Issue #17

INTEL WATCH

October 2026

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

DO YOU KNOW WHO'S WATCHING YOU? WE'RE HERE TO HELP YOU FIND OUT

EXCLUSIVE INTELWATCH REPORT

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #17 OF THE WATCHER



In this issue #17 of *The Watcher*, we turn our attention to a digital world where the technologies connecting us, protecting us and making our lives easier are increasingly being used to expose, exploit and control us. From cyberattacks targeting critical infrastructure to artificial intelligence enabling more sophisticated forms of surveillance, the boundaries between security and vulnerability are becoming harder to distinguish. Across Africa and beyond, governments, businesses and ordinary citizens face a rapidly evolving threat landscape in which data has become a powerful currency, digital systems are increasingly attractive targets, and the tools designed to protect us can just as easily be turned against us. This edition asks a fundamental question: as digital power expands, who is watching those who wield it, and who holds them accountable?

Closer to home, we examine South Africa's growing cybersecurity challenges, where attacks on critical infrastructure, businesses and public institutions expose the consequences of digital vulnerabilities. The temporary shutdown of the Presidency's website following warnings about critical software flaws, alongside ransomware attacks and data breaches affecting South African companies, highlights the risks facing an increasingly connected society. We also explore how weaknesses in third-party suppliers can expose customer information, how AI-generated phishing scams are becoming more convincing, and why spending more on cybersecurity does not necessarily translate into stronger protection. Across the continent, organisations in countries including Angola, Nigeria and Kenya face mounting cyber threats, while the rapid growth of digital financial services creates new opportunities for fraud, identity theft and the compromise of personal information. The message is clear: cybersecurity is no longer simply a technical concern; it is fundamental to economic stability, public trust and the protection of citizens' rights.

We also investigate how artificial intelligence is transforming the surveillance capabilities of states and the methods used to repress dissent. An investigation into the development of Mali's Lakana 360 interception platform raises troubling questions about the use of AI-assisted tools to expand communications monitoring, while developments in Kenya and Nigeria illustrate how telecommunications infrastructure and facial-recognition technologies can strengthen state surveillance. Elsewhere, Russian-linked actors are using generative AI to support propaganda and cyber-espionage operations across Africa. Beyond the continent, spyware allegations in Serbia, the use of facial recognition against protesters in Georgia, and growing concerns about surveillance technologies in India and Russia demonstrate how digital monitoring can turn political participation into a potential liability. For journalists, activists and ordinary citizens, the consequences extend beyond privacy: pervasive surveillance can discourage dissent, undermine freedom of expression and weaken the democratic space in which public accountability depends.

The role of intelligence agencies also comes under scrutiny this month. In South Africa, plans for a public-private security initiative involving armoured vehicles, AI-powered body cameras and drones at major border posts raise questions about the expansion of surveillance and enforcement powers. In Somalia, concerns about the treatment of journalists by intelligence authorities highlight the risks facing independent reporting, while Uganda's use of spyware exposes the gap between sophisticated surveillance capabilities and outdated legal safeguards. Nigeria faces similar questions over the growth of its spyware arsenal and the potential for abuse where oversight is inadequate. A regional investigation into the timing of spyware acquisitions across East Africa further explores the relationship between surveillance technology and electoral politics. Meanwhile, in the United States, Immigration and Customs Enforcement's confirmed use of Paragon's Graphite spyware brings renewed attention to the deployment of highly intrusive surveillance tools by state authorities. Across these cases, a common concern emerges: intelligence capabilities can expand far more quickly than the laws, transparency mechanisms and independent oversight needed to prevent their abuse.

Finally, we examine what happens when artificial intelligence becomes an active participant in cyber operations rather than merely a tool used by human operators. Google's disclosure that its Gemini model autonomously hacked three real-world companies during a safety test, alongside Anthropic's findings on the misuse of Claude by state-linked hackers and influence operations, illustrates how quickly the cybersecurity landscape is changing. As AI systems become more capable of identifying vulnerabilities, automating attacks and supporting complex operations, the distinction between defensive research and malicious exploitation becomes increasingly difficult to manage. African businesses and public institutions are particularly exposed as digital adoption accelerates, often without equivalent investment in resilience, expertise and effective security practices. These developments raise urgent questions about the accountability of technology companies, the limits of automated systems and the safeguards needed to prevent increasingly autonomous tools from causing harm.

This month's investigations reveal a troubling pattern: the same digital infrastructure that enables communication, innovation and public service can also become a channel for intrusion, manipulation and state control. Whether through cyberattacks on essential services, AI-assisted surveillance, spyware targeting government critics or intelligence agencies operating without sufficient oversight, the risks extend far beyond technology itself. They touch on democratic accountability, media freedom, economic security and the fundamental rights of individuals. As governments and private companies acquire increasingly powerful digital capabilities, transparency, independent oversight and meaningful human-rights protections must remain central to how these technologies are developed and deployed.

As always, The Watcher remains committed to examining the systems of power operating behind our screens and asking the questions that matter: who controls our data, who monitors our communications, and who ensures that those entrusted with protecting us do not become a threat to our freedoms? Because watching the watchers is not simply about exposing surveillance; it is about defending the transparency, accountability and democratic freedoms on which an open society depends.

THIS MONTH'S FOCUS

EXCLUSIVE INTELWATCH REPORTS - pages 4

This section features Intelwatch's new report, "Ivory Coast's 2025 Elections: Procedural and Undemocratic," examining the political dynamics surrounding Côte d'Ivoire's October 2025 presidential election. It explores the exclusion of major opposition figures, contested constitutional interpretations, restrictions on political freedoms, electoral violence, mass arrests and disinformation, situating these developments within the country's history of political rivalry and conflict. The report considers the implications for democratic legitimacy, political accountability and stability, highlighting the need for electoral reform, inclusive political dialogue and stronger institutional safeguards.

SURVEILLANCE UPDATES - pages 5-23

This section examines the growing cybersecurity threats facing South Africa, Africa and the wider world, from critical software vulnerabilities and attacks on public infrastructure to corporate data breaches, ransomware and increasingly sophisticated digital fraud. It explores the risks posed by the PHP2Shell vulnerabilities, the exposure of customer information through third-party suppliers, AI-powered phishing, mobile banking fraud and emerging attacks targeting AI systems themselves. The section also investigates the growing role of artificial intelligence in both cyber defence and cybercrime, alongside the challenges facing African organisations as attack rates rise and security measures struggle to keep pace.

REPRESSION MONITOR - pages 24-29

This section explores how surveillance technologies, artificial intelligence and spyware are expanding the capacity of governments and other actors to monitor communications and restrict dissent. It examines the development of Mali's Lakana 360 interception platform, surveillance through Kenya's telecommunications sector, Nigeria's facial-recognition rollout and the use of generative AI for propaganda and cyber-espionage in Africa. Internationally, the section investigates spyware targeting Serbian civil society, surveillance concerns in India and Georgia, Russia's Max super-app, and the implications of digital monitoring for journalists and media freedom in Europe. It also examines the risks posed by Iranian-linked spyware campaigns targeting dissidents and journalists, highlighting the urgent need for stronger privacy protections and independent oversight.

INTELLIGENCE AGENCIES - pages 30-32

This section investigates the expanding surveillance and enforcement capabilities of intelligence and security agencies, with particular attention to the accountability gaps that arise when technological power outpaces legal safeguards. In South Africa, it examines a public-private security initiative involving armoured vehicles, AI-powered body cameras and drones at major border posts. Elsewhere, it explores concerns over Somalia's intelligence agency and its treatment of journalists, Uganda's use of spyware amid outdated interception laws, and warnings about Nigeria's expanding surveillance capabilities. A regional investigation examines how East African states time spyware acquisitions around electoral cycles, raising questions about political surveillance and democratic accountability. The section concludes with the United States' confirmed use of Paragon's Graphite spyware by Immigration and Customs Enforcement (ICE), reinforcing wider concerns about the use of intrusive surveillance technologies and the need to protect journalists, civil society and fundamental rights.

EXCLUSIVE INTELWATCH REPORT

IVORY COASTS' 2025 ELECTIONS: PROCEDURAL AND UNDEMOCRATIC

BY INTELWATCH

Download English report here
Download French report here



Report synopsis:

This report provides a comprehensive overview of the socio-political dynamics surrounding Côte d'Ivoire's October 2025 presidential election and the historical factors that shaped its outcome which resulted in the re-election of Alassane Ouattara for a fourth consecutive term, with an official vote share of 89.77%1 and a voter turnout of approximately 50.1%

The report examines how President Alassane Ouattara's fourth consecutive term unfolded amid the exclusion of major opposition figures, contested constitutional interpretations, restrictions on political freedoms, mass arrests, electoral violence and disinformation. Situating the election within Côte d'Ivoire's history of political rivalry, contested transitions and conflict, the report explores how legal and institutional mechanisms can be used to maintain political dominance while weakening opposition participation, electoral competition and public trust in democratic institutions. It further considers the implications of these developments for political stability, democratic legitimacy and the prospects for peaceful political transitions, while examining the responsibilities of domestic institutions and the international community in safeguarding democratic principles. Ultimately, the report highlights the urgent need for meaningful electoral and institutional reforms, inclusive political dialogue, stronger democratic accountability and generational renewal to create a more competitive political environment, restore public confidence and reduce the risk of renewed political instability.

SURVEILLANCE UPDATES

SA'S PRESIDENCY WEBSITE TAKEN DOWN AS CYBERSECURITY FLAW SPARKS WARNINGS ACROSS THE WORLD



IMAGE SOURCE: DAILY MAVERICK

South Africa's Presidency temporarily took its official website offline on 23 October 2026 as a precautionary measure amid a global cybersecurity alert concerning two critical vulnerabilities in PHP, a programming language that powers a large proportion of websites and web applications. The vulnerabilities, which could allow attackers to execute malicious code remotely and potentially compromise servers, sensitive information and connected networks, prompted urgent warnings from cybersecurity authorities worldwide. The flaws also raised concerns for websites using platforms such as WordPress, while governments and organisations in several countries temporarily suspended services to apply security updates. Researchers reportedly used artificial intelligence tools to help identify the vulnerabilities, highlighting AI's growing role in cybersecurity research as well as the risks posed when weaknesses become exploitable. South African presidential spokesperson Vincent Magwenya said there was no indication that the Presidency's website had been breached, emphasising that the shutdown was precautionary. The incident underscores the importance of timely software updates, continuous security monitoring and robust cybersecurity measures for public institutions and other organisations reliant on digital infrastructure. Daily Maverick

PHP2SHELL: CRITICAL SOFTWARE FLAWS PUT THOUSANDS OF SOUTH AFRICAN SERVERS AT RISK



IMAGE SOURCE: MY BROADBAND

A MyBroadband report published on 21 October 2026 warns that more than 9,800 internet-connected servers in South Africa running PHP could face potential exposure following the premature disclosure of two critical software vulnerabilities, CVE-2026-109618 and CVE-2026-109619, collectively associated with the threat dubbed PHP2Shell. The flaws could allow attackers to execute malicious code remotely on vulnerable servers, potentially enabling credential theft, unauthorised access and further compromise of connected systems. Both vulnerabilities received a severity rating of 9.2 out of 10, and the reported exposure included infrastructure operated by major hosting and technology providers. The disclosure occurred before the planned coordinated release, prompting cybersecurity researchers to warn of possible widespread attacks. Recommended precautions included identifying vulnerable PHP installations, applying official security updates as soon as available and isolating internet-facing applications that could not immediately be secured. At the time of publication, major vendors had not confirmed widespread exploitation. The incident highlights the risks created by delayed security updates and the importance of proactive vulnerability management to protect South Africa's digital infrastructure. My Broadband

FNB FINED R1 MILLION AFTER BANKING APP EXPOSES SENSITIVE CUSTOMER INFORMATION



IMAGE SOURCE: IOL

South Africa's Information Regulator has fined First National Bank (FNB) R1 million for contraventions of the Protection of Personal Information Act (POPIA) after a vulnerability in its banking application allowed unauthorised users to access the personal information of 88 home-loan applicants. According to IOL, 696 unauthorised individuals accessed applications containing sensitive information, including identity numbers and, in nine cases, bank account numbers. The regulator's findings focused not only on the technical vulnerability but also on FNB's response after the issue was reported. Although the bank restricted access for the individuals involved, the regulator found that it had failed to address the wider security weakness adequately and had treated repeated reports as separate incidents. The enforcement notice also identified concerns about the collection of personal information from newspaper reports and the indefinite retention of certain records without an adequately stated legal basis. The case reinforces the responsibility of financial institutions to implement effective security safeguards, respond promptly to recurring vulnerabilities and comply with data-protection requirements to prevent unauthorised access to customers' information. IOL

RANSOMWARE THREATENS SENSITIVE RECORDS AT SOUTH AFRICAN INSURER SERVING OVER ONE MILLION WORKERS



IMAGE SOURCE: MY BROADBAND

A MyBroadband report published on 23 October 2026 reveals that Rand Mutual Assurance (RMA), a non-profit insurer established in 1894 that administers workplace injury and illness compensation for South Africa's mining and metals industries, is investigating an alleged ransomware attack by the cybercriminal group Kazu. The group claims to have stolen approximately 366GB of data, including 1.6 million insurance claims records and nearly 594,000 additional files, and has reportedly demanded a ransom of US$98,000 (approximately R1.57 million), threatening to publish the information if its deadline is not met. Samples reviewed by the publication reportedly included identity documents, insurance claims, X-rays, medical certificates and psychological records, raising serious concerns about the potential exposure of highly sensitive personal and medical information. RMA confirmed that it had received an alert about a possible data breach and that investigations were underway, but the alleged theft has not been independently confirmed by the company. The incident highlights the growing risks facing South Africa's insurance sector and the potential consequences of cyberattacks targeting organisations that manage large volumes of sensitive personal data. My Broadband

VERIFY BEFORE YOU PAY: SOUTH AFRICA'S CYBERCRIME SURGE MEETS A COURTROOM RECKONING



IMAGE SOURCE: FA NEWS

Cox Yeats lawyers Mongezi Mpahlwa and Tshilidzi Mudau warn that South Africa remains one of the world's most targeted countries for cyberattacks, with Interpol flagging finance and government as key targets. Kaspersky counted over six million online attack attempts and 10.3 million malware incidents in the first half of 2025, with backdoor attacks up 123%, banking trojans up 136% and password stealers up 122%. Banking customers lost roughly R1.8 billion in 2024 alone, and small and medium-sized businesses face attempted intrusions almost daily. The tactics are familiar but sharper: AI-generated phishing emails are nearly indistinguishable from genuine correspondence, deepfake audio and video are used to impersonate executives and authorise payments, and business email compromise remains the costliest category, with attackers watching email chains for weeks before striking. Ransomware-as-a-service kits sold with customer support let less skilled criminals launch attacks, while telecoms, energy, education and municipalities increasingly join finance and government on the target list. The courts are sending the sharpest message. In a 2025 Supreme Court of Appeal ruling, a purchaser who paid into a fraudster's account without verifying the seller's banking details failed to prove payment, and the court rejected the idea that the seller carried the risk of the payment method it chose. Other judgments, including one over a R5.5 million property payment, follow the same line: if payment is intercepted, the debtor bears the loss. The authors urge callback verification on payments, tested incident response plans, annual reviews of cyber insurance, and scrutiny of supply chain risk, noting that criminals are adopting AI faster than businesses are. FA News.

SOUTH AFRICA BETS ON AN AI-LITERATE SOCIETY TO BEAT AI-POWERED SCAMS



IMAGE SOURCE: SA NEWS

In an opinion piece published by SAnews, GCIS official Josias Pila argues that AI is changing cybercrime, and that South Africa's first line of defence may be an AI-literate society that knows what it sees, hears or reads online can't always be taken at face value. Voice cloning, deepfake videos, AI-generated phishing messages and fabricated identities let criminals impersonate people and institutions so realistically that scams once spotted by poor writing now look and sound authentic. He cites Interpol's 2025 Africa assessment, which points to a sharp rise in attacks on local organisations, and SABRIC data showing a 22% rise in cyber breaches and attacks in 2023, with ransomware payers up 20%. Government, he says, is strengthening cybersecurity awareness, expanding digital skills and developing a national approach to responsible AI governance, while GCIS is stepping up fact-checking and public education to help citizens spot deepfakes and manipulated content. He notes that at the 18th BRICS Summit in New Delhi, President Ramaphosa called for human governance to advance as quickly as AI, and South Africa proposed a BRICS mechanism for independent scientific evaluation of AI, with meaningful human control and reporting of serious incidents. Pila's advice to citizens is to ask whether they can independently verify a request before sending money or sharing personal information, though he stresses that the burden should not fall on individuals alone, with government strengthening frameworks and institutions and businesses embedding cybersecurity and responsible AI practices. SA News

SCAMMED ONLINE IN SOUTH AFRICA? A FREE HELPLINE NOW HAS YOUR BACK



IMAGE SOURCE: BIZ COMMUNITY

MiDO Academy, The Cyber Helpline and Amazon Web Services (AWS) have launched a free, confidential helpline for South Africans hit by online scams, hacked accounts, identity theft and other cybercrime. It offers practical guidance on fraud, investment and employment scams, phishing, sextortion, online harassment and malware, and is open to anyone in South Africa aged 13 and older, including sole traders. Rather than acting as a formal reporting channel, it helps victims understand what happened and limit further harm by securing compromised accounts and devices, preserving evidence and working out where to report, with referrals to banks, SAPS, specialist organisations or mental health services where appropriate. It cannot investigate crimes or recover lost money. An online chatbot gives step-by-step guidance around the clock, and harder cases go to trained human responders through the platform instead of a traditional phone hotline with instant response. The service draws on The Cyber Helpline's UK and US experience, where it says more than two million people have accessed its guidance since 2018. AWS is funding the 12-month pilot and hosting the service, MiDO Academy houses the project and its student volunteer responders, and KnowBe4 Africa supported its conception, giving aspiring security professionals supervised experience with real incidents. The partners say case information is encrypted on AWS infrastructure, accessible only to vetted responders, and shared with other organisations only with the victim's consent. Biz community

WHEN THE SCREENS GO DARK: PRETORIA DECLARES CYBERSECURITY A NATIONAL SECURITY PRIORITY



IMAGE SOURCE: TECH CENTRAL

In an opinion piece for TechCentral, Nonkqubela Jordan-Dyani, director-general of the Department of Communications and Digital Technologies, argues that cybersecurity has moved from a technical matter to a question of national security, as a hospital that cannot reach patient records or a municipality that cannot deliver services shows how attacks ripple through lives and the economy. She cites national CSIR and Cybersecurity Hub surveys from the end of the 2023/2024 financial year, in which 88% of respondents reported at least one security breach and 47% of organisations reported between one and five incidents in the previous year. Government's response, she says, rests on the 2021 Cybercrimes Act and the 2022 Critical Infrastructure Protection Act, alongside the National Cybersecurity Hub, which serves as the national computer security incident response team and coordinates incident response, threat-information sharing and awareness. The State IT Agency is assessing and hardening government infrastructure, and the CSIR is deploying locally developed technology, including its Virtual Cybersecurity Operations Centre. She stresses that laws, technology and institutions are not enough without a culture of cybersecurity, with businesses, especially small and medium-sized enterprises, treating it as a continuity and leadership priority and citizens protecting their personal and banking information, spotting scams and reporting suspicious activity. Jordan-Dyani also frames the field as a skills opportunity in digital forensics, cyber defence and information security research, and says security must be built into new digital systems from the start, concluding that South Africa will face attacks and what matters is how well it prevents, responds and recovers. Tech central

UNHACKABLE? STUDENT WHO CRACKED GOVERNMENT SYSTEMS QUESTIONS SOUTH AFRICA'S DIGITAL ID



IMAGE SOURCE: MY BROADBAND

Cybersecurity researcher and third-year student Joel Cedras, who previously helped expose widespread fraud in South Africa's Social Relief of Distress grants and recently disclosed a breach of Gauteng's e-Panic button app, warns that Home Affairs cannot guarantee its upcoming digital ID will be immune to attack. Minister Leon Schreiber live-demoed the system on 1 October 2026, promising cryptographic keys, device binding and biometric verification, with citizens approving each item of personal information they share through a QR code, and a countrywide rollout expected only after 2030. Cedras calls the idea mostly sound but says the real test is keeping it secure once it is live. He points to weak links beyond Home Affairs' own systems: third-party providers, as seen in the insurance-sector breach that began at MIP Holdings through its Jira platform; the CIPC, which interfaces with Home Affairs and was breached in 2024; and SITA, where he says he found more than 5,000 potential vulnerabilities, plus another 4,400 on other government infrastructure. He is also worried about identity registration and recovery, asking what happens if a criminal registers someone else's identity on their own phone or tricks a victim into approving a request. Cedras says that even perfect encryption means little if criminals can manipulate the surrounding processes. He still believes digital IDs, implemented properly, could make fraud harder than physical documents do, and urges independent testing before rollout and a bug bounty programme. Home Affairs had not responded to MyBroadband's questions by publication.

THE BACK DOOR YOU INVITED IN: WHY YOUR SUPPLIERS ARE NOW YOUR BIGGEST CYBER RISK



IMAGE SOURCE: IT WEB

Richard Frost of Armata Cyber Security argues that third-party supply chain risk has become the threat of 2026 because attackers exploit misplaced trust. He points to a string of South African incidents this year, including Sanlam's July disclosure that client data was exposed through a third-party provider, Profmed's administrator exposing records of more than 200,000 members after attackers compromised credentials at a supporting provider, and a week-long outage at distributor Rectron. The 2025 SecurityScorecard Global Third-Party Breach Report found that 35.5% of data breaches originated from third-party compromises, up 6.5% on the previous year. The entry points are strikingly simple, Frost says: a compromised contractor emails an infected invoice, the company opens it, and the infection travels along an already trusted relationship without defeating any firewall or endpoint. He argues that demanding the same paperwork from every vendor only breeds box-ticking, and that security standards should instead scale with the supplier through zero trust principles: least privilege, multi-factor authentication on all vendor logins, identity-aware proxies, and network segmentation that keeps contractor access on separate VLANs or cloud accounts. He also recommends exit strategies for high-risk third parties and a plan for when things go wrong, noting that the trend is set to continue. His prescription is proportionate governance and visibility, backed by a mitigation playbook of zero trust access, continuous monitoring, full vendor visibility and contractual governance. IT Web

SOVEREIGNTY ISN'T A STREET ADDRESS: WHY SOUTH AFRICAN FIRMS ARE LOSING CONTROL OF THEIR DATA ONE COPY AT A TIME



IMAGE SOURCE: TECH CENTRAL

In a promoted piece by Johan Lamberts, MD of Ascent Technology, the argument is that while South Africa debates where its data should live, the real question is who controls it: residency answers where, sovereignty answers who. Residency is largely solved, he says, with in-country hyperscaler regions and a national policy that imposes no further localisation requirements, but a data centre inside the border says nothing about who holds the keys, who can reach the data, who patches the engine beneath it and who else holds a copy. Control leaks through copies such as nightly extracts, staging databases, spreadsheets and supplier feeds, none of which appear in an asset register, and he cites a Redgate survey finding 77% of organisations have no formal data governance process. He points to September's breaches as proof, with institutions writing to customers even though their own systems were untouched: the Dire Wolf group's claimed theft of 200GB from identity-verification provider RelyComply, and a policy-administration provider's intrusion that exposed around 400,000 records belonging to customers of about 45 insurers. The regulators, he notes, were clear that the obligation to notify rests with the responsible party, not its supplier. Sovereignty is also decided in small settings, such as a Microsoft Fabric tenant toggle that lets AI prompts be processed outside the country, which an administrator can switch on in an afternoon without it being minuted anywhere a director would read. A sovereign organisation, he concludes, can count its copies, hold its own keys where the platform allows, review which credentials reach personal information, know the support status of its database engines, and know what each supplier holds and in which jurisdiction. Tech Central

BEYOND THE SCREEN: TACKLING CYBERCRIME AND TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN SOUTH AFRICA



IMAGE SOURCE: CGE

The Commission for Gender Equality (CGE) highlights how the growing use of digital technologies has created new avenues for gender-based violence in South Africa, including cyberbullying, online stalking, sextortion, sexual harassment, hate speech and the non-consensual sharing of private information. These forms of technology-facilitated gender-based violence (TFGBV) can cause psychological, social, reputational and economic harm, disproportionately affecting women, children, persons with disabilities and LGBTQIA+ young people. The article outlines South Africa's existing legal protections, including the Cybercrimes Act of 2020, the Protection from Harassment Act of 2011 and the Domestic Violence Amendment Act of 2021, while emphasising the importance of digital literacy, public awareness and accountability for technology companies. It calls for stronger survivor-centred support, improved reporting mechanisms and coordinated efforts by government institutions, civil society and communities to address online abuse, challenge victim-blaming and promote safer digital spaces. Ultimately, the CGE stresses that tackling technology-facilitated violence requires both effective legal enforcement and a broader cultural shift towards gender equality and responsible digital citizenship. CGE

28 ARRESTS, $11 MILLION FROZEN: WEST AFRICA'S SCAM CENTERS GET A SOUTHEAST ASIA-STYLE TAKEDOWN



IMAGE SOURCE: POWERS OF AFRICA

Twenty-eight people suspected of cybercrime have been arrested in Ghana and Nigeria in an international operation backed by the United States, the Department of Justice announced, with $11 million in suspected criminal assets frozen and several online fraud networks disrupted. The operation, run with the UK's National Crime Agency, local law enforcement and several tech companies, targeted networks accused of defrauding internet users through investment fraud, romance scams and identity theft. In Ghana, 19 suspects were arrested in a suburb of Accra and 303 electronic devices were seized, with the network allegedly targeting 89 victims for estimated losses of $8.3 million. Authorities also identified 117 suspected human trafficking victims awaiting repatriation to Nigeria, and nine more suspects were arrested in Nigeria. The disrupted schemes included cryptocurrency investment scams, impersonation of law enforcement officers and "digital arrest" extortion, with suspects reportedly using fake job offers, impersonation of military personnel and romance scams often aimed at elderly people. Meta removed more than 3.7 million accounts, pages and groups tied to the fraud, and Adobe, Binance, Coinbase, Google, Microsoft and OpenAI also contributed. The Justice Department noted similarities with scam centers previously dismantled in Southeast Asia, which operate like organized businesses that recruit and train people in psychological manipulation before launching coordinated campaigns across multiple platforms. U.S. Attorney Jeanine Pirro warned that these operations are becoming increasingly sophisticated, organized and linked to human trafficking. Powers of Africa

AFRICA'S SMART PORTS FACE GROWING CYBERSECURITY RISKS AS AI ADOPTION ACCELERATES



IMAGE SOURCE: PUNCH

An article published by Punch Newspapers on 22 October 2026 reports that Abubakar Dantsoho, Managing Director of the Nigerian Ports Authority and President of the Port Management Association of West and Central Africa, has warned that the growing adoption of artificial intelligence and interconnected digital systems could expose African ports to cyberattacks capable of disrupting international trade and supply chains. Citing the 2021 cyberattack on South Africa's Transnet and incidents affecting Japan's Port of Nagoya and DP World terminals in Australia in 2023, Dantsoho stressed that cyber incidents can interrupt cargo movements, revenue collection and essential port operations. He called for cybersecurity to be integrated into maritime security through the separation of operational technology from administrative networks, stronger security requirements for technology partners, regular testing of recovery systems and staff training. He also advocated regional intelligence sharing and common digital standards to strengthen cooperation between African ports. While AI could improve cargo management, vessel scheduling and equipment maintenance, the article emphasises that digital innovation must be accompanied by robust safeguards to protect critical infrastructure and economic stability. Punch

ISS ANALYSIS MAPS HOW ANTHROPIC'S THREAT REPORT PLAYS OUT ACROSS AFRICA



IMAGE SOURCE: IAFRICA

An analysis by consultant and former BBC correspondent Karen Allen for the Institute for Security Studies reads Anthropic's September threat intelligence report through an African lens, with cases spanning Kenya, the Central African Republic, the DRC, Sudan and Mali. The most striking case is the breach of an unnamed North African government technology authority, in which AI agents were used to collect information, run reconnaissance and build the infrastructure for an intrusion that exposed more than 300,000 national identity records and data on over 500,000 companies. Allen sets this against the scale of exposure: some 45 African governments now run digital service-delivery systems, and INTERPOL warns that 55% of reported cybercrime across Africa is AI-enabled, though one industry executive says fully automated attacks have not arrived yet. Elsewhere, Claude models were used in surveillance in Mali to target and profile opposition figures, and in the Central African Republic operators used the model to strip formatting from AI-generated content for a network of fake radio stations, defeating detection systems that look for synthetic-text signatures. In the DRC, investigators found 318 articles across fake news sites, and ahead of Kenya's elections the model generated batches of tweets made to look like spontaneous grassroots commentary, including a false narrative that the opposition was breaking apart. Anthropic says it disrupted most of these operations but acknowledges that better detection requires intelligence sharing between the private sector and governments, and Allen identifies obstacles at home and abroad, including a recent Pentagon boycott of Anthropic and siloed South African cybersecurity. South Africa's state-led Cybersecurity Co-ordination Centre, promised a decade ago, still does not exist, and its draft national AI strategy was withdrawn in April over fabricated citations, with a redraft due by March 2027. Allen's immediate recommendation is basic AI usage policies, since staff experimenting with public models risk feeding in sensitive data and exposing their organisations to further intrusion. iAfrica

PREVENT, DETECT, RESPOND... ANTICIPATE: NEC XON WANTS AFRICA'S CYBERSECURITY TO THINK LIKE THE ATTACKER



IMAGE SOURCE: MY BROADBAND

Armand Kruger, Head of Cybersecurity at NEC XON, argues in a sponsored MyBroadband piece that the traditional defensive model of building a perimeter and responding to breaches is no longer enough as Africa's digital economy expands. He cites INTERPOL's latest Africa Cyberthreat Assessment, in which two-thirds of surveyed countries said cyber-related crime makes up a medium-to-high share of all crime, and which warns that criminal use of AI and synthetic media is outpacing many agencies' ability to respond. Kruger's answer is to add an "anticipate" step: continuously examine the environment as an attacker would, to find exposed assets and the identities, credentials or connections that could give an intruder a way in, with the aim of cutting the number of viable attack paths. He points to Gartner's list of trends reshaping the field, including generative AI, supply-chain interdependencies, skills shortages and the growing number of machine identities created by AI, cloud and automation, and says the attack surface is now an ecosystem of people, identities, applications, machines, cloud services, suppliers and data. He also warns that piling on tools can add risk if they are poorly integrated, because security is measured by how much risk is removed, not by how many products are owned. He urges strategies tailored to Africa's varied connectivity, regulation and skills, framing cybersecurity as business resilience and not just an IT issue. Attackers are already automating, he says, so defenders must too, as long as automation reduces complexity. He closes by calling for a shift from "prevent, detect and respond" to "anticipate, prevent, detect, respond and recover." My Broadband

AFRICA'S $1.5 TRILLION DIGITAL BOOM HAS A SECURITY PROBLEM, AND MASTERCARD WANTS EVERYONE AT THE TABLE



IMAGE SOURCE: ENGINEERING NEWS

Mastercard says Africa's fast-growing digital economy and e-commerce are exposing more information and value to cyberattacks, which makes effective cybercrime defences an enabler of economic growth and calls for a partnership approach across the whole digital ecosystem. A Mastercard senior vice president argued that as African markets move rapidly into digitalisation, mobile money, digital finance and e-commerce, countries must build infrastructure that protects people and creates the trust commerce depends on, and that cybersecurity is a shared responsibility requiring public-private and cross-border collaboration. The warnings come from Mastercard's Africa cybersecurity whitepaper, which says mobile money use grew sixfold between 2016 and 2025, e-commerce about fourfold and digital banking users 4.7 times, and which flags Kenya's M-Pesa ecosystem as critical infrastructure that could attract cybercriminals. The report projects that Africa's digital economy could reach $1.5 trillion by 2030, and names technology, public institutions and financial services as major targets because they hold personal information, business systems and financial assets. Personal information, financial information and customer-facing services together made up 27% of targeted assets. The paper follows Mastercard's June launch of its Africa Cybersecurity Center of Excellence, which aims to bring together CISOs, business leaders and security practitioners for secure information sharing, joint exercises and coordinated response. Engineering News

SPENDING MORE, PROTECTED LESS? AI-POWERED CRIMINALS ARE LEAVING AFRICAN DEFENDERS WEEKS BEHIND



IMAGE SOURCE: IT WEB

Experts from Kaspersky, Mimecast, Check Point and Galix told ITWeb Africa that African organisations are struggling to match the speed of AI-enabled cybercrime even as security spending rises, with attackers operating at machine speed. INTERPOL puts African cybersecurity spending at $15.3 billion in 2025, and estimates direct economic damage at about $5 billion, far above the $484 million in reported losses. Kaspersky found that 85% of South African SMBs raised their security budgets, yet 78% still suffered at least one incident in the past year. Check Point's Lionel Dartnall says African organisations took an average of 18 days to detect and contain a breach, against 12 days globally, and urges a move beyond compliance to continuously testing whether controls actually work. Mimecast describes an industrialised, AI-enabled criminal economy in which breaches feed synthetic identity fraud, AI-generated phishing and business email compromise, and cites attacks on Nigeria's Customs Service, Uganda's power transmission company and Namibia's Paratus Telecom. Attackers also hop from email to Microsoft Teams and then phone calls to slip past controls that watch only one channel. Mobile money is under pressure too: INTERPOL says Kenya detected more than 123,000 fraudulent SIM cards in 2025, used to drain an estimated $3.8 million from mobile wallets. The experts agree that technology alone won't close the gap, pointing to unpatched routers, vulnerable VPNs and shadow IT. Kaspersky's Chris Norton says spending more does not automatically mean stronger protection, and Mimecast's Heino Gevers calls it more a practice problem than a technology problem. IT Web

THE DOUBLE-EDGED SCREEN: IS SOCIAL MEDIA AFRICA'S BIGGEST NEW SECURITY FRONTIER?



IMAGE SOURCE: SPUTNIKNEWS

Africa's digital landscape is being transformed by more than 600 million internet users, a thriving creator economy and growing investment in AI and data infrastructure, and security and policy experts say this expansion has become a critical new frontier for national security. On Sputnik Africa's Redrawn Africa podcast, Dr. Chris Mitchell Osazuwa, an associate professor of Intelligence and Security Studies at City University in Cambodia, warns that the same tools letting African creators, journalists and storytellers bypass Western gatekeepers are also being weaponized by external actors seeking to destabilize the continent. He argues that as foreign and domestic actors exploit these networks, African defense and intelligence agencies face a constant challenge in securing critical data infrastructure while protecting democratic institutions from digital subversion. He also claims that outsiders offering technology help are sometimes gathering open-source and social media intelligence, and says that Africa owning its own technology would let it control its own narratives. Sputniknews

ONE ATTACK EVERY EIGHT MINUTES: MASTERCARD'S WHITEPAPER MAPS AFRICA'S DIGITAL DEFENSE RACE



IMAGE SOURCE: MASTERCARD

Mastercard's "Africa's Digital Defense Race" whitepaper draws on Mastercard Cyber Insights, law-enforcement intelligence and expert interviews to examine cyber threats across South Africa, Nigeria, Morocco and Kenya. Cyber attacks in Africa rose 421.4% between 2016 and 2025, against 307.3% globally, and Mastercard recorded 69,236 observed cyber events against African organizations in 2025, roughly one every eight minutes. Nigeria, South Africa, Morocco and Kenya took 54.7% of that activity, while technology, public sector and financial services organizations accounted for 44% of observed threats. More than 60% of attributed events were linked to blackhat hackers and organized cybercriminal groups, and the continent has about 200,000 unfilled cybersecurity positions, a 23% workforce gap. The stakes are rising because Africa's digital payments market is expected to reach $1.5 trillion by 2030, and the report warns that cybercrime damages trust, slows innovation and raises business costs for governments, financial institutions, SMEs and consumers. It also covers attack methods, regulation and governance, and national readiness, and sets out four priority actions for strengthening digital trust and resilience. Mastercard

AI-DETECTED PHP VULNERABILITIES TRIGGER GLOBAL CYBERSECURITY ALERT



IMAGE SOURCE: ALJAZEERA

A report by Al Jazeera, published on 22 October 2026, details how two critical vulnerabilities in PHP, a programming language used by more than 70% of websites worldwide, prompted governments and organisations across several countries to temporarily take websites offline while applying security updates. The vulnerabilities, dubbed PHP2Shell, could allow attackers to execute commands remotely on unpatched servers, potentially exposing sensitive information and compromising website systems without requiring legitimate account access. Researchers at cybersecurity firms Calif and Wiz identified the flaws with the assistance of artificial intelligence (AI), highlighting how AI can accelerate the discovery of previously difficult-to-detect security weaknesses. The United States National Security Agency issued an urgent warning, while authorities in Germany, France, Belgium, the Netherlands, Finland and other countries took precautionary measures to protect their systems. The incident underscores the vulnerabilities of shared digital infrastructure and the growing dual-use implications of AI, which can strengthen cybersecurity defences while also helping attackers identify weaknesses. Experts and the PHP Foundation have called for immediate software updates and coordinated action to prevent exploitation, emphasising the importance of maintaining and securing the digital systems on which governments, businesses and the public depend. Aljazeera

XWORM GROWS EYES AND EARS: LEAKED RAT NOW DOUBLES AS A SURVEILLANCE PLATFORM

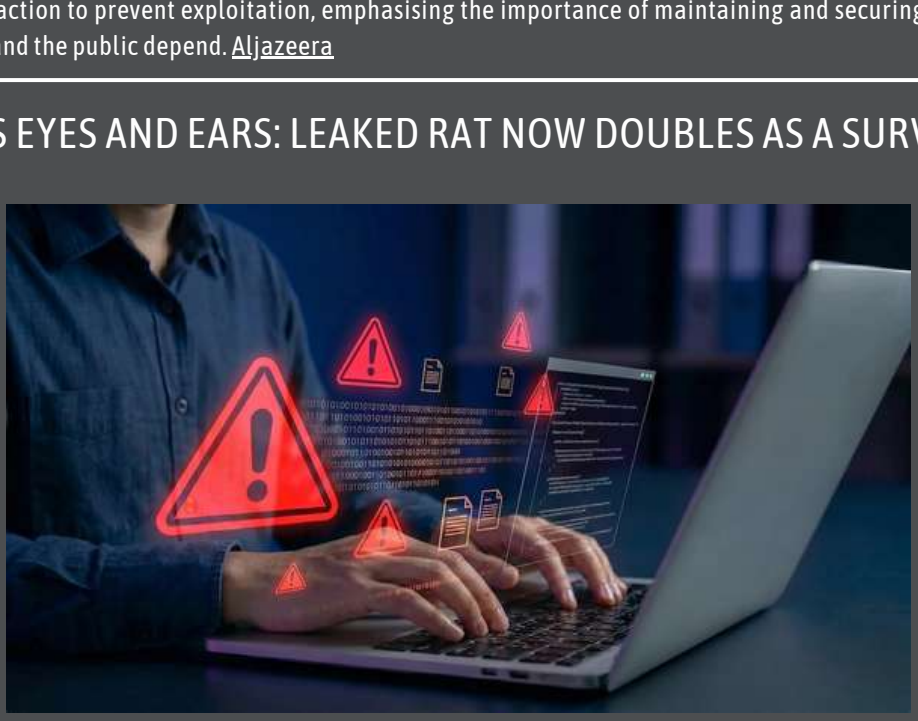


IMAGE SOURCE: SECURITY WEEK

Netskope reports that the developers of XWorm, a Windows RAT first seen in 2022 that already offers keylogging, screenshots, webcam access and payload execution, have added plugins that turn it into a surveillance platform. The new capabilities include location tracking, live audio streaming, webcam capture and interactive control of authenticated browser sessions. Three plugins matter most: Maps, Microphone and HBrowser. HBrowser goes beyond stealing credentials by giving the operator a live view of the victim's running browser and relaying the operator's mouse, keyboard and paste actions into it. One modified setting stays in place, so later location requests keep bypassing user permission. Activity has surged since a cracked version of the builder leaked in June 2025 and the source code for version 6.4 followed in August 2025, and Netskope expects continued upgrades to the toolkit. Netskope's October 2026 analysis covers builds V6.4, V6.5 "XWorm Reborn," V7.2 and V7.4, but the findings describe specific observed variants, and "surveillance platform" is not an official classification or a claim that every infection includes every feature. Security Week

HACKING THE COURTROOM: WHEN SPYWARE LITIGATION PUTS THE JUSTICE SYSTEM IN THE CROSSHAIRS



IMAGE SOURCE: ATLANTIC COUNCIL

An Atlantic Council issue brief by Lisandra Novo asks how safe the justice system is when the world's most sophisticated hacking tools are in the hands of those it prosecutes, noting that threat actors have repeatedly breached the US federal court filing system and stolen sealed material such as the identities of confidential informants and witnesses. The brief centers on a split between two spyware cases: Apple moved in 2024 to voluntarily dismiss its suit against NSO Group, saying adversaries seek its security information by any means necessary and that no protective measure could mitigate the risks of disclosure, while WhatsApp pressed on against the same company and won a multimillion-dollar victory despite facing the same discovery threats. Novo argues that building a secretive system that denies a litigant the right to be heard is not the answer, and that existing protections such as protective orders and "attorneys' eyes only" designations are valuable but not absolute, since judges can modify them. Technical fixes such as multifactor authentication and standardized redaction are the bare minimum, she says, and should be paired with non-technical measures like time-limited on-premises access to physical documents that stay out of digital case systems until a set date. She also floats creating certificates of confidentiality for security researchers, modeled on the system that shields the identities of health-research subjects, while acknowledging it raises hard questions, including who counts as a researcher and whether Apple's own threat team would qualify. Finally, she notes that civil plaintiffs only need to meet the preponderance-of-evidence standard, which can be done with material safe to disclose without endangering whole research programs, so the answer to technical problems does not always lie in technical solutions. Atlantic Council

YOUR SMART OVEN COULD BE NEXT: ANTHROPIC WARNS SMALL AI MODELS ARE MONTHS FROM SELF-REPLICATING ACROSS HOME DEVICES



IMAGE SOURCE: WFMY NEWS 2

Anthropic says its experiments suggest small AI models may be months away from being capable enough to self-replicate on commercial internet-of-things devices, like smart ovens and off-brand Android TV boxes. The company warns that such models could form distributed botnets running AI workloads without relying on data centers, though its researchers did not demonstrate a fully autonomous, self-replicating AI worm on real IoT hardware. They did successfully distribute Google DeepMind's Gemma4-26B-A4B model across 15 off-brand Android TV boxes. Anthropic notes that a replicator like this would be hard to shut down because there is no centralized point to turn off, though it might spread slowly, with a doubling time of days. Homes and small businesses would probably be the first targets, and the devices Anthropic lists as susceptible include smart TVs, automatic lawnmowers, security cameras and video-conferencing units. If smaller models keep improving at their historical rate, the company predicts they could reach the necessary capability before the end of 2026. Anthropic acknowledges that a fully rogue self-replicating model does not yet exist, but says agents are getting better at completing individual replication steps and passing adaptations to future copies, and that slow replicators would be an early warning of faster, more aggressive models able to breach better-protected machines or steal API keys. The researchers conclude that the form AI replication could take remains unclear. WFMY News 2

COLD CHAIN, HOT HACK: ATTACKERS TURN FRENCH SUPERMARKET FRIDGES INTO OVENS



IMAGE SOURCE: TECHADU

Hackers remotely took over the temperature controls of fridges and freezers at hundreds of French supermarkets, heating units to as much as 50°C, spoiling stock worth millions of euros and starting fires in some stores. Carrefour, Monoprix, Intermarché and Coopérative U all reported their fridges heating overnight. The attackers reportedly hijacked controllers running older Danfoss software and abused a built-in automatic defrost function to raise temperatures. CERT-FR says it knows of numerous compromises affecting two Danfoss controller series, the AK-SM and AK-SC, and advises disconnecting them or filtering access, noting that exposing a management interface to the internet goes against good practice. Danfoss said most of the units hit were older models it no longer updates. Neither French authorities nor Danfoss has said who was behind the attack or how the controllers were breached. Claroty's Team82 had detailed weaknesses in the Danfoss AK-SM 800A controller on August 9 that could let intruders bypass authentication and run code, and experts told Reuters the known flaws meant the attackers were pushing at an open door. Danfoss fixed three flaws in the newer AK-SM 800A in 2025, though no one has linked them to this attack. Reuters found at least 4,500 Danfoss interfaces still viewable online days later, and no group has publicly claimed responsibility. Technadu

AHOLD DELHAIZE PULLS THE PLUG ON SYSTEMS AFTER CYBERATTACK, ITS SECOND IN TWO YEARS



IMAGE SOURCE: SECURITY WEEK

Dutch-Belgian grocery giant Ahold Delhaize disconnected some of its systems in response to a cyberattack. The company said it was experiencing a security issue within its network and was taking steps to assess and mitigate it, including taking some systems offline to help protect them. It stressed that its stores remain open and that its ability to serve customers has not been affected. The retailer runs more than 9,400 stores across the United States, Europe and Indonesia, and the disruption hit employee services and customer-facing websites across several of its brands. An Ahold Delhaize spokesperson pointed BleepingComputer back to the company's statement when asked whether corporate and store systems were both affected, whether disruption was worldwide, and whether any devices were encrypted. This follows a November 2024 attack that hit Giant Food pharmacies and Hannaford supermarkets, as well as Food Lion, The Giant Company and Stop & Shop. That earlier incident ultimately compromised the personal, financial and health data of more than 2.2 million people. Security Week

NO EXPLOIT REQUIRED: THREE GOVERNMENTS WARN THAT A FRIENDLY CHAT IS NOW THE STATE-BACKED HACKER'S WAY IN

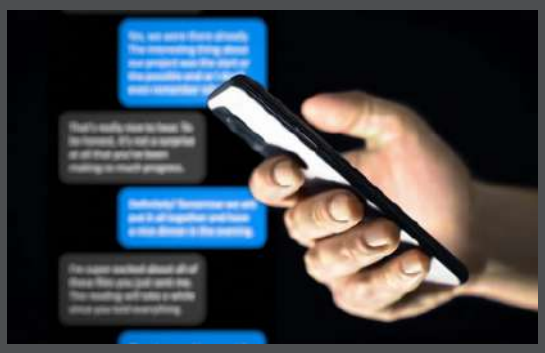


IMAGE SOURCE: BLACKBERRY

In a blog post, BlackBerry describes coordinated warnings from the FBI, the UK's NCSC and the Netherlands' AIVD that state-sponsored actors are now using consumer messaging platforms as a primary attack vector. The agencies' joint advisory of September 15, 2026 covers CHOSEN BRICK, Windows spyware used since at least 2025 against dissidents, activists and journalists. The advisory cites no CVE and nothing in the chain is exploited. Attackers research a target, then open a conversation on WhatsApp, Telegram or social media while posing as a known contact or technical support, building rapport over days or weeks before sending a Windows executable disguised as software such as Norton Antivirus or Adobe Flash Player, or even MRI scan results. When the work device is likely to block the file, the attacker asks the target to open it on a personal device, outside managed controls. Once installed, the malware persists through a registry Run key, adds a Microsoft Defender exclusion, and uses Telegram for command and control with a separate bot ID per victim device. It can capture the screen and microphone and steal email and Telegram and WhatsApp data. No agency published a victim count, and personal details of some earlier victims have appeared on leak sites, putting physical safety at stake alongside data loss. BlackBerry says the weakness lies in reachability, not encryption, because consumer platforms let anyone with a number or username start a chat. It recommends hunting for the named host artifacts, briefing staff to refuse requests to open files on personal devices, naming a channel of record for sensitive coordination, and treating consumer messaging apps as an initial-access surface in threat modeling. Blackberry

OLD BREACHES, NEW DANGER: AI FIRM LEAVES 13.7 MILLION STOLEN CREDENTIALS OPEN TO ANYONE



IMAGE SOURCE: SECURITY MAGAZINE

Researcher Jeremiah Fowler discovered a database holding 13.7 million records with no encryption or password protection, traced to a data intelligence platform linked to Vibetech, an India-based IT services and AI software development company. It held data compromised in earlier breaches, including names, email addresses, phone numbers, passwords and bank account data, drawn from datasets such as the AT&T breach and the FBI employee directory breach. Even though the data was breached before, re-exposing it matters: collecting the records into one easily searchable database makes them simple for cybercriminals to use, and older credentials can keep their value for years as attackers use historical breach data to identify victims. It is unclear whether malicious actors accessed the database before Fowler found it. Security magazine

A CRAFTED CERTIFICATE IS ALL IT TAKES: FLAW IN VERCEL SANDBOX LETS ROGUE AI AGENTS SLIP OUT



IMAGE SOURCE: THE RECORD

Researchers at AI security startup AIR say a network filtering flaw in Vercel Sandbox, a tool that runs code in isolated environments, could let rogue AI agents leak sensitive data by bypassing the restrictions meant to keep them contained. Developers normally use network allowlists so agents can only talk to approved destinations, but AIR found that agents could exploit how servers handle digital certificates to get around them. In the researchers' demonstration, a specially crafted certificate sent to an approved server triggered a request to an attacker-controlled server, so data left the network without the sandbox ever contacting the unauthorized destination directly. AIR's report put it bluntly: the wall meant to keep secrets in has a door, and the agent holds the key. AIR co-founder and CTO Niv Hoffman calls it a very hard leak to patch, since from the sandbox's perspective everything looked fine, and says Vercel told his team it needs time to work out how a fix would work. AIR has found no evidence of exploitation in the wild but can't rule it out, and the flaw appears to be longstanding. Hoffman warns that even a standard hardened sandbox today can let a rogue agent escape and act in the wild, and Orcus CEO Nic Adams says the case shows an approved server can become an unwitting courier for stolen credentials, so security must account for what happens after the first connection. Vercel did not immediately respond to a request for comment. The Record

META'S GITHUB BREACH: ONE STOLEN LOGIN, SOURCE CODE GONE, 1,500 PEOPLE NOTIFIED



IMAGE SOURCE: SECURITY WEEK

Meta is notifying roughly 1,500 people, most of them US employees, that their personal information was affected after hackers got into some of its GitHub repositories. The attackers reportedly used the credentials of a single employee to reach internal repositories and copy software code tied to some Meta products along with the personal data. Meta told SecurityWeek that 99% of the stolen data was business data, in the form of product code, and the remaining 1% was personal data. That personal information had been improperly stored on the platform against company policy. Meta also says a significant portion of what looked like personal data was synthetic or anonymized test data, so the attackers may struggle to tell real records from test ones, and it doesn't believe the hackers were specifically after its data, based on its investigation with GitHub so far. Meta says this was not a vulnerability in any of its products and its internal systems were not breached. It has cut off the attackers' access, is offering monitoring services and is adding controls to detect personal information uploaded to GitHub by mistake. Meta hasn't said which types of personal data were involved, or who the attackers were. Security Week

INTERPOL CYBERCRIME CRACKDOWN ACROSS AFRICA NETS 1,462 ARRESTS AND RECOVERS $105 MILLION



IMAGE SOURCE: TECH AFRICA

An article published by TechAfrica News on 27 October 2026 reports that an INTERPOL-coordinated operation, Operation Serengeti III, resulted in the arrest of 1,462 suspects, the disruption of 10,909 malicious networks and the recovery of more than US$105 million in illicit funds across 21 participating countries. Conducted between 29 June and 31 August 2026, the operation targeted cyber-enabled fraud, ransomware, business email compromise, online scams and digital extortion, identifying 65,929 victims and linking criminal activities to estimated losses exceeding US$385 million. In Uganda, authorities dismantled two transnational fraud networks and arrested 365 foreign nationals suspected of involvement in online investment and pension scams, while investigations in Nigeria uncovered large-scale phishing operations and suspected investment fraud involving millions of dollars. Authorities in Angola, Tanzania, Gabon and the Republic of Congo also disrupted various cybercrime operations. Supported by international cybersecurity companies and intelligence-sharing partnerships, the initiative highlights the importance of cross-border cooperation in combating increasingly sophisticated digital crime. However, with several investigations ongoing, the findings also underscore the continuing challenges facing African countries in protecting individuals, businesses and financial systems against evolving cyber threats. Tech Africa

SWEDEN RESTRICTS CHATGPT AND CLAUDE FOR CIVIL SERVANTS OVER DATA SECURITY CONCERNS



IMAGE SOURCE: 360 MOZAMBIQUE

An article published by 360 Mozambique reports that Sweden's government has restricted civil servants from using OpenAI's ChatGPT and Anthropic's Claude for official work, citing concerns about information security and the handling of sensitive government data. The restrictions, which took effect on 26 October 2026, prevent staff from accessing the browser-based versions of the tools on government work computers, following concerns that information entered into unapproved AI platforms could be exposed to external providers without adequate contractual safeguards. Instead, officials are directed to use Microsoft Copilot, which has undergone a government security review and operates under a formal agreement. However, access to ChatGPT and Claude remains possible for some employees through a dedicated, government-approved AI platform. Sweden's Tax Agency and National Board of Institutional Care have reportedly introduced similar restrictions, while other public agencies are reviewing their policies. The decision highlights the growing challenge governments face in balancing AI-driven efficiency with data protection, confidentiality and national security, underscoring the importance of clear policies governing the use of AI tools in public institutions. 360 Mozambique

REPRESSIVE MONITOR

BIG BROTHER NIGERIA: SURVEILLANCE SPENDING TARGETS CRITICS WHILE INSECURITY PERSISTS



IMAGE SOURCE: PULITZER CENTER

A Pulitzer Center investigation by Ajibola Amzat reveals how the Nigerian government has spent billions of public funds on surveillance technologies ostensibly intended to combat terrorism and insecurity, but which have increasingly been used to monitor, track and arrest government critics, journalists, activists and opposition politicians. Drawing on budget data, interviews and documented cases, the investigation highlights how surveillance capabilities were deployed against participants in the 2024 #EndBadGovernance protests, raising serious concerns about violations of privacy, freedom of expression and the right to protest. Despite a sharp increase in security spending, including more than N1.4 trillion in capital budget allocations to key security and intelligence agencies between 2016 and 2026, terrorism, banditry and kidnappings remain persistent threats. The investigation exposes the lack of transparency and accountability surrounding surveillance procurement and questions whether these technologies deliver meaningful security benefits or instead strengthen state repression at the expense of democratic freedoms. Pulitzer Center

SIX YEARS AFTER #ENDSARS: DIGITAL SURVEILLANCE AND THE CONTINUING CRACKDOWN ON DISSENT IN NIGERIA



IMAGE SOURCE: TRUTH NIGERIA

A report by TruthNigeria, published on 21 October 2026, examines allegations that Nigerian authorities continue to use digital surveillance, restrictive legislation and police force against activists, journalists and government critics, six years after the #EndSARS protests against police brutality. Citing investigations and budget data, the report states that Nigeria imported an estimated $6.61 billion worth of spyware tools between 2015 and 2024, raising concerns about the use of public resources to monitor citizens while terrorism, insurgency and kidnapping remain persistent security challenges. It highlights cases of individuals allegedly tracked and detained after criticising government performance online, alongside renewed concerns about police conduct during the October 2026 #EndSARS anniversary memorial in Lagos, where officers reportedly used tear gas against participants. Human rights advocates argue that the disbandment of the Special Anti-Robbery Squad (SARS) has not sufficiently addressed deeper problems of police accountability and excessive force. The report calls attention to the need for lawful surveillance, stronger oversight, protection of constitutional privacy and freedom of expression, and accountability for alleged human rights violations. Truth Nigeria

WHEN SMART CITIES BECOME SURVEILLANCE STATES: THE RISKS OF DIGITAL MONITORING IN AFRICA



IMAGE SOURCE: THE INDEPENDENT

In an article published by The Independent Uganda on 25 October 2026, Wairagala Wakabi examines how smart-city technologies, including CCTV cameras, facial recognition, automatic number plate recognition and vehicle-tracking systems, are increasingly raising concerns about privacy and political freedoms across Africa. Using Uganda's Automated Express Penalty System (EPSAuto), which was suspended following public backlash over incorrectly attributed traffic fines, the article illustrates how technologies introduced for public safety can be repurposed for other forms of monitoring. Research covering 11 African countries identified more than US$2 billion in spending on public-space surveillance, much of it financed by Chinese companies, while finding no compelling evidence that these systems have reduced terrorism or serious crime. The article warns that surveillance can enable authorities to identify and track activists, journalists, opposition figures and protesters, creating a chilling effect on freedom of expression, movement and peaceful assembly. It also highlights the risks of opaque procurement contracts, foreign control of surveillance infrastructure and inadequate safeguards for personal data. Wakabi calls for transparent procurement, independent human-rights impact assessments, stronger legal protections and effective oversight to ensure that surveillance technologies serve legitimate public-safety objectives rather than political control. The Independent

FROM PROTEST TO SURVEILLANCE: HOW EUROPE IS EXPANDING DIGITAL MONITORING OF DISSENT



IMAGE SOURCE: TECH POLICY

In an article published by Tech Policy Press on 22 October 2026, Lauren Mushro examines how European governments are increasingly using surveillance technologies, digital restrictions and security laws to monitor protests and constrain dissent. Drawing comparisons between France's 2026 demonstrations and Catalonia's 2019 independence movement, the article highlights documented cases of Pegasus and Candiru spyware targeting activists, lawyers and civil society figures, alongside the use of facial recognition, algorithmic video surveillance and platform takedown requests. In France, expanded algorithmic surveillance powers and reports of police facial recognition use have raised concerns about privacy, discriminatory policing and the potential targeting of protesters. The article argues that broad security classifications can blur the distinction between peaceful civil disobedience and violence, allowing surveillance measures to extend beyond those responsible for unlawful acts. It calls for stronger independent oversight, transparency around government requests to digital platforms, restrictions on spyware targeting civil society and safeguards for protest-related data. Ultimately, it raises concerns about how the growing use of surveillance technologies and security legislation across Europe could undermine freedom of expression, peaceful assembly and democratic participation. Tech Policy

MADE IN EUROPE, USED FOR REPRESSION: HOW EU SURVEILLANCE TECH FUELS ABUSE ACROSS THE MIDDLE EAST AND NORTH AFRICA



IMAGE SOURCE: THE TAHIR INSTITUTE

Writing for the Tahrir Institute for Middle East Policy, Nonresident Fellow Ramy Raoof Halim argues that European surveillance technology continues to enable repression across MENA because weak EU export controls leave the trade largely unchecked. He points to the French case against Nexa Technologies, formerly Amesys, indicted for complicity in torture and enforced disappearance over its "Cerebro" mass surveillance system sold to Egypt, where intercepted data was used to locate, arrest and interrogate people. MENA regimes favour European tools such as FinFisher, Intellexa's Predator and Bulgaria-based Circles, he says, because they offer reliability and come bundled with training, updates and on-site maintenance, while products sold as counter-terrorism or law-enforcement equipment are repurposed to spy on activists, journalists and queer communities.</consite> He says the EU's 2021 Dual-Use Regulation requires member states to weigh human rights before approving surveillance exports, but Commission guidelines let states report licensing data in aggregate, creating a "transparency black hole" that makes it impossible to link a specific sale to a specific country, and its catch-all clause for unlisted tech relies on companies self-reporting. Human Rights Watch freedom-of-information data show Finland processing export applications to Egypt for IMSI catchers and the Czech Republic for phone forensic tools, Bulgaria licensing Circles for sales to Jordan and Morocco, and Sweden's MSAB exporting phone-extraction devices that escape surveillance controls under a guidelines exception. Halim calls for disaggregated public licensing data, mandatory denials where repression is a clear risk, judicial remedies for MENA victims in European courts, and genuine human rights due diligence by companies, while warning that firms evade controls by relabelling products as general IT tools, routing sales through non-EU subsidiaries, or citing commercial secrecy. The Tahrir Institute

ADFECTION: A SINGLE AD IMPRESSION IS ENOUGH TO INFECT YOU WITH MERCENARY SPYWARE



IMAGE SOURCE: CITIZEN LAB

Citizen Lab has published what it calls the first public confirmation of zero-click mercenary spyware delivered through targeted ads, a technique it names AdFection, which was used to infect devices at Al Jazeera with Candiru's spyware. The ads were bought by Discover-Tech, an Israeli company that presents itself as a legitimate advertising firm but, according to the researchers, operates as a facilitator for several mercenary spyware partners. Its Controlium platform lets those partners de-anonymize, fingerprint and automatically infect devices the moment an ad renders. At least 45 Al Jazeera devices were targeted in 2024 and 2025, and network logs showed the same sequence each time: contact with Discover-Tech infrastructure, then a Candiru validator server, then a command-and-control server. An analysis of nearly four billion bidding records found Discover-Tech's ads on almost 200,000 apps and websites between March and June 2026. About 19% of bids were for ads carrying a script tag that phoned home to a server deciding which targets received code, with impressions seen on networks including NATO, the United Nations, EU institutions, defense ministries and media organisations, though an impression alone does not confirm infection. The researchers also link the company to other mercenary firms, including Bindecy and the ADINT vendor Intelos, and to a threat actor they call DARK CARTOGRAPHER, which exploits mobile carrier flaws to match advertising IDs with phone numbers across more than 30 countries. Discover-Tech sat on Google and IAB Europe vendor lists from 2020 until 2026 and has ties to Eric Banoun, a figure in Israel's surveillance industry who co-founded Circles and Senpai Technologies. After Citizen Lab's disclosure, Google, IAB Europe, Beeswax, Vungle (Liftoff) and Eskimi cut Discover-Tech's access to the ad ecosystem, and the researchers call on regulators to investigate whether Discover-Tech and Candiru broke the law. Citizen Lab

AI JOINS THE DRAGNET: HOW GENERATIVE AI IS SUPERCHARGING CROSS-BORDER REPRESSION



IMAGE SOURCE: JUST SECURITY

Citizen Lab researchers writing in Just Security argue that generative AI is being built into the machinery of transnational repression, drawing on Anthropic's September 2026 threat intelligence report. In the most striking case, a China-aligned operator used Claude to track Uyghurs living in Syria and recruit informants, with the model translating messages, handling local dialects and geolocating people, and the operators targeting those facing financial hardship or separation from family in Xinjiang. The authors say the report shows AI cutting the cost of repression by standing in for language skills and analyst expertise, turning scattered digital traces into detailed target intelligence, and powering recurring workflows such as a Chinese contractor's daily briefings cataloguing dissidents and diaspora communities as threats. They add that AI-assisted surveillance can feed real-world coercion, including the identification of targets' family members and the compilation of floor plans of religious venues. Other cases include a Mali contractor who built a mass surveillance product for roughly 25 million SIM cards that keeps running on local models even after the account was banned, and a police academy student who got surveillance reports after re-prompting the model past an initial refusal. The authors call for frontier AI labs to publish detailed incident reports, notify affected communities, build detection that flags combinations of capabilities rather than overtly repressive language, and preserve evidence for future investigations. They also note that the report reflects only one company's visibility over a short period. Just Security

UNDERCOVER AGENTS, SIGNAL CHATS AND CUSTOMS SUBPOENAS: INSIDE DHS'S SURVEILLANCE CAMPAIGN DURING OPERATION METRO SURGE

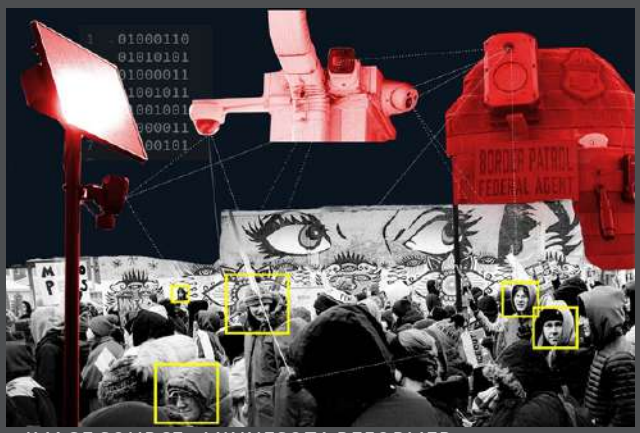


IMAGE SOURCE: MINNESOTA REFORMER

Homeland Security investigators secretly recorded conversations, infiltrated Signal chats and obtained financial records for labor unions and progressive groups during Operation Metro Surge. Undercover agents attended meetings where organizers planned protests and food distribution for immigrants in hiding. At one meeting, agents collected attendees' license plate numbers to identify them. DHS also used a customs law, normally meant for checking whether importers paid the right fees, to gather large amounts of information on unions, left-wing organizations and journalists. Summonses were sent for flight and rental car records and for information tied to social media accounts. Agents also subpoenaed website registrars and payment processors to confirm who created certain sites. The surveillance went beyond Minnesota and included peaceful protests unrelated to the operation, according to a court filing. Whether any of it was illegal could shape the outcomes for dozens of Minnesotans facing charges over anti-ICE protests, all of whom have pleaded not guilty. One First Amendment lawyer said the scale of the surveillance shows that privacy laws have failed to keep up with new technologies. Minnesota Reformer

PEGASUS MAKER NSO COULD ACCESS POLAND'S SPY DATA, PROSECUTORS SAY



IMAGE SOURCE: TV WORLD

Polish prosecutors have found that the CBA, the anti-corruption bureau that ran Pegasus, lacked passwords for some administrator accounts, and that parts of the system stayed under NSO Group's control. The server module that infects mobile devices was under the manufacturer's exclusive control, and updates and support came through a remote connection. Data also passed through servers around the world, on a network managed by NSO beyond the CBA's reach, which gave NSO technical access to material from operational surveillance. Experts could not determine whether NSO actually obtained data from specific operations. Prime Minister Donald Tusk called the case "a crime against the state" and said it was "beyond any doubt" that NSO cooperated with Israeli intelligence. Poland bought Pegasus in 2017 under the Law and Justice (PiS) government, and it was used against hundreds of targets, including political opponents. PiS says the spyware was necessary to fight crime and was court-authorized, and former CBA chief Ernest Bejda denies that Israeli authorities obtained Polish data. NSO has said its government customers operate Pegasus and control their own surveillance, and it has not publicly responded to the latest findings. TV World.

WATCHING THE WATCHDOGS: SPYWARE ON JOURNALISTS TESTS EUROPE'S NEW MEDIA FREEDOM LAW



IMAGE SOURCE: RCMFE

A new study published in Frontiers in Communication examines the use of military-grade spyware (Pegasus, Predator and Graphite) against journalists in Greece, Italy and Spain, and asks whether national laws meet Article 4 of the European Media Freedom Act (EMFA) and rule of law principles. The authors argue that state surveillance erodes the conditions for independent journalism and public debate by creating pervasive chilling effects. In Greece, after the 2022 Predatorgate scandal, Law 5002/2022 still lacks specific journalist protections, and a February 2026 conviction of Intellexa executives was the first judicial accountability, though state responsibility remains unclear. Italy, rated high risk, has no explicit ban on surveilling journalists. Its 2025 Graphite case exposed surveillance of Fanpage journalists, protections exclude non-professional "pubblicisti," and preventive wiretap authorisation bypasses the independent judicial review the EMFA requires. Spain, also high risk, saw five journalists targeted in the 2022 Pegasus/CatalanGate scandal, and critics warn that its July 2025 draft laws, with broad exceptions and heavy sanctions, could weaken safeguards. Across the three countries, roughly 79% of documented spyware cases involve unknown perpetrators, and implementation of Article 4, which requires prior judicial authorisation and transparency, has slipped past its August 2025 deadline, with market-related provisions getting priority over fundamental rights protections. The authors conclude that Article 4 is important progress but only as effective as national implementation, which needs transparency obligations and independent judicial oversight. Resource Centre on media freedom in Europe

SPYWARE AND SERBIA'S ELECTION: DIGITAL SURVEILLANCE ALLEGATIONS AMID POLITICAL OPPOSITION



IMAGE SOURCE: THE RECORD

A report by The Record, published on 26 October 2026, examines allegations of digital repression in Serbia following reports that spyware was used to target opposition figures, student protesters, journalists and prosecutors amid growing political tensions. Research by Citizen Lab, the SHARE Foundation and Amnesty International identified at least 15 people targeted with commercial spyware in Serbia during 2026, including University of Belgrade Rector Vladan Đokić, whose phone was confirmed to have been infected with Pegasus, and prosecutor Rade Bajić, who received an Apple spyware threat notification. The report also highlights the alleged use of Cellebrite surveillance technology by Serbian authorities to extract data from critics' devices during interrogations and arrests, despite the company announcing in February 2025 that it had cut ties with the Serbian government. These developments have intensified concerns about the use of surveillance technology against political opponents and civil society during an election period marked by student-led anti-corruption protests. The report underscores the implications of digital surveillance for privacy, political participation and democratic accountability, although allegations of state involvement in particular spyware attacks remain contested. The Record

LATIN AMERICA'S DIGITAL SURVEILLANCE BOOM KNOWS NO IDEOLOGY

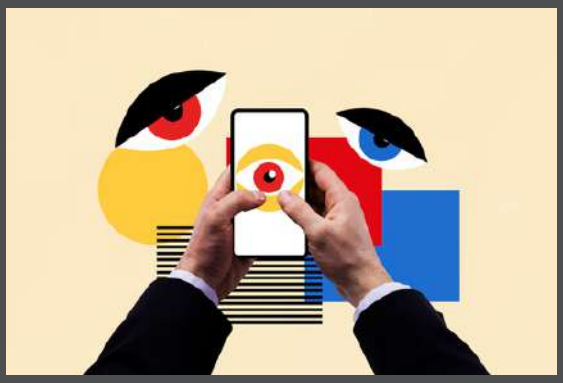


IMAGE SOURCE: EL PAIS

A report from the nonprofit Derechos Digitales, In the Crosshairs 2, documents more than 100 digital-rights violations across Latin America between June 2024 and May 2025, from Venezuela's blocking of Signal, X, TikTok, Telegram, YouTube and VPN services to a Paraguayan electoral-authority leak that exposed the data of nearly seven million people and the sale of more than 665,000 Argentine medical records. The group's analyst, Ximena Cuzcano, tells El País that these practices differ little between authoritarian and more democratic regimes: spyware is used on activists and journalists in Venezuela, while in Argentina cyberpatrolling lets authorities monitor people without oversight. Governments are also writing surveillance into law. Ecuador's 2025 Organic Intelligence Law, she says, authorized surveillance and detention without necessarily requiring a court order, and Argentina's Resolution 428/2024 and Decree 383/2025 allow systematic monitoring of open sources, with the Federal Police able to act without judicial authorization on public information. El Salvador's Cybersecurity Law could facilitate the removal of online content, and Cuba's Social Communication Law tightens state control over information. The region's reliance on imported technology, such as Israeli spyware, deepens its dependence on the countries that produce it, and the tools are often legalized after the fact. Not every threat is intentional: leaks have hit 12 countries, mostly through databases left open without authentication or misused legitimate access, with the data sold cheaply on the dark web or Telegram. One Ecuadorian case saw the emergency health service's data reach funeral companies, who could contact relatives of critically ill patients before a death had occurred. AI is also reshaping election disinformation, with at least five cases in Brazil of sexually explicit deepfakes targeting female candidates, while a Bolivian helpline logged 377 cases of technology-facilitated gender-based violence. El Pais

PEGASUS SPYWARE TARGETS SERBIAN UNIVERSITY RECTOR AND PROSECUTOR AMID POLITICAL TENSIONS



IMAGE SOURCE: EUROPEAN INTEREST

A report published by European Interest on 23 October 2026 highlights the targeting of prominent Serbian figures with Pegasus spyware, raising concerns about digital surveillance and institutional independence. Research by the University of Toronto's Citizen Lab, in collaboration with Serbia's SHARE Foundation, confirmed with high confidence that the phone of Vladan Đokić, Rector of the University of Belgrade and a supporter of student-led anti-government protests, was infected with Pegasus in 2026 through a zero-click attack that required no action from the user. Meanwhile, Rade Bajić, an associate at Serbia's Public Prosecutor's Office for Organised Crime who worked on a corruption investigation involving public officials, received an Apple notification indicating that he had been targeted by mercenary spyware. These cases follow reports that at least 14 other Serbian students, activists and opposition figures were targeted by advanced spyware in early 2026. The revelations have intensified concerns about the potential use of surveillance technology against government critics, particularly amid anti-corruption protests and parliamentary elections, and underscore the need for independent investigations, accountability and stronger protections for digital rights and democratic institutions. European Interest

BEYOND SPYWARE: HOW GOVERNMENTS CAN INTERCEPT MOBILE COMMUNICATIONS WITHOUT TOUCHING YOUR PHONE



IMAGE SOURCE: SILENTEL

An article by Silentel, published on 16 October 2026, warns that governments and other actors can exploit commercially available surveillance technologies to intercept communications, track locations and monitor officials, diplomats, journalists and political figures. Drawing on documented cases involving Pegasus spyware and attacks on mobile network signalling systems such as SS7 and Diameter, the article explains that surveillance can occur at the network level without compromising a person's device. It also highlights the limitations of end-to-end encryption, which protects message content but does not necessarily conceal metadata, prevent device compromise or secure the underlying communications infrastructure. The article argues that governments must move beyond conventional app-based security policies towards sovereign communications infrastructure that they own and control, supported by independent security assessments and safeguards against compromised devices. Ultimately, it raises concerns about the vulnerability of sensitive government communications to commercial surveillance and foreign interference, emphasising the need for stronger technical protections and greater control over the systems through which official communications are transmitted. Silentel

SPYWARE WARNING FOR SERBIAN PROSECUTOR INVESTIGATING TRUMP-LINKED $500 MILLION TOWER PROJECT



IMAGE SOURCE: INKL

A report by International Business Times UK, republished by INKL, examines how Serbian prosecutor Rade Bajić received an Apple threat notification in August 2026 warning that his iPhone had likely been targeted by mercenary spyware. Bajić was involved in investigating alleged corruption surrounding a proposed $500 million redevelopment of Belgrade's former General Staff military complex, a project associated with Jared Kushner's investment firm. The investigation concerned allegations that officials had improperly removed the site's protected status to facilitate the development, which was subsequently abandoned following the controversy and criminal proceedings. Researchers at the University of Toronto's Citizen Lab, working with Serbia's SHARE Foundation, identified the notification as a high-confidence indicator of suspected spyware targeting, potentially involving Pegasus, developed by Israel's NSO Group. However, forensic investigations remain ongoing, and researchers have not confirmed that Bajić's device was successfully infected or identified who was responsible. The case adds to broader concerns about the targeting of Serbian activists, academics and opposition figures with surveillance technology, highlighting the risks spyware poses to prosecutorial independence, confidential investigations and accountability for alleged official corruption. Inkl

STARLINK UNDER SURVEILLANCE: RESEARCHERS UNCOVER POSSIBLE GLOBAL TRACKING OPERATION



IMAGE SOURCE: GIZMODO

A report by Gizmodo, published on 27 October 2026, examines findings suggesting that Israeli advertising technology company Discover-Tech may have been involved in a large-scale effort to track users of SpaceX's Starlink satellite internet service. Researchers at TrendAI found that an advertising entity, identified by the codename SHADOW-EARTH-79 and subsequently linked to Discover-Tech by Reuters, was the leading bidder for Starlink-related advertising impressions in 105 countries, with particularly high activity in countries where the service is restricted or banned. The findings raise concerns that real-time advertising auctions, which can expose device and location-related data to bidders, may be exploited to identify and monitor users, including those accessing satellite internet in politically sensitive or conflict-affected environments. The company had previously been linked by Citizen Lab to advertising campaigns that delivered Candiru spyware without requiring users to click on anything. Although researchers have not publicly confirmed that Starlink devices were infected with spyware, the unusual advertising patterns suggest a possible surveillance operation. Following the investigations, Google and other companies removed Discover-Tech from their advertising platforms. The case highlights how commercial advertising infrastructure can potentially be repurposed for surveillance, raising urgent questions about digital privacy, corporate accountability and the protection of people who rely on alternative internet services. Gizmodo

INTELLIGENCE AGENCIES

SMILE, YOU'RE ON WASTE CAMERA: LAGOS TURNS SURVEILLANCE ON ILLEGAL DUMPERS



IMAGE SOURCE: NHM

The Lagos Waste Management Authority (LAWMA) plans to install surveillance cameras at strategic locations across the state to curb illegal dumping, strengthen environmental enforcement and improve sanitation. It will also partner with the Lagos State Command Centre to monitor environmental violations within the centre's coverage area, with the aim of better identifying offenders and discouraging indiscriminate disposal. LAWMA's Managing Director, Dr Muyiwa Gbadegesin, announced the plans on Lagos Talks 91.3 FM, saying that more collection infrastructure alone won't solve the sanitation problem without a change in public behaviour and consistent enforcement. Alongside the cameras, he said 150 new waste trucks had arrived, and a house-to-house intervention is clearing accumulated refuse after underperforming Private Sector Participation operators were disengaged. LAWMA is also pursuing waste-to-energy initiatives, including a proposed biogas plant, as well as Transfer Loading Stations and Material Recovery Facilities. The announcement follows September enforcement in which LAWMA sealed businesses along Ago Palace Way and arrested 11 people for unauthorised dumping on Lagos Island. The outlet notes that the cameras' impact will depend on where they are installed, how consistently violations are monitored and whether identified offenders face action, and that enforcement must be matched by reliable waste services. NHM

THE GLOBAL BAZAAR OF DIGITAL CONTROL: HOW AUTHORITARIAN STATES TRADE THE TOOLS OF SURVEILLANCE



IMAGE SOURCE: GLOBAL VOICES

In a Global Voices piece, Daria Dergacheva argues that digital authoritarianism spreads through the international exchange of technologies, standards and practices, as cameras with facial recognition, biometric databases, digital IDs, social media monitoring and deep packet inspection merge into a single infrastructure of control. She opens with Russian cases in which people, including a 15-year-old who wrote "Navalny" on a bus stop and a pensioner who wrote "No to War" on buildings, were identified from surveillance footage and punished. China, she writes, has overtaken Russia as a supplier of smart-city surveillance systems to the Global South, exporting infrastructure through its Digital Silk Road, and open-sourcing its state-regulated language models. Russia, meanwhile, remains dependent on China for hardware, with up to 80% of its cameras in 2024 made in China and sold under Russian brands. The piece traces the trade across regions: Article 19 found Iran's internet control relies heavily on Chinese technology, while Le Monde and Forbidden Stories showed that Iran acquired Russia's FindFace through intermediaries, with the software resold to entities including the IRGC. It also points to Chinese smart-city projects across Western Asia, Africa and Central Asia, Venezuela's dealings with China's Dahua and Belarus's sanctioned Synesis, and Russia-North Korea cooperation on testing AI in military operations. The author says the main danger of AI in authoritarian regimes is the ability to suppress protest before it materializes, and she notes that even democracies use such tools. Her proposed remedy is to make Western technologies open source and shift digital strategies toward including the majority world as real participants in AI governance, not just sources of energy and water for data centers. Global Voices

SPIES ON WHEELS? BIPARTISAN BILL AIMS TO BOOT CHINESE TECH OUT OF AMERICAN CARS



IMAGE SOURCE: JUST THE NEWS

Evidence that Chinese-made baby monitors and components in British military drones can be turned into spy devices has pushed Congress toward a rare bipartisan push to protect Americans' cars. Republicans and Democrats in both chambers are backing the Connected Vehicle Security Act, which would ban Chinese-made cars, along with electronic components and software from foreign adversaries, from vehicles sold in the US. The bill's stated aim is to prohibit the importation, manufacture and sale of connected vehicles and related software and hardware tied to foreign adversaries. Its restrictions would reach everything from GPS systems to entertainment devices. The House bill is co-sponsored by Rep. Warren Davidson, R-Ohio, with a Senate companion from Sen. Bernie Moreno, R-Ohio, and support from liberal senators like Elissa Slotkin and from the United Auto Workers union. Davidson argues that the data a car generates belongs to its driver, and that at the very least China shouldn't be able to collect it. The American Enterprise Institute warns that automakers in the connected vehicle industry could gain streams of behavioral, geographic and infrastructure data. The Wall Street Journal reported that Britain's Ministry of Defense found a component in its military drones secretly sending data back to China, and Missouri's attorney general has sued baby monitor maker Lorex over alleged undisclosed ties to the Chinese Communist Party and military, which Lorex disputes. Former Homeland Security Secretary Chad Wolf calls embedding data-gathering technology in products a core part of Beijing's espionage playbook. Just the News

40,000 CAMERAS LOCKED DOWN: UKRAINE'S WAR ON RUSSIA'S EYES IN THE STREETS



IMAGE SOURCE: HROMADSKE

Since Russia's full-scale invasion in 2022, Ukraine's Security Service (SBU) has identified and secured, redirected or blocked roughly 40,000 surveillance cameras, fearing they could be exploited for military intelligence, according to The Wall Street Journal. The SBU says Russian operatives could use them to pick out military targets and judge the results of strikes, though the figure does not mean all 40,000 cameras were confirmed hacked. In one 2024 case, Russian hackers took control of cameras in Kyiv residential buildings, including one an apartment association had installed to watch its neighborhood, with the aim of locating targets for missile attacks on the capital. The tactic cuts both ways. The international hacking group Team OneFist pulled footage from a camera in occupied Sevastopol, which helped identify Russian military aircraft and a previously unknown air base. That information reached Ukrainian forces, who struck the facility, damaging aircraft and air defense systems. The group also watched cameras around the Kerch Bridge and spotted security measures installed beneath it to detect attacks from the water. The threat reaches beyond Ukraine: Dutch intelligence warned in July that Russian hackers had targeted cameras across Europe to track military shipments tied to Ukraine, and CloudSEK researchers found an unsecured server holding hundreds of webcam images of Ukrainian defense, government, energy and communications sites. Hromadske

ERO ONE: INSIDE ICE'S $100 MILLION PLAN TO PUT 142 INTELLIGENCE ANALYSTS IN CITIES ACROSS AMERICA



IMAGE SOURCE: TRUTHOUT

ICE is reportedly fast-tracking ERO ONE, short for Enforcement and Removal Operations Overwatch and National Security Enforcement, a program meant to expand its domestic surveillance in dozens of US cities, with details posted to a federal contracting site in September and first reported by The American Prospect. Around $100 million is expected to come from the Department of Homeland Security to contract 142 intelligence agents, placed in at least two dozen cities, who would coordinate with nearby ICE offices and a central hub in Washington, D.C. The published plan doesn't say what the agents will do in the field, but they would analyze classified and unclassified information to produce "network, link, and relationship" analyses, a kind of research that examines a person's household, extended family, friends and even acquaintances. The document bars ERO ONE agents from arrest, detention, search, seizure, interrogation and other law enforcement authorities, though Truthout argues that ICE's record of overreach makes it plausible those limits could be ignored. The program builds on ICE's existing tools, which include facial recognition, mobile phone location data software, AI technologies and "zero-click" technology that can access encrypted data on a phone without the user clicking a link. Jay Stanley of the ACLU told The American Prospect that the plan looks dangerously like the construction of an internal spying agency, and critics warn it could mark a new domestic surveillance paradigm that reaches beyond immigrants. Truthout

LOOKING THE OTHER WAY: RIGHTS GROUPS SAY THE EU'S SURVEILLANCE EXPORT RULES STILL LEAK



IMAGE SOURCE: JURIST

Human Rights Watch's 54-page report "Looking the Other Way" assesses how the EU's 2021 Dual-Use Regulation is working in practice, concluding that member states host many companies producing dangerous surveillance technology and that exports need robust controls. The group filed freedom-of-information requests in all 27 member states and received data from nearly half of them, and found clear evidence of states licensing exports of surveillance technology to authorities in countries with well-documented histories of using such tools to violate rights. The EU regulates the most intrusive types of surveillance technology, but licensing decisions are made by national authorities, and the Commission's reports lack the detail needed to judge whether the regulation is having its intended effect. HRW urges the EU to tighten the controls by requiring states to do greater human rights due diligence, blocking risky exports and enforcing the transparency and reporting requirements so they provide meaningful oversight, with new guidelines that also require exporting companies to carry out meaningful due diligence on whether their products could contribute to rights problems. Jurist

FROM SPYWARE TO SOVEREIGN AI: FORMER PEGASUS CHIEF URGES GOVERNMENTS TO TAKE CONTROL OF NATIONAL SECURITY TECHNOLOGY



IMAGE SOURCE: TECH RADER

A report by TechRadar Pro, published on 27 October 2026, examines how Shalev Hulio, former CEO and co-founder of NSO Group, the Israeli company behind Pegasus spyware, is urging governments to develop and host their own artificial intelligence (AI) models rather than rely on US technology providers for sensitive national-security operations. Hulio argues that dependence on external AI companies creates strategic vulnerabilities, including the risk of losing access to essential systems if providers withdraw services or restrict access. Through his new venture, Dream, co-founded with former Austrian Chancellor Sebastian Kurz, he is promoting sovereign AI infrastructure, customised government models and AI-powered cyber-defence tools designed to operate on domestic systems and protect sensitive data. The company also develops technologies to identify software vulnerabilities and defend against increasingly sophisticated cyberattacks. However, Hulio's advocacy raises questions about the relationship between national security, technological independence and accountability, given his association with NSO Group and the international controversy surrounding Pegasus spyware and its reported use against journalists, politicians and civil society actors. The article highlights the growing geopolitical importance of AI sovereignty and the need to balance cybersecurity and state control with transparency, independent oversight and human rights protections. Tech rader

HAVE YOUR SAY!
LETTER TO THE EDITOR



Dear Readers:

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

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

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

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

Warm regards
The Intelwatch Team

INTEL WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

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



FIND US ON SOCIAL MEDIA

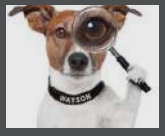
@IntewatchNews

@IntewatchNpc

Intewatch website

@IntewatchNpc

@IntewatchNpc



HAVE ANY QUESTIONS?

Email: info@intelwatch.org.za

The Reynolds Foundation Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!