRECTS, REAL THREAT? WHAT'S ACTUALLY HIJACKING YOUR BROWSER



IMAGE SOURCE: THE LOGIN BANNER

Your browser opens a page you never typed, new tabs multiply on their own, and every search seems to detour through some unfamiliar site — but a single stray redirect doesn't automatically mean malware, and treating every glitch as a "virus" can send you chasing the wrong fix. The real culprits are usually more specific: a browser hijacker quietly rerouting your homepage and search engine, or a compromised extension exploiting permissions it was never meant to have, especially ones installed without a clear, conscious decision. Fake "your device is infected" pop-ups add another layer of confusion, since these scareware alerts are built purely to provoke a click, a download, or a payment rather than to warn of any actual threat. The clearest red flags are recurrence and pattern — settings that keep reverting after every restart, unfamiliar login items launching automatically on a Mac, or redirects that persist across multiple browsers — each pointing toward a genuine infection rather than a one-off web hiccup. From there, the fix is methodical: audit installed extensions and site permissions first, check for rogue startup items if the problem survives a restart, run a scan with a trusted security tool if it persists, and going forward, install extensions sparingly, verify their source, and keep software updated to close the vulnerabilities attackers rely on. [The Login Banner](#)

FAKE JOB OFFER, REAL BACKDOOR: MIRAGE KITTEN'S NEW LINKEDIN TRAP FOR DEVELOPERS



IMAGE SOURCE: INDUSTRIAL CYBER

A LinkedIn message from a friendly "tech recruiter" is all it takes to get pulled into Mirage Kitten's latest scheme, which Kaspersky's GReAT team has traced to a fake recruitment pipeline targeting software engineers in aviation and fintech across Egypt, Ethiopia and Afghanistan, with related infections turning up as far afield as Germany, India and Ireland. Candidates are pressured into downloading a "coding challenge" under a tight one-to-three-hour deadline and explicitly warned off using AI code assistants — a warning that's really there to stop those tools from flagging the malware hidden inside. Once the developer starts working, two newly discovered threats slip in behind the scenes: NodeRabbit, a remote-access trojan that hijacks VS Code extensions and code repositories to relaunch itself every time the victim saves or merges a project, and PollCat, which waits for a fake "one-time password" before quietly harvesting system data. The bigger shift is technical rather than tactical — by rewriting its toolkit in Node.js and JavaScript instead of native Windows code, Mirage Kitten can now hit Windows, macOS and Linux with a single codebase, turning developers' own elevated network access into exactly the kind of high-value foothold cyber-espionage groups are chasing. [Kaspersky](#)

Watching the watchers. Guarding the guardians.

PERFECT CODE, IMPOSSIBLE CHOICE: IS AI ABOUT TO REVIVE THE ENCRYPTION BACKDOOR WARS



IMAGE SOURCE: VOCAL MEDIA

For over a decade, a fragile truce has held between digital privacy and state surveillance: governments hack their targets by exploiting software bugs rather than demanding backdoors baked into everyone's devices. Cryptography professor Matthew Green now warns that AI could quietly blow that truce apart — as large language models get frighteningly good at scanning codebases and squashing vulnerabilities before hackers can weaponize them, the exploit market intelligence agencies rely on for lawful surveillance could simply dry up, and researchers like Katie Moussouris predict that scarcity would trigger the same political pressure for mandated backdoors that cryptography alone never quite managed to provoke. It's a genuinely uncomfortable irony: AI succeeding at making software more secure could be exactly what pushes governments to demand it be deliberately weakened again. Not everyone buys the premise, though — skeptics like Hamid Kashfi argue AI is only mopping up low-hanging fruit while the complex, chained logic flaws sophisticated attackers actually rely on stay stubbornly out of reach, and Eva Galperin points out that finding a bug is one thing, but getting it patched across sprawling global software supply chains is another problem entirely, one AI hasn't solved. Where you land probably depends on how much you trust "vibe-coded" software not to keep introducing fresh vulnerabilities just as fast as AI patches the old ones. [Vocal media](#)

FREE WI-FI, FULL TRACE: HOW CHINA'S PUBLIC NETWORKS TURN EVERYDAY BROWSING INTO SURVEILLANCE DATA



IMAGE SOURCE: KHABARHUB

A July 2026 incident at Hunan Library — where public Wi-Fi was suspended after authorities detected users employing circumvention tools to access blocked overseas sites — has laid bare how China's routine internet infrastructure doubles as a surveillance layer. Under the Cybersecurity Law and related rules, public Wi-Fi operators must retain user registration data and network logs for at least six months, while mobile-number verification and a new national online identity framework (operational since July 2025) tightly bind browsing sessions to identifiable subscribers. Network engineers report that managed routers and access points can log device identifiers, connection timestamps, traffic volumes and, in many configurations, destination metadata; even when HTTPS or VPNs encrypt content, the act of connecting — and especially of attempting to bypass the Great Firewall — can trigger detectable events that feed into broader monitoring systems. With Freedom House rating China's internet freedom at 9/100 and documenting pervasive real-name requirements, facial-recognition coverage and police access to personal data, the episode underscores a shift from visible censorship to embedded traceability: in China's public spaces, free connectivity increasingly means monitored connectivity. [Khabarhub](#)

Watching the watchers. Guarding the guardians.

MODEM-LEVEL SPYWARE: GOOGLE'S PIXEL PATCH CONFIRMS ACTIVE EXPLOITATION BY COMMERCIAL SURVEILLANCE OPERATORS



IMAGE SOURCE: TECH TIMES

Google's September 2026 Pixel security bulletin has patched CVE-2026-58704, a privilege-escalation flaw in the cellular modem subcomponent that was already being used in real, targeted attacks before the fix shipped — a hallmark of commercial spyware tradecraft rather than opportunistic hacking. Because the baseband processor operates below the Android OS layer, compromise at this level can evade most endpoint detection tools while granting access to call metadata, SMS and location data, and potentially enabling lateral movement into the core OS — exactly the kind of stealthy, high-value access that mercenary surveillance vendors sell to government clients. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the flaw to its Known Exploited Vulnerabilities catalog with a three-day remediation deadline for federal agencies, underscoring both the severity and the narrow window in which unpatched Pixels remain exposed. For Pixel owners, the advisory is blunt: update immediately to the 2026-09-05 patch level or, if the device is end-of-life, retire it for sensitive use — because this is not a theoretical risk, but a confirmed, actively exploited pathway into the most privileged layer of the phone. Tech Times

MANTAX OTAX: INDONESIA'S HYBRID MOBILE MALWARE THAT RANSOMS YOUR FILES WHILE SPYING ON YOUR SCREEN



IMAGE SOURCE: ESECURITY PLANET

Zimperium's September 2026 analysis has uncovered Mantax Otax, an Indonesian Android malware that fuses ransomware encryption with full-spectrum spyware — turning infected phones into both locked vaults and live surveillance feeds under attacker control. Distributed via sideloaded APKs, the malware first secures device-admin and accessibility permissions, then registers the victim with a dynamically resolved C2 server before encrypting images, documents and media on older Android versions and forcing an on-screen chat portal for real-time ransom negotiation. In parallel, it harvests contacts, call logs, SMS (including OTPs), browser history, location, WhatsApp and Telegram data, streams screenshots and video to the cloud, and can silently snap photos with front and rear cameras; version 2 adds screen-blocking overlays, touch suppression, dialog spamming, full-screen video obfuscation and remote text-to-speech harassment. With evidence pointing to Indonesian targeting and a misconfigured Firebase backend exposing victim dialogues, Mantax Otax illustrates a dangerous convergence: mobile ransomware is no longer just about extortion — it's about total visibility, psychological pressure and persistent control over the device and the person behind it.

Zimperium

BLOOD TESTS, HOME ADDRESSES, AND A GRUDGE: INSIDE THE HACK THAT EXPOSED THE ENTIRE FBI



IMAGE SOURCE: BBC

ShinyHunters, a group not even regarded as particularly sophisticated by cybersecurity standards, is claiming to have breached the FBI's systems and stolen data on the agency's entire workforce — names, home addresses, badge numbers, spouse details, and shockingly, thousands of confidential "fitness-for-work" medical exams containing blood and urine test results and doctors' notes on conditions from high cholesterol to blood in the urine. Current and former agents describe genuine fear rippling through group chats, worried the leak could expose undercover operatives, enable "violence-as-a-service" attacks from young cybercriminal gangs, or even put family members normally shielded from the job's risks directly in harm's way. Bizarrely, the hackers aren't after money at all — their four-day ultimatum demands the FBI retract a May advisory that apparently "offended" them, a demand the agency seems unlikely to meet, meaning the data may go public regardless. Beyond the immediate danger, there's a deeper sting for agents: fury at what one insider called "sloppy and lazy security failures" that let a group known more for taunting reporters on Telegram than technical sophistication walk away with one of the world's most sensitive workforce databases — and a grim reminder from a former FBI cyber official that once data like this leaks, it tends to keep resurfacing on the dark web for years. BBC

3 MILLION RECORDS, INCLUDING 294,000 DEAD PEOPLE: THE PENTAGON'S NINE-MONTH DATA BLIND SPOT



IMAGE SOURCE: TIMES OF INDIA

A Pentagon personnel database quietly leaked Social Security numbers and job details on more than 3 million people — 2.76 million of them still living, 294,000 already deceased — and nobody caught it for nine months, with unauthorized access running from October 2025 all the way to July 2026 before the vulnerability was even discovered. The breach hit the Defense Manpower Data Center, one of the Pentagon's core record-keeping systems covering more than 60 million active-duty troops, reservists, civilians, contractors, veterans and military families, and officials say they're currently seeing no evidence the stolen data has been misused, offering credit monitoring to those affected. The timing couldn't be worse: it broke just as the FBI was already managing a separate breach of its own jobs portal, where hacking group ShinyHunters claims to have obtained employees' Social Security numbers, home addresses and emergency contacts — though the group now insists, almost defensively, that the whole thing was a "marketing campaign" rather than extortion, and that it never intended to publish the data at all. Two of the US government's most security-conscious institutions, hit within days of each other, are left offering nearly identical advice to their own people: stay alert, don't talk to reporters, and call 911 if journalists show up at your door. Times of India

REPRESSIVE MONITOR

ONE CONSULTANT, 25 MILLION SIM CARDS: INSIDE MALI'S CLAUDE-BUILT SPY PLATFORM



IMAGE SOURCE: THE ECONOMIC TIMES

Buried in Anthropic's latest threat report is one of its most striking single cases: a Bamako-based tech consultant, working with junta-led Mali's state intelligence service, used Claude Code as an "engineering workforce" to build Lakana 360 — a national interception platform capable of monitoring roughly 25 million SIM cards across all three of the country's mobile operators. The system could capture calls, texts, and voice traffic, link identities across SIM-card swaps by voice recognition, flag anyone using encryption or a VPN, and generate a searchable dossier on any phone number — and at one operator's request, the consultant had Claude help remove a legal requirement for a court order before that data could be handed over. Because the platform ran locally on other AI models once built, banning the Claude account that helped design it did nothing to shut down the deployed system, a detail Anthropic itself flagged as a limit on how far account bans can reach once code walks out the door. The case sits alongside similar findings from China and Iran in the same report — including a Chinese religious-affairs intelligence unit that Anthropic says shrank from "many teams of analysts" to a single office producing thousands of AI-assisted investigations a month — underscoring how much easier AI has made it for governments to build the kind of population-scale surveillance infrastructure that once required entire agencies of human analysts. [The Economic Times](#)

TELECOMS, UBIQUITOUS SURVEILLANCE AND STATE CRIME: A CASE STUDY FROM KENYA

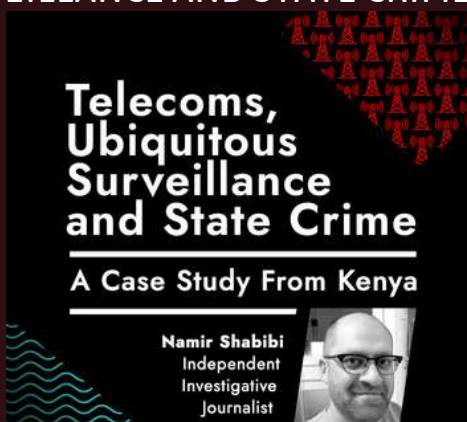


IMAGE SOURCE: DISRUPTION NETWORK INSTITUTE

A September 2026 report by researcher Namir Shabibi, published with the Kenya Human Rights Commission (KHRC), argues that Kenya's telecommunications sector has been transformed into a core pillar of the state's surveillance architecture, with mobile operators — especially Safaricom — enabling real-time tracking, call-data harvesting and predictive profiling of citizens without meaningful judicial oversight. Building on a 2024 Daily Nation investigation, the report details how Safaricom allegedly granted security agencies routine, warrantless access to call detail records (CDRs) and location data, and co-developed software with UK-based Neural Technologies that gave police "virtually unfettered" access to subscriber information, allegedly aiding operations linked to enforced disappearances, renditions and extrajudicial killings. Shabibi situates these practices within a broader "ubiquitous surveillance" regime: telecom infrastructure is no longer a neutral utility but a data-rich chokepoint that allows the state to monitor movements, communications and social networks at scale, often under the cover of counter-terrorism and crime-control narratives. The report calls for statutory limits on data access, independent oversight bodies, mandatory breach notifications and stronger enforcement of Kenya's data protection and interception laws — warning that without such reforms, telecoms will remain the quiet backbone of a surveillance state that operates largely outside the confines of constitutional privacy guarantees. [Disruption Network Institute](#)

BIOMETRIC SURVEILLANCE AND THE RIGHT TO PRIVACY IN NIGERIA: THE LEGAL CHALLENGES IN THE AGE OF FACIAL RECOGNITION TECHNOLOGY



IMAGE SOURCE: DEVELOPING TELECOMS

A legal analysis on biometric surveillance in Nigeria exposes how the rapid proliferation of facial recognition technology across public spaces and law enforcement agencies is severely threatening citizens' constitutional rights to privacy. The legal study highlights that while the Nigerian government increasingly deploys advanced facial recognition and biometric tracking under the banner of national security and crime prevention, the country's existing legal safeguards—primarily the Nigeria Data Protection Act and Section 37 of the 1999 Constitution—are ill-equipped to counter state overreach, vague public-interest exemptions, and mass surveillance without oversight. Legal experts emphasize that without specialized legislative frameworks governing automated facial processing, strict judicial warrant requirements, and clear limits on biometric data retention, state actors and private vendors operate in a regulatory vacuum—leaving millions of citizens vulnerable to indiscriminate tracking, biometric identity theft, and unchecked state-sponsored surveillance. [SSRN](#)

FROM PROPAGANDA TO PIPELINE: RUSSIA'S AI-POWERED HYBRID WARFARE IN AFRICA



IMAGE SOURCE: THE INVISIBLE INSIDER

A report by The Invisible Insider reveals how Russian-linked state and proxy actors—including remnants of the Wagner/Africa Corps ecosystem—are increasingly using generative artificial intelligence as a weaponized force multiplier to industrialize influence operations, cyber espionage, and surveillance across Africa. Highlighting documented cases in the Central African Republic and West Africa, the analysis details how AI is being leveraged to automatically produce local-language articles, social media scripts, and synthetic media designed to attack Western entities while covertly laundering pro-Kremlin narratives through local news outlets like Bangui's Radio Lengou Songo. Beyond automated propaganda, security researchers emphasize that AI tools are actively assisting in real-time cyber operations—such as adaptive malware development, automated phishing, and rapid network reconnaissance—while accelerating state surveillance capabilities in nations like Mali. Experts warn that the rise of "influence-as-a-service" and AI-driven information laundering makes attribution increasingly difficult, eroding democratic institutions and transforming state influence into a scalable, high-speed commodity available to the highest bidder. [The invisible insider](#)

Watching the watchers. Guarding the guardians.

MOROCCO: WHISTLEBLOWER REVEALS HOW AUTHORITIES USED A WEB OF SURVEILLANCE TO SILENCE JOURNALISTS AND ACTIVISTS



IMAGE SOURCE: AMNESTY INTERNATIONAL

For almost a decade, a Moroccan intelligence officer going by the pseudonym "Safir" watched from inside the DGST — the kingdom's domestic security service — as it built one of the most aggressive surveillance operations ever documented against journalists and dissidents, and now he's telling *Forbidden Stories*, Amnesty International's Security Lab, and 13 media partners everything he saw. Pegasus, the notorious Israeli spyware first linked to Morocco back in 2021, turns out to be just one tool in a far wider arsenal: operatives reportedly bugged internet cafes and even persuaded shopkeepers to sell phones pre-infected with spyware directly to targets, all coordinated out of a house nicknamed "the FSSYS villa" after the Emirati surveillance broker that helped supply the tools — a setup Safir compared to splitting a Netflix subscription, suggesting Morocco shared access to surveillance capability with allied Gulf security services. The investigation corroborates his account with leaked emails, targeting records, victim testimony and internal training material, adding fresh detail to earlier revelations that Moroccan journalists and activists were hacked as far back as 2017, alongside high-profile targets like French President Emmanuel Macron's own circle. For African press-freedom advocates, the reach is the real headline: this isn't just one country's spy story, but a case study in how commercial spyware markets let authoritarian-leaning governments build population-scale surveillance capacity once reserved for major intelligence powers — all while Rabat has spent years flatly denying any of it happened. [Amnesty International](#)

ESCALATING DIGITAL SURVEILLANCE, REPRESSION AND ATTACKS AGAINST WOMEN HUMAN RIGHTS AND WOMEN ENVIRONMENTAL DEFENDERS IN SOMALIA.



IMAGE SOURCE: DHRO

A joint statement from three Somali civil society groups — DHRO, CSHRD and HANAHR — paints a troubling picture of women human rights defenders, journalists and environmental activists reporting the classic telltale signs of spyware infection: phones overheating for no reason, batteries draining unusually fast, communications mysteriously interfered with, and organizational inboxes flooded with spam, all raising fears that Pegasus or similar commercial surveillance tools are being deployed against them. These digital red flags aren't happening in isolation — they're surfacing alongside arrests, physical assaults, home and office raids, and confiscated phones and laptops, devices that often hold sensitive information about abuse survivors, witnesses and other at-risk sources, meaning a single seized phone can endanger an entire network of people far beyond its owner. Two cases anchor the statement: activists Rahma Yusuf and Zainab Abdi, reportedly held under house arrest in Beledweyne since early September and allegedly assaulted, and social-media activist Sadia Moalim Ali, sentenced to three years by Banadir Regional Court seemingly over her peaceful protest participation and online expression — a case the groups frame as part of a broader pattern of women being targeted specifically because of their public visibility. The statement closes with a direct call for an independent technical investigation into the suspected device compromises and for Somali authorities to clarify the legal basis, if any, behind the surveillance and detentions — while noting the stakes go well beyond individual defenders, since silencing one organizer can chill an entire civic network at once. [DHRO](#)

Watching the watchers. Guarding the guardians.

PEGASUS IN THEIR POCKETS: THE SPYWARE SCANDAL ROCKING SERBIA'S ELECTIONS



IMAGE SOURCE: REUTERS

At least 14 members of Serbia's civil society - student activists, opposition MPs, a local councillor - discovered their phones had been secretly turned into surveillance devices in the run-up to March's local elections, in what [Citizen Lab](#) and the [SHARE](#) Foundation calls the largest documented spyware wave the country has ever seen. The infections only came to light in August, after Apple warned people in 110 countries they'd likely been hit by mercenary spyware, and at least one device was confirmed to carry NSO Group's notorious Pegasus tool, capable of remotely switching on a phone's microphone and camera without any warning. One student activist described the violation bluntly at a Belgrade press conference, saying the spyware let someone listen in on private moments as intimate as a shower. Reuters couldn't pin down who was behind the attacks, and NSO Group maintains it sells only to governments, while a senior ruling-party official has already dismissed the students' claims outright — leaving a chilling question hanging over Serbia's civil society just as another round of national elections looms. [Reuters](#)

SPYING ON ITS OWN CITIZENS, BLIND TO ITS OWN LEAKS: SPAIN'S SECURITY PARADOX



IMAGE SOURCE: MORROCCO WORLD NEWS

A nearly [500-page](#) file of leaked personal data on Guardia Civil, National Police, and Armed Forces personnel has reopened uncomfortable questions about Spain's ability to secure its own institutions — the latest in a string of breaches that also saw someone arrested for querying restricted government databases with illicit software, and another leak reaching officials tied to the Public Prosecutor's Office and National Cybersecurity Institute itself. This opinion piece argues the pattern runs deeper than data leaks, tracing it back to the Pegasus scandal, in which Spain's intelligence agency admitted to spying on 18 Catalan independence figures using NSO Group's notorious spyware — only for the same tool to later be found on the phones of the prime minister and three cabinet ministers, with the perpetrator never identified and the case closed twice without answers. Add in an active parliamentary probe into alleged police surveillance of Catalan politicians, a parapolice spying operation against a party treasurer awaiting judgment, and a former police commissioner already sentenced for illegally accessing a phone, and the piece frames a pointed question: before pointing fingers abroad over recent unrest, shouldn't Madrid first figure out who's spying inside its own institutions, and why it can't keep its secrets secret? [Morrocco World News](#)

INDIA'S SURVEILLANCE GAP: WHEN FACIAL RECOGNITION MEETS LEGAL SILENCE



IMAGE SOURCE: [LIVE LAW](#)

A July 2026 deployment of Delhi Police's [Ikshana van](#) — a mobile surveillance vehicle equipped with AI-powered facial recognition cameras — to monitor protesters at Jantar Mantar has ignited a constitutional challenge over India's gaping lack of legal guardrails for biometric surveillance. Critics argue the operation violated the Puttaswamy privacy test by failing all four prongs: there is no statute authorising real-time facial recognition at public assemblies, no clear legitimate aim beyond vague "public order" claims, no proportionality assessment, and no procedural safeguards governing data retention, access, or deletion. The article traces how colonial-era interception laws and modern statutes like the IT Act (2000), Telecommunications Act (2023), and the Digital Personal Data Protection Act (2023) collectively grant the state sweeping surveillance powers while exempting it from data minimisation rules and independent oversight — creating a regime where unlawful surveillance rarely triggers consequences. With the Supreme Court now examining proportionality and the petitioners demanding statutory thresholds, judicial review, and mandatory data erasure timelines, the case underscores a broader democratic deficit: India has constitutional privacy rights on paper, but no enforceable architecture to stop the state from turning every protest into a biometric dragnet. [Live Law](#)

TROJAN HORSE ON THE SCREEN: HOW RUSSIA'S FORCED "MAX" SUPER-APP TURNED MOBILE PHONES INTO STATE BACKDOORS



IMAGE SOURCE: [THE GUARDIAN](#)

An investigative investigation published by The Guardian reveals that tens of millions of Russian citizens—including civil servants, university students, teachers, and school children—are being systematically coerced into adopting "Max," a state-backed messaging and payments super-app that functions as a sophisticated surveillance backdoor directly on users' personal devices. Developed by VKontakte (VK), a tech firm deeply entangled with the Kremlin, the all-in-one app has been touted as a domestic replacement for blocked Western services like WhatsApp and Telegram. However, forensic analysis by computer science researchers at the University of Michigan uncovered that Max can quietly capture phone screenshots without consent, access stored mini-app data, read messages, extract financial transactions, impersonate users, and even inject code into connected mini-apps that could potentially execute targeted cyberattacks. Security researchers warn that Max serves as a dangerous, exportable blueprint for digital authoritarianism—giving the Kremlin unprecedented real-time surveillance oversight under the guise of everyday public services, while forcing politically connected elites to buy burner phones solely to simulate compliance. [The Guardian](#)

Watching the watchers. Guarding the guardians.

ITALY'S PUBLIC BROADCASTER UNDER POLITICAL PRESSURE: MFRR REPORT FLAGS MEDIA IMPARTIALITY CRISIS



IMAGE SOURCE: ITALIAN YEARBOOK OF HUMAN RIGHTS

The Media Freedom Rapid Response (MFRR) consortium's July 2026 mission report warns that Italy's public service broadcaster, Radiotelevisione Italiana (Rai), remains subject to entrenched political interference that undermines editorial independence and media pluralism — a direct breach of the European Media Freedom Act (EMFA), which entered full force in August 2025. Based on a fact-finding visit to Rome in March 2026, the report documents how Rai's board appointments and governance continue to track parliamentary majorities rather than independent, merit-based criteria, enabling successive governments to exert outsized influence over newsroom priorities, staffing, and coverage of sensitive political issues. Beyond Rai, the MFRR identifies a broader pattern of media freedom backsliding: journalists face escalating strategic lawsuits against public participation (SLAPPs), digital surveillance via spyware, and physical threats — including the 2024 car-bomb attack on investigative reporter Marco Reguzzoni — with weak judicial safeguards and incomplete transposition of EU anti-SLAPP protections leaving reporters exposed. The consortium urges Rome to urgently reform Rai's governance in line with EMFA, extend anti-SLAPP shields to domestic cases, mandate full media ownership transparency, and introduce robust judicial oversight of digital surveillance to halt what it describes as a "systematic erosion" of Italy's media landscape. [Italian yearbook of human rights](#)

EVERY AD YOU SEE IS WATCHING BACK: A JOURNALIST'S GUIDE TO FIGHTING AD TECH SURVEILLANCE



IMAGE SOURCE: CPJ

Every targeted ad you scroll past is powered by a system quietly building a profile of you — one that CPJ and Harvard's Carr-Ryan Center have shown can put journalists at risk both at home and in exile, since the same data that fuels personalized ads can end up bought, sold, or handed to governments and other bad actors. The good news is that most of that exposure comes down to settings most people never touch: this piece walks through exactly where to find and disable the advertising ID and location-sharing permissions buried in Android, iOS, Windows and Google account menus, plus free tools like Privacy Badger that block third-party trackers your browser would otherwise wave straight through. It doesn't stop at prevention either — there's guidance on scrubbing personal data already sitting with data brokers, checking which apps are quietly harvesting sensitive information through hidden SDKs, and links to CPJ's dedicated advisories on ad-delivered spyware, Pegasus, and online harassment. For anyone who assumes ad tracking is just an background nuisance, this is a reminder that the infrastructure behind it is a genuine surveillance risk — and a practical checklist for actually doing something about it. [CPJ](#)

Watching the watchers. Guarding the guardians.

SEEN AND SILENCED: HOW RUSSIAN SURVEILLANCE SOFTWARE SUPPRESSES GEORGIAN CIVILIANS RIGHTS



IMAGE SOURCE: ALGORITHM WATCH

Nino only found out how effective the cameras outside Georgia's Parliament were when a court showed her footage of herself crossing a road during a protest — footage precise enough to convict her, freeze her bank accounts, and impose a fine she could only pay through crowdfunding. That system, called Polyface, has been quietly procured since 2013 from Papillon AO, a Moscow company sanctioned by multiple Western governments and tied to Russia's FSB, and it now runs on a deep-learning engine built by a Russian state-backed AI firm capable of identifying masked faces in crowds and reconstructing a person's entire protest history across every demonstration they've ever attended. As Georgia's government criminalized face coverings, road-blocking, and even online criticism following disputed 2024 elections, the technology did something batons and water cannons couldn't: it made showing up to protest a permanent, searchable liability, and thousands of Georgians who once marched daily have quietly stopped. Security analysts warn the stakes go beyond individual fines — with a core piece of state infrastructure legally answerable to Russian security services, the same database used to identify protesters could just as easily be used to map a country's entire political opposition from the ground up. [Algorithm Watch](#)

CHOSEN BRICK: HOW IRAN TURNS TELEGRAM, FAKE ANTIVIRUS AND SOCIAL ENGINEERING INTO A GLOBAL SPYWARE CAMPAIGN

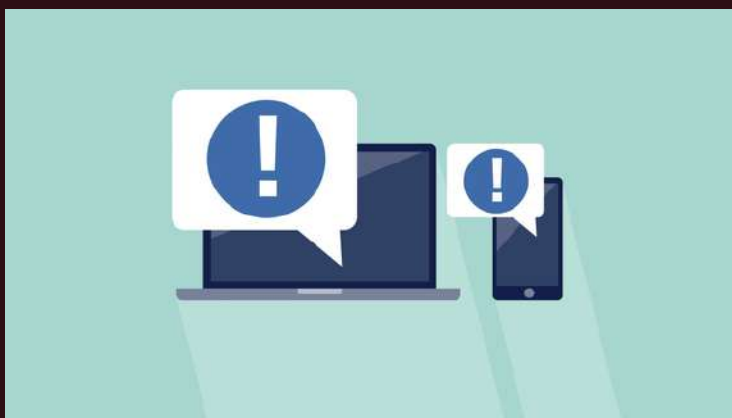


IMAGE SOURCE: NCSC

A joint advisory from the UK's National Cyber Security Centre, the US FBI and the Netherlands' AIVD warns that Iranian state cyber actors have been using a malware family dubbed [CHOSEN BRICK](#) since at least 2025 to target dissidents, activists and journalists worldwide — including in the UK, US and Netherlands — enabling remote harvesting of contacts, emails, social-media messages and screen content that can be used to track victims' movements and, in some cases, expose their identities on pro-Iranian leak sites. The operation relies on highly tailored social engineering over WhatsApp and Telegram: attackers pose as trusted contacts or platform support staff, persuade targets to open seemingly legitimate files (from fake MRI scans to counterfeit antivirus and productivity apps), and then deploy CHOSEN BRICK, which persists via Windows registry run keys, disables or evades Microsoft Defender, and uses unique Telegram bot IDs for command-and-control to blend in with normal traffic. Once installed, the malware can capture screenshots, record audio, steal email and messaging data, download additional payloads and even wipe devices, with exfiltration routed through Telegram and cloud object stores such as VultrObjects and StorjShare; the advisory urges at-risk individuals and organisations to treat unsolicited files and links as hostile, keep systems updated, run reputable antivirus, and check for suspicious registry entries and unexpected connections to Telegram and proxy services. [NCSC](#)

INTELLIGENCE AGENCIES

FORTIFYING THE FRONTIER: SA BORDER MANAGEMENT AUTHORITY DEPLOYS TECH-DEFENSE ARSENAL



IMAGE SOURCE: ADF

The South African Border Management Authority (BMA) has teamed up with domestic defense and cybersecurity firms in a pilot initiative that deployed advanced surveillance and protective technologies across two of the nation's busiest border posts, Beitbridge and Lebombo. The public-private partnership integrated a multi-layered defense stack—combining Springbuck armored personnel carriers from DCD Protected Mobility, AI-powered body cameras equipped with facial and license plate recognition from Unipro, unmanned aerial reconnaissance drones from A2D Geoscan and Battlecopter, and specialized cybersecurity safeguards supplied by Snode Technologies. BMA Commissioner Dr. Michael Masiapato hailed the operational test as a massive success after border forces processed over 4.9 million travelers, intercepted nearly 27,000 illegal entrants, and made dozens of high-level arrests for cross-border crimes including weapon smuggling and stolen vehicle trafficking, signaling a permanent shift away from "soft target" border vulnerabilities toward real-time, tech-driven threat detection. [ADF](#)

BAGGED, BLINDFOLDED, INTERROGATED: SOMALIA'S SPY AGENCIES TURN ON THE PRESS



IMAGE SOURCE: INDEX ON CENSORSHIP

Freelance journalist Mohamed Bulbul was eating dinner in Mogadishu with two colleagues when masked gunmen stormed in, beat all three, and dragged him away with a bag over his head - punishment, he says, for co-authoring a story two days earlier about the prosecution of an activist. Interrogated by Somalia's National Intelligence and Security Agency and given a stark ultimatum — work for them, leave the country, or die — Bulbul fled and now lives in hiding, unable to see his own children. His case sits alongside a string of others documented across Somalia and Puntland: a journalist jailed for 13 days over a 15-second video of armed militia, a reporter blindfolded and held four days without a lawyer for photographing shuttered market stalls, and a media founder abducted and detained for 39 days without charge. Analysts describe a troubling pattern — security institutions built with international support after Somalia's civil war are now being redirected away from courts and due process entirely, deployed instead to silence reporting the government would rather the public never see, all unfolding against the backdrop of a contested constitutional overhaul. [Index on Censorship](#)

BEYOND THE LAW: HOW UGANDA'S SPYWARE ERA OUTFRONS ITS SURVEILLANCE STATUTES



IMAGE SOURCE: PRESS READER

Uganda's deployment of advanced spyware — including NSO Group's Pegasus — has exposed a widening gap between the state's surveillance capabilities and the country's outdated legal framework, which was drafted long before encrypted messaging apps and device-level hacking tools became commonplace. The 2010 Regulation of Interception of Communications Act and the Anti-Terrorism Act (2002, amended 2022) authorise interception of communications "in the course of transmission" for national security and counter-terrorism purposes, but they do not contemplate spyware that can exfiltrate stored photos, contacts, location data, microphone and camera feeds, or messages before they are sent — activities that fall outside the statutes' original scope yet are routinely justified under broad "public safety" and "national security" clauses. Citing Freedom House's 2026 report and regional trends, the investigation argues that Uganda — rated 33/100 and classified as "not free" — uses this legal ambiguity to target journalists, activists and opposition figures, with terrorism provisions sometimes weaponised to legitimise surveillance of political adversaries. Drawing on persuasive precedents such as the U.S. WhatsApp v NSO ruling and South Africa's AmaBhungane decision, the piece contends that key provisions of Uganda's interception and anti-terrorism laws lack necessary safeguards — including independent authorisation, minimisation, post-surveillance notification and protection of privileged communications — and may therefore fail the constitutional test under Article 43(2)(c), which bars rights limitations that are not "demonstrably acceptable and justifiable in a free and democratic society." [EACIR](#)

SPYWARE VS SAFEGUARDS: NIGERIA'S DIGITAL POLICING PUSH SPARKS PRIVACY ALARM



IMAGE SOURCE: ICIR

At a September 2026 virtual forum organised by The ICIR, digital rights experts warned that Nigeria's expanding use of spyware and other covert surveillance tools is outpacing the country's legal and institutional safeguards, putting journalists, activists and ordinary citizens at risk of unchecked privacy violations. Senior tech legal counsel Natalia Krapiva described spyware as malicious software that can be installed remotely without a target's knowledge to harvest messages, photos, contacts, keystrokes and device metadata — capabilities that enable not only criminal investigations but also political monitoring of protesters and critics. Digital rights lawyer Olumide Babalola acknowledged that Nigerian law — including the Constitution, the Nigerian Communications Act, the NCC's 2019 Lawful Interception Regulations and data protection statutes — permits interception in narrowly defined circumstances, but stressed that such powers must be exercised lawfully, proportionately and with judicial oversight, warning that the real harm often lies in the erosion of personal autonomy rather than just arrests or prosecutions. While the Nigeria Police Force's National Cybercrime Centre defended its need for sophisticated digital tools under the Cybercrimes Act 2021 (as amended) to combat increasingly tech-enabled crime, the panel underscored a growing tension: without clearer statutory thresholds, independent authorisation, minimisation rules and post-surveillance notification, Nigeria's surveillance arsenal risks becoming a tool of rights abuse rather than a narrowly tailored instrument of law enforcement. [ICIR](#)

Watching the watchers. Guarding the guardians.

ELECTIONS, SPYWARE AND THE EAST AFRICAN SURVEILLANCE PLAYBOOK



IMAGE SOURCE: EACIR

A September 2026 investigation by VOX POPULI traces how East African states have repeatedly timed the acquisition and deployment of intrusive malware to coincide with election cycles, turning general elections into high-stakes surveillance operations that target dissidents, journalists and opposition figures. In Uganda, the report links the 2026 hack of exiled human rights lawyer Nicholas Opiyo to a long pattern that began with the post-2011 “Fungua Macho” operation using FinFisher spyware, continued through failed attempts to buy Hacking Team tools in 2015, and escalated ahead of the January 2026 polls with leaked wiretaps of Bobi Wine, Jimmy Spire Ssentongo and prominent journalists, alongside a phishing-driven malware attack on Nation Media Group’s networks. The piece documents how import records and shipping manifests show Uganda procuring advanced surveillance gear — including signal analysers, radio testers and data-processing equipment — in the run-up to 2026, while regional peers followed similar scripts: Tanzania’s 2025 election was preceded by Circles-style telecom exploitation tools and US-made Oxygen Forensics hardware, and Kenya’s response to the 2024 Gen Z tax protests saw Cellebrite extraction tools used on activist Boniface Mwangi’s phone and FlexiSPY found on the devices of filmmakers behind the Blood Parliament documentary. With Rwanda also confirmed to have received NSO Group products via Q Cyber Technologies ahead of its 2029 election, the article argues that East Africa’s electoral calendar now doubles as a procurement and operational timetable for digital repression, where spyware is not an exceptional emergency measure but a routine instrument of political control. [EACIR](#)

NO CLICK NEEDED: ICE CONFIRMS IT'S USING \$2M ZERO-CLICK SPYWARE



IMAGE SOURCE: MILITARY.COM

In a letter that took six months to answer a congressional inquiry, acting ICE Director Todd Lyons quietly confirmed what privacy advocates had feared for over a year: the agency is deploying Graphite, Israeli firm Paragon Solutions' "zero-click" spyware capable of breaking into a phone's encrypted messages without the target ever tapping a link. The \$2 million contract was signed at the tail end of the Biden administration, frozen amid concerns it violated an executive order restricting government spyware use, then quietly revived under Trump last fall — with Lyons framing the tool as essential for tracking fentanyl traffickers and transnational criminal networks exploiting encrypted apps. The timing raises uncomfortable questions, since WhatsApp had already disclosed that roughly 90 journalists and civil society members worldwide were targeted by the same software, and Paragon has since cut ties with at least one European government over similar abuses. With ICE still stonewalling public records requests — prompting 404 Media to sue for access to the contract itself — lawmakers and civil liberties groups are left asking exactly who this tool will be pointed at next, as the agency's mass-deportation campaign continues to expand. [Military.com](#)

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



GET INVOLVED!

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](https://twitter.com/IntewatchNews)



[@IntewatchNpc](https://facebook.com/IntewatchNpc)



Intewatch website



[@IntewatchNpc](https://youtube.com/IntewatchNpc)



[@IntewatchNpc](https://linkedin.com/company/IntewatchNpc)



HAVE ANY QUESTIONS?



Email: info@intelwatch.org.za



Luminate



Funded by
the European Union

We are grateful for the support of our donors!