Issue #12

INTEL WATCH

May 2026

Watching the watchers. Guarding the guardians.

THE WATCHER

Monthly

DEFENDING HUMAN RIGHTS, PROTECTING CIVIC SPACE

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

SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

INTEL WATCH

Watching the watchers. Guarding the guardians.

THIS MONTH UNDER THE MICROSCOPE

WELCOME TO ISSUE #12 OF THE WATCHER

This May 2026 edition arrives at a moment when the intersection of technology, security, and human rights has never felt more consequential.

This month, South Africa commands centre stage: from a devastating R2 billion cyber fraud uncovered within the City of Ekurhuleni, to Nigerian hacktivist groups targeting government systems amid rising xenophobic tensions, to the embarrassing withdrawal of the country's draft AI policy after fabricated citations - likely AI-generated - were discovered within its pages. Closer to home, Pick n Pay has confirmed a customer data breach, while new research crowns South Africa as the world's leading nation for cybercrime exposure.

Beyond our shores, the global surveillance landscape grows ever more complex and concerning - Chinese authorities are deploying AI-powered smart glasses and building detailed digital profiles of foreign nationals, European firms continue to export spyware to governments with troubling human rights records, and African governments are quietly investing in foreign surveillance infrastructure with minimal public oversight.

In our Repression Monitor, we examine how artificial intelligence is increasingly being weaponised as a tool of political control across the continent, and internationally, landmark legal battles over Pegasus spyware are reshaping the future of digital privacy.

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

INTEL WATCH

Watching the watchers. Guarding the guardians.

SURVEILLANCE UPDATES

NIGERIAN HACKTIVISTS TARGET SA GOVERNMENT ENTITIES IN CYBERCRIME WAVE IN RESPONSE TO XENOPHOBIA

IMAGE SOURCE: DAILY MAVERCIK

The article reports that several South African government entities were targeted in a wave of cyberattacks carried out by Nigerian hacktivist groups claiming to act in response to rising xenophobic tensions in the country. According to the report, the attacks involved website disruptions and digital interference aimed at drawing attention to anti-foreigner violence and political tensions in South Africa. Cybersecurity experts warned that politically motivated cyberattacks are becoming more common globally, with hacktivist groups increasingly using digital platforms to make political statements or retaliate against governments. The article also highlights concerns about the vulnerability of South African public-sector systems, noting that many institutions may lack the resilience needed to defend against coordinated cyber campaigns during periods of social unrest - (18 May 2026). Daily Maverick

EKURHULENI CYBERATTACK LINKED TO ALLEGED R2BN THEFT

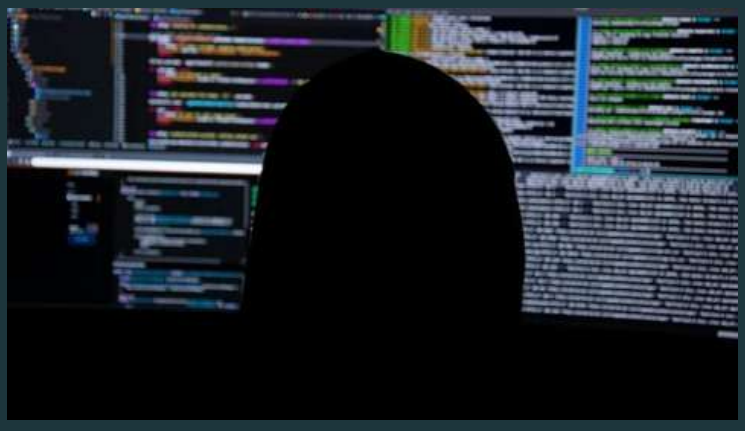

IMAGE SOURCE: CAPE TOWN ETC

The article reports that investigators uncovered a massive cybercrime and fraud scheme inside the City of Ekurhuleni - in the East Rand of Gauteng province - where hackers and alleged insiders manipulated the municipality's IT and billing systems in a scam linked to losses of nearly R2 billion. According to forensic findings, attackers exploited weak cybersecurity controls, unsecured Wi-Fi networks, shared administrator accounts, and spyware to gain access to systems, alter debt records, and redirect municipal funds into fraudulent accounts. Reports suggest the scheme operated for years before detection and may have involved collusion between cybercriminals, municipal officials, and external parties. The scandal has sparked outrage because the stolen money was meant for public services while residents continue facing infrastructure and service delivery problems. It has also intensified calls for deeper investigations, stronger municipal cybersecurity, and accountability from officials responsible for safeguarding public systems - (17 May 2026). Cape Town etc

INTEL WATCH

Watching the watchers. Guarding the guardians.

THE INVISIBLE CYBER TAX: HOW HACKERS ARE QUIETLY RAISING YOUR GROCERY BILL

IMAGE SOURCE: IOL

The article explains that South African households are facing a "hidden surcharge" on grocery bills caused by rising costs linked to cybercrime and cyber disruptions across supply chains. It argues that when retailers, logistics companies, and suppliers are hit by cyberattacks, the resulting downtime, recovery costs, higher cybersecurity spending, and increased insurance premiums are often passed on to consumers in the form of higher prices. Even though shoppers don't see a direct "cyber fee" on receipts, these costs are embedded in the price of everyday goods as businesses try to recover losses and maintain operations. Experts warn that as cyberattacks become more frequent and expensive, they are quietly contributing to inflation and putting additional pressure on already strained household budgets in South Africa - (15 May 2026). IOL

WHATSAPP OVERTAKES EMAIL IN SOUTH AFRICAN WORK COMMUNICATIONS, RAISING CYBERSECURITY CONCERNS

IMAGE SOURCE: IOL

The article reports that WhatsApp has now overtaken email as the most widely used work communication tool in South Africa, with 89% of employees using the messaging platform for professional communication compared to 88% using email. Cybersecurity experts warn that while WhatsApp is popular because it is fast, familiar, and convenient for remote and hybrid work, it was not designed for enterprise use and lacks critical business-level security controls, audit trails, and compliance features. This creates growing risks such as data leaks, phishing attacks, impersonation scams, and the uncontrolled sharing of sensitive business information, prompting experts to urge organisations to implement clearer communication policies and adopt more secure enterprise platforms - (24 April 2026). IoL

INTEL WATCH

Watching the watchers. Guarding the guardians.

WHY SOUTH AFRICA LEADS THE WORLD IN CYBERCRIME EXPOSURE

IMAGE SOURCE: THE CITIZEN

The article explains that South Africa has recorded the highest cyberattack rate in the world, with new research showing that many organisations still lack proper control over user identities and access management. According to the report, 36% of South African organisations experienced cyberattacks, while nearly 80% admitted they cannot fully track who has access to their systems and sensitive data. Experts warn that this "identity visibility gap" leaves businesses vulnerable to phishing, password theft, and insider threats, especially as cloud services, AI systems, and third-party integrations rapidly expand. The article also highlights that many organisations still lack Zero Trust security strategies and that smaller businesses are particularly exposed due to limited cybersecurity resources. Despite increasing investment in cybersecurity, researchers argue that without stronger identity governance and access controls, South African companies remain at high risk of data breaches, financial losses, and POPIA compliance failures - (11 May 2026). The Citizen

HACKER GROUP TARGETED COMPANIES IN SOUTH AFRICA USING FAKE SARS NOTIFICATIONS

IMAGE SOURCE: MY BROADBAND

A hacker group known as SilverFox targeted companies in South Africa using a phishing campaign that impersonated the South African Revenue Service (SARS), sending fake tax audit notifications and court summons emails designed to trick employees into downloading malicious files. Once opened, the attachments installed malware that could give attackers remote control over infected systems, steal data, and disable security tools. The campaign, which also hit organisations in other countries, involved over 1,600 malicious emails and used increasingly sophisticated social engineering techniques to appear legitimate and urgent, exploiting trust in tax authorities to breach systems across sectors like industry, consulting, transport, and trade. Security researchers noted that the group had evolved into a more advanced threat actor using multi-stage malware delivery and stealth tactics to avoid detection - (10 May 2026). My Broadband

INTEL WATCH

Watching the watchers. Guarding the guardians.

MZANSI'S DRAFT AI POLICY IS BEING REWORKED. WHERE DOES THAT LEAVE US IN THE MEANTIME?

IMAGE SOURCE: EXPLAIN

South Africa's draft National AI Policy was withdrawn - and two officials suspended - after being found to contain fake or unverified academic citations, likely generated with AI, raising concerns about oversight in policy drafting. While the policy was intended to position South Africa as a leader in AI governance and included proposals for new institutions, ethical safeguards, and innovation incentives, it was pulled back shortly after publication for public comment when credibility issues emerged. In the meantime, the article argues that AI is still rapidly advancing without formal guardrails, leaving a gap between fast-moving technology and delayed regulation. It stresses that this incident highlights the urgent need for stronger human oversight, credible policy development processes, and clear regulatory frameworks to ensure AI is deployed responsibly and transparently in South Africa. - (30 April 2026). Explain

NEW DEADLINE FOR AI POLICY SET FOR 27 JANUARY 2027

IMAGE SOURCE: MY BROADBAND

South Africa's Department of Communications and Digital Technologies has announced that a revised version of the country's national AI policy will only be published for public comment in January 2027 after the original draft was withdrawn for containing fictitious, likely AI-generated references. Communications Minister Solly Malatsi told Parliament that the department only became aware of the fabricated citations after a media exposé, leading to an internal investigation and the suspension of two officials accused of irresponsibly using generative AI. A new independent panel of AI, legal, cybersecurity, and governance experts — chaired by leading AI researcher Benjamin Rosman — will now review and rewrite the policy, replace fake sources with verified references, and advise government before the revised document goes to Cabinet in late 2026 - (26 May 2026). My Broadband

PICK N PAY CONFIRMS DATA BREACH AFFECTING DELIVERY SERVICE USERS

IMAGE SOURCE: IOL

South African retailer Pick n Pay has confirmed a data breach affecting users of its former on-demand delivery platform, previously known as Bottles and later Pick n Pay asap!, after a dataset dating back to 2022 was discovered online. According to the company, exposed information may include customers' names, contact details, home addresses, and limited banking information, although full card numbers and CVV codes were reportedly not stored and therefore could not be used directly for fraudulent purchases. Pick n Pay said it is working with an independent cybersecurity firm to investigate the breach, strengthen how historical customer data is managed, and support affected users, while also advising customers to change passwords and remain alert to phishing attempts or suspicious communications using leaked personal details. The incident adds to growing concern in South Africa over data protection, cybercrime, and corporate accountability following a series of major breaches affecting both businesses and public institutions - (28 May 2026). IOL

AFRICA'S AI AMBITIONS STILL RUN ON AMERICAN TECH

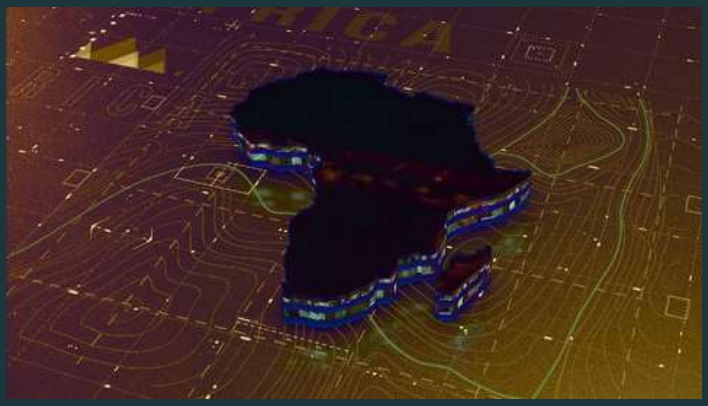

IMAGE SOURCE: IAFRICA

The article reports that Africa's four leading tech economies — South Africa, Nigeria, Kenya, and Egypt — have acknowledged in their national AI strategies that they remain heavily dependent on major U.S. technology firms like Google, Microsoft, NVIDIA, and Meta for AI infrastructure, funding, and expertise. Governments across the continent are increasingly concerned that this reliance threatens digital sovereignty, data control, and long-term economic independence, leading to calls for stronger local infrastructure, African-owned datasets, regional cooperation, and stricter governance over foreign AI providers. However, Africa still holds less than 1% of global data centre capacity, forcing many countries to rely on overseas cloud services and foreign-managed systems even as new initiatives — including the African Union's Continental AI Strategy, the Africa AI Council, and a proposed $60 billion AI fund — attempt to build a more self-sufficient continental AI ecosystem - (28 May 2026). iAfrica

ARCTIC WOLF TAKES AIM AT SOUTH AFRICA'S SECURITY BLIND SPOTS

IMAGE SOURCE: TECH CENTRAL

Cybersecurity company Arctic Wolf says many South African organisations lack a clear, up-to-date understanding of their own IT environments, creating dangerous "blind spots" that cybercriminals can exploit. The company has launched a new Asset Surface Management (ASM) capability designed to give businesses a continuously updated view of all devices, servers, cloud systems, and unmanaged assets across their networks. Arctic Wolf argues that many local companies still rely on outdated spreadsheets and manual tracking systems that cannot keep pace with modern hybrid IT environments, especially amid growing ransomware and credential-based attacks. The platform is aimed at helping overstretched security teams quickly identify unknown or unprotected assets, improve compliance, and strengthen overall cyber resilience without requiring complex deployments or large internal security teams - (29 May 2026). Tech Central

AI IN THE COURTROOM? JOHANNESBURG RULING SPARKS CONCERNS OVER "HALLUCINATED" JUDGMENTS

IMAGE SOURCE: NEWS 24

A Johannesburg High Court case has raised alarm after allegations that an acting judge may have relied on artificial intelligence to help draft a ruling that contained questionable and possibly fabricated legal citations. Lawyers in the case argue that several references in the judgment could not be verified, including one apparently linking to a non-existent or misattributed case involving Volkswagen, suggesting possible AI "hallucinations" in the legal reasoning. The matter has sparked broader concern about the use of generative AI in the justice system, with critics warning that unverified AI-generated content could undermine trust in court decisions, while supporters say the incident highlights the urgent need for clear rules and verification systems when courts or legal professionals use AI tools - (17 May 2026). News24

INTEL WATCH

Watching the watchers. Guarding the guardians.

SOUTH AFRICA TO INTENSIFY INTELLIGENCE REFORMS AS CYBER AND HYBRID THREATS ESCALATE

REPUBLIC OF SOUTH AFRICA

In her 2026/27 State Security Agency (SSA) Budget Vote speech, Minister in the Presidency Khumbudzo Ntshavheni outlined a major push to modernise South Africa's intelligence and security capabilities in response to growing cyber threats, organised crime, and geopolitical instability. She stressed that intelligence institutions must become more agile, data-driven, and technologically capable, with a stronger focus on anticipating and disrupting threats rather than reacting to them.

The minister highlighted ongoing reforms including the restructuring of intelligence services under the forthcoming General Intelligence Laws Amendment Act (GILAA), the establishment of a National Centre for Intelligence Coordination, and the development of new shared services to improve efficiency across intelligence bodies. A key priority is strengthening cyber resilience through a revised National Cybersecurity Strategy, alongside expanded use of AI, data science, geospatial intelligence, and advanced digital systems within the State Security Agency.

Ntshavheni also linked domestic security challenges to broader global instability, warning that organised crime networks, terrorism financing, and cyberattacks are increasingly transnational. She emphasised cooperation with regional and international partners, while positioning intelligence reform as central to protecting South Africa's sovereignty, democratic institutions, and economic stability - (22 May 2026) . SA Gov News

EY RETRACTS STUDY AFTER RESEARCHERS DISCOVER AI HALLUCINATIONS

IMAGE SOURCE: EY

The Financial Times article examines growing concern in the corporate world over the rise of artificial intelligence "hallucinations" being used in professional work, after EY reportedly had to withdraw a report that contained fabricated data, fake citations, and even a non-existent McKinsey reference. The incident highlights how generative AI tools, when used without proper verification, can produce convincing but false information that may still slip into consulting, research, and business decision-making. Critics argue this exposes a wider governance problem in how firms are adopting AI too quickly without robust quality controls, while companies like EY say they are strengthening oversight and responsible-use policies. The broader concern is that AI is increasingly being used not just to generate content, but also to validate and commercialise that same content, creating a feedback loop where errors can scale quickly if left unchecked - (15 May 2026). Ey

AI, GLOBAL UNCERTAINTY TO TOP TALKS AT SOUTHERN AFRICA'S LEADING CYBER SECURITY EVENT

IMAGE SOURCE: ENGINEERING NEWS

Southern Africa's leading cybersecurity event, the ITWeb Security Summit, will focus heavily on artificial intelligence and global uncertainty as key drivers reshaping the cyber threat landscape, with experts warning that AI is accelerating both the scale and sophistication of cyberattacks. The conference will bring together over 1,000 security professionals in Johannesburg under the theme "Redefining security in the face of AI-driven attacks, fragile supply chains and a global skills gap", highlighting risks such as AI-powered phishing, deepfakes, ransomware, and vulnerabilities in third-party software ecosystems. Speakers will also examine how geopolitical instability and regulatory uncertainty are complicating cybersecurity planning, while organisations struggle with skills shortages and rising attack complexity. The event aims to explore practical responses, including stronger cyber resilience strategies, improved threat intelligence sharing, and greater use of AI for defensive security purposes - (21 May 2026). Engineering News

GLOBAL SOUTH COUNTRIES PRESENT STRATEGIES FOR DEVELOPING NEW CYBERSECURITY ARCHITECTURE

IMAGE SOURCE: TV BRICS

Countries from the Global South, including Russia, Brazil, Thailand, Indonesia, Egypt, and Zimbabwe, have outlined plans for a more coordinated international cybersecurity architecture during a security forum held in Russia. Speakers emphasised that cyber threats are increasingly transnational and require stronger global cooperation, with the United Nations and BRICS highlighted as key platforms for developing shared rules and standards. Delegates called for legally binding international norms on information security, improved information-sharing systems for cyber incidents, and clearer regulation of emerging technologies such as artificial intelligence and post-quantum cryptography. The discussions also stressed capacity-building, sovereign equality in cyberspace governance, and the need to reduce technological inequality between countries while strengthening collective resilience against cybercrime and digital attacks - (27 May 2026). TV BRICS

INTEL WATCH

Watching the watchers. Guarding the guardians.

SAFARICOM PRIVACY RULING SIGNALS A TURNING POINT FOR KENYA'S DIGITAL RIGHTS

IMAGE SOURCE: HAPA KENYA

A landmark Kenyan court ruling ordering Safaricom to pay KSh 9.9 million to 11 subscribers over unlawful data exposure is being viewed as a major moment for digital privacy and corporate accountability in Kenya's fast-growing tech economy. The High Court found that sensitive customer information — including financial records, betting activity, device identifiers, and location data — had been improperly accessed and shared without consent, rejecting Safaricom's argument that the breach was solely the work of rogue employees. Legal analysts say the decision strengthens constitutional protections around privacy, consumer rights, and data governance, while increasing pressure on telecom firms, fintech platforms, and AI-driven services to improve transparency and oversight. The ruling also arrives amid broader public concern over surveillance, algorithmic decision-making, and data misuse in Kenya, where Safaricom's platforms play a central role in everyday financial life - (21 May 2026). Hapa Kenya

BANKS ON THE BRINK: UGANDA'S FINANCIAL SYSTEM BRACES FOR GLOBAL CYBER THREAT SURGE

IMAGE SOURCE: RED PEPPER

The article reports that Ugandan banks have been placed on high alert after a wave of global cyberattacks targeting financial systems and customer data raised concerns about local vulnerability. It explains that hackers are increasingly targeting banks through techniques such as phishing, system infiltration, and exploiting third-party service providers, putting sensitive customer information and transactions at risk. The report highlights that while Uganda's banking sector has strengthened digital services and cybersecurity measures, the rapid shift to online and mobile banking has expanded the attack surface, making institutions more exposed. It also notes that regulators and banks are urging stronger vigilance, investment in cybersecurity infrastructure, and better coordination to prevent breaches and protect customer trust as cyber threats continue to grow worldwide - (25 April 2026). Red Pepper

AFRICA'S DATA SOVEREIGNTY CHALLENGE: WHO REALLY CONTROLS THE CONTINENT'S DIGITAL FUTURE?

IMAGE SOURCE: CIRCLE ID

The article argues that Africa's growing digital economy has created a major data sovereignty challenge, as much of the continent's digital infrastructure—including cloud services, data storage, and online platforms—is controlled by foreign technology companies. This dependence means that sensitive African data is often stored outside the continent and governed by external laws, raising concerns about cybersecurity, economic control, privacy, and political independence. The piece explains that simply keeping data within national borders is not enough; true digital sovereignty also requires Africa to build its own technological capabilities, including local data centres, cybersecurity expertise, cloud infrastructure, and stronger regional cooperation. It highlights that without investment in local innovation and coordinated governance, Africa risks remaining dependent on foreign digital systems while losing economic value and strategic control over its digital future - (17 May 2026). Circle ID

CYBER THREAT OUTLOOK FOR AFRICA IN 2026 AND BEYOND

IMAGE SOURCE: EY

EY's "Africa's Cyber Risk Trends Boards Must Address in 2026" explains that cyber risk in Africa has moved firmly into a board-level business issue, not just an IT concern. It highlights that threats are becoming more complex due to AI-driven attacks, expanding digital ecosystems, and growing reliance on third-party and cloud providers, which increase exposure across organisations. The article outlines key trends such as the rising importance of operational resilience (protecting services from disruption rather than just data breaches), increasing regulatory pressure across different jurisdictions, and the need for stronger identity and access management as identity compromise becomes a primary attack method. It also stresses that boards must take greater responsibility for cyber oversight, ensuring investment in resilience, governance, and risk management keeps pace with rapidly evolving threats that can directly impact business continuity and trust - (6 May 2026). Ey

AS AFRICA RAPIDLY GOES DIGITAL, IT BECOMES A PRIME TARGET FOR HACKERS

IMAGE SOURCE: RFI

The article explains that as Africa rapidly expands its digital infrastructure—through mobile banking, online government services, and connected public systems—it is becoming an increasingly attractive target for cybercriminals. This growth is happening faster than many countries can build strong cybersecurity defences, leaving gaps that hackers exploit through ransomware, phishing, and data theft attacks against governments, businesses, and critical services. It highlights real incidents across the continent, such as breaches of public institutions and large-scale data leaks, to show how serious the threat has become. Experts quoted in the article warn that without stronger investment in cyber resilience, skills, and coordinated national and regional security strategies, Africa's digital progress could be undermined by rising cybercrime and instability - (15 May 2026). RFI

CANVAS BACK ONLINE AFTER CYBERATTACK DISRUPTS UNIVERSITIES WORLDWIDE

IMAGE SOURCE: SABC

The article reports that the Canvas online learning platform was restored after a major cyberattack disrupted universities and schools worldwide, affecting students during a critical academic period. The attack, linked to the hacker group ShinyHunters, temporarily blocked access to coursework, assignments, grades, and exams, forcing institutions to delay assessments and use alternative systems. Investigators said the breach may have exposed user information such as names, email addresses, student IDs, and private messages, although passwords and financial data were reportedly not compromised. The incident highlighted how heavily universities depend on centralised digital learning platforms and raised concerns about the cybersecurity readiness of the global education sector as cyberattacks on schools and academic institutions continue to increase - (8 May 2026). SABC

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTERPOL COORDINATES ARRESTS OVER 200 IN SWEEPING MIDDLE EAST AND AFRICA CYBERCRIME CRACKDOWN

IMAGE SOURCE: OCCRP

The article reports that Interpol has arrested more than 200 suspected cybercriminals across a coordinated crackdown spanning the Middle East and Africa, targeting a wide range of online fraud networks. The operation focused on disrupting criminal groups involved in activities such as phishing, business email compromise, ransomware, and online scams, which have caused significant financial losses to individuals, companies, and government institutions. Authorities also seized devices, dismantled scam infrastructure, and recovered funds linked to illicit transactions. Interpol described the operation as part of a broader effort to strengthen international cooperation against cybercrime, noting that these networks are increasingly transnational and adapt quickly by shifting operations across borders. The article highlights that while arrests are significant, cybercrime remains a persistent and evolving threat that requires continued cross-border enforcement and intelligence sharing - (18 May 2026). OCCRP

CRACKDOWN IN SOUTHEAST ASIA PUSHES SCAM NETWORKS TO SRI LANKA

IMAGE SOURCE: ENCA

The article reports that cybercrime networks displaced by crackdowns in Southeast Asia are increasingly shifting their operations to Sri Lanka, raising alarm among authorities that the island is becoming a new hub for online scam activity. According to officials, coordinated enforcement actions in countries like Cambodia and Myanmar have disrupted major scam compounds, but criminal groups are simply relocating rather than shutting down. Sri Lanka has seen a sharp rise in arrests of foreign nationals suspected of running or supporting online fraud schemes, with authorities linking the trend to its relatively open visa policies and strong internet infrastructure. The article warns that this “geographical migration” of scam networks highlights how difficult it is to dismantle transnational cybercrime operations, as they adapt quickly by moving across borders rather than being eliminated - (17 May 2026). eNCA

INTEL WATCH

Watching the watchers. Guarding the guardians.

INTERPOL COORDINATES ARRESTS OVER 200 IN SWEEPING MIDDLE EAST AND AFRICA CYBERCRIME CRACKDOWN

IMAGE SOURCE: MOONSTONE

The article argues that despite growing investment in cybersecurity tools, motor dealerships remain highly vulnerable because employees, weak processes, and poor data-handling practices are still the main entry points for cybercrime. Drawing on discussions from the 2026 F&I Virtual Summit, experts explained how dealerships are increasingly targeted through phishing, ransomware, fake officials, and data leaks involving sensitive customer information governed by South Africa's POPIA legislation. The article stresses that compliance and cybersecurity are no longer just technical or legal requirements but core business responsibilities tied to customer trust and operational resilience. Panellists highlighted the importance of staff training, role-based access control, proper consent records, third-party data-sharing agreements, breach-response plans, and governance from leadership level downward. Although AI-driven attacks and automated systems are creating new risks, the consensus was that dealerships first need to strengthen basic cybersecurity habits and reduce human mistakes, which are estimated to cause around 80% of breaches - (25 May 2026). Moonstone

CYBERSECURITY MUST BE BUILT INTO AFRICA'S DIGITAL TRANSFORMATION

IMAGE SOURCE: WE ARE TECH

The article argues that Africa's digital transformation must integrate cybersecurity from the start rather than treating it as an afterthought. In an interview with We Are Tech Africa, cybersecurity expert Babel Balsomi explains that many organizations in Côte d'Ivoire still rely on outdated systems, weak security practices, and low employee awareness, making them highly vulnerable to phishing, ransomware, business email compromise, and emerging AI-driven cyberattacks. While the government has strengthened national cybersecurity institutions, Balsomi says there remains a major gap between policy ambitions and operational reality, especially among SMEs and public institutions that lack proper backups, encryption, incident response plans, and staff training. He warns that AI adoption in sectors like healthcare, agriculture, and education could amplify risks if security is not built into systems "by design," stressing that Africa has a rare opportunity to avoid the mistakes made elsewhere by developing secure digital ecosystems from the beginning - (23 May 2026). We are Tech

INTEL WATCH

Watching the watchers. Guarding the guardians.

ANDROID'S NEW INTRUSION LOGGING TRACKS SPYWARE ACTIVITY ON YOUR PHONE

IMAGE SOURCE: TECHLICIOUS

Android 16 introduces a powerful new security feature called “Intrusion Logging,” designed to help detect sophisticated spyware attacks that often target journalists, activists, politicians, and other high-risk users. Developed by Google in partnership with Amnesty International and Reporters Without Borders, the feature securely records encrypted logs of suspicious activity — including app installations, network connections, USB access, and device unlocks — and stores them in the cloud for up to 12 months so attackers cannot easily erase evidence of a breach. Available through Android’s Advanced Protection Mode on supported devices like Google Pixels, the system is being described as a major breakthrough in mobile forensics because it allows users and security experts to investigate compromises after an attack occurs, rather than relying only on prevention - (26 May 2026). Techlicious

LA LIGA TO INTRODUCE AI FOR REFEREE EVALUATIONS FROM NEXT SEASON

IMAGE SOURCE: IDMAN & BIZ

La Liga president Javier Tebas has announced that artificial intelligence will be introduced from next season to help evaluate and select referees, marking one of the most significant technological shifts in European football officiating. The system will analyse match data across multiple criteria to assess referee performance more objectively, aiming to replace part of the current manual review process conducted by Spain’s refereeing committee. Tebas said AI could help make around 40% of decisions in the evaluation process more data-driven, while still leaving final judgments in human hands. The technology will also assist in assigning referees by generating shortlists of candidates for each match, as part of a broader push to improve consistency and transparency amid ongoing debates over VAR decisions and officiating standards in top-flight football - (22 May 2026). Idman & Biz

INTEL WATCH

Watching the watchers. Guarding the guardians.

REPRESSION MONITOR

AI AND THE NEW MACHINERY OF AFRICAN REPRESSION

IMAGE SOURCE: EURASIA REVIEW

The article argues that artificial intelligence is making authoritarian control cheaper, faster, and more effective across parts of Africa by strengthening existing systems of surveillance and political repression rather than creating entirely new dictatorships. The article describes how governments in countries such as Kenya, Uganda, Zimbabwe, and Nigeria are investing heavily in AI-powered surveillance tools — including facial recognition, biometric databases, smart-city CCTV systems, and social media monitoring — often supplied by foreign technology firms and justified as public-safety or modernization projects. Bencherif warns that weak courts, limited oversight, and politicised security forces allow these technologies to be used against activists, journalists, and protest movements, citing examples like Kenya's Gen Z protests and concerns over Chinese-backed surveillance infrastructure. While acknowledging AI's potential benefits in areas like healthcare and education, the piece argues that without strong democratic institutions, digital rights protections, and transparent regulation, AI risks becoming a tool for "political sorting" that discourages dissent before it can even organise itself - (23 May 2026). African Arguments

REVEALED: ISRAELI TECH EXPOSES USERS OF MUSK'S STARLINK SATELLITE-BASED INTERNET

IMAGE SOURCE: HAARETZ

The article reports that an investigation by Haaretz reveals how Israeli tech companies have developed tools capable of identifying and tracking users of Starlink satellite internet, including linking devices and online activity to real-world identities. These systems do not hack Starlink directly; instead, they use large-scale "data fusion" techniques, combining advertising identifiers, app data, and digital traces from smartphones and other connected devices to locate Starlink terminals and infer who is using them. The report warns that this capability represents a major shift in surveillance technology, making even satellite-based internet—often seen as more private or resilient—potentially traceable. It raises concerns about privacy, especially for journalists, activists, and people in conflict zones who rely on Starlink for secure communication, and highlights growing fears about how commercial data ecosystems can be repurposed for intelligence and surveillance purposes - (12 May 2026). Haaretz

INTEL WATCH

Watching the watchers. Guarding the guardians.

WHEN SAVING RHINOS MEANS WATCHING PEOPLE

IMAGE SOURCE: OXPECKERS

The article explains how conservation efforts in South Africa's protected wildlife areas are increasingly relying on high-tech surveillance systems—including drones, CCTV networks, automated number-plate recognition, and centralized data platforms—to prevent rhino poaching and other environmental crimes. While these tools are designed to improve security and protect endangered species, the investigation argues that they also create a form of "green panopticon," where both suspected criminals and ordinary visitors are continuously monitored through extensive data collection and tracking systems. It raises concerns about privacy, transparency, and accountability, noting that surveillance data is often shared across agencies with limited public oversight and that communities near conservation areas may be affected by misidentification or excessive monitoring. Overall, the article questions whether the increasing militarisation of conservation is justified by necessity or whether it risks normalising mass surveillance in the name of environmental protection (2026). Oxpeckers

THE WAR ON POACHING HAS GONE FULL TECH DYSTOPIA—AND IT MAY NOT BE WORKING

IMAGE SOURCE: GIZMODO

The article explains that wildlife conservation efforts aimed at stopping poaching have increasingly adopted high-tech surveillance and militarised tactics, including drones, AI monitoring systems, armed ranger units, and extensive tracking infrastructure, but these approaches are creating serious unintended consequences for local communities. While these tools can help detect and deter poaching, the report argues they are often used in ways that lead to harassment, intimidation, and even violence against people living near protected areas, turning conservation zones into heavily monitored spaces where communities feel criminalised and constantly watched. Critics say this "tech-driven" conservation model prioritises enforcement over addressing deeper causes of poaching such as poverty and land inequality, and may ultimately undermine trust between residents and authorities. The article concludes that despite the growing use of advanced technology, the strategy may not be effectively solving poaching and could be worsening social tensions and long-term conservation outcomes - (28 February 2026). Gizmodo

FROM SPY TECH TO ARMY IN THE PARKS: INSIDE UGANDA'S MILITARISED CONSERVATION STATE

IMAGE SOURCE: EURASIA REVIEW

The article explains how Uganda's wildlife conservation system has become increasingly militarised and surveillance-driven, using advanced technologies like drones, GPS tracking, AI platforms (such as EarthRanger), thermal cameras, and centralized data systems to monitor national parks and combat poaching. While these tools have improved enforcement and helped secure convictions in wildlife crime cases, they also blur the line between conservation and security operations because Uganda Wildlife Authority works closely with the military in joint patrols and intelligence sharing. The report highlights concerns that this "digital dragnet" can extend beyond targeting poachers to potentially monitoring ordinary local communities, raising fears about privacy violations, human rights abuses, and reduced trust between residents and conservation authorities. Critics argue that this heavy reliance on surveillance and armed enforcement risks turning protected areas into highly controlled security zones and may undermine long-term conservation goals by alienating communities who live near the parks and depend on them - (April 2026). InfoNile

EUROPE EXPORTED SPYWARE TO HUMAN RIGHTS ABUSERS, WATCHDOG SAYS

IMAGE SOURCE: THE JAPAN TIMES

The article reports that a major new Human Rights Watch investigation has found European companies are still exporting commercial spyware and surveillance tools to governments with known human rights abuses, despite EU rules introduced in 2021 meant to regulate these exports. The report argues that enforcement is weak, allowing spyware from EU member states to reach countries where it is used to monitor journalists, activists, and political opponents, undermining privacy and civil liberties. Human Rights Watch says the EU's "dual-use" export controls are inconsistent across member states and lack transparency, and it calls for stronger oversight, stricter due diligence, and more effective enforcement to prevent European technology from enabling repression abroad. - (12 May 2026) . The Japan Times

INTEL WATCH

Watching the watchers. Guarding the guardians.

SILENCED BY SPYWARE: THE HIDDEN COST OF BEING A TARGET

IMAGE SOURCE: KASHMIR TIMES

The article tells the story of a journalist who was targeted with Pegasus spyware, part of a wider global surveillance campaign against reporters, activists, and critics. After the attack was discovered, the journalist describes how it disrupted their personal and professional life—creating fear, mistrust, and isolation because they no longer knew who else might be monitoring their communications. The piece highlights how Pegasus infections are often silent and hard to detect, but can completely compromise a phone, exposing messages, contacts, and sensitive sources. It also places the incident in a broader context of increasing digital surveillance of journalists, especially in regions where press freedom is already under pressure, and shows how such attacks can lead to self-censorship and long-term psychological stress - (29 April 2026). Kashmir Times

EUROPEAN COUNTRIES ARE EXPORTING SURVEILLANCE TECH TO COUNTRIES WITH POOR HUMAN RIGHTS RECORDS, REPORT SAYS

IMAGE SOURCE: CAPTAIN COMPLIANCE

The article explains that EU member states and companies are continuing to export surveillance and spyware technologies to countries with serious human rights concerns, despite existing rules intended to regulate these sales. A Human Rights Watch investigation found that firms across several EU countries have supplied tools like intrusion software and communications interception systems to governments accused of using such technology to monitor journalists, activists, and political opponents. It argues that the EU's 2021 export control framework is inconsistently applied and lacks transparency and strong enforcement, allowing abusive regimes to access powerful surveillance tools. Human rights groups warn that this weak oversight means Europe is indirectly contributing to global repression and are calling for stricter, more unified export rules and better accountability mechanisms - (12 May 2026). The Record

JOURNALISTS WORLDWIDE CALL FOR STRONGER ACTION ON SPYWARE ABUSE

IMAGE SOURCE: IFJ NEWS

The article reports that the International Federation of Journalists (IFJ) and affiliated press freedom organisations are calling for stronger global action to stop spyware abuse targeting journalists. It highlights growing concern over the widespread use of commercial surveillance tools like Pegasus and similar spyware, which have been used to hack journalists' phones, monitor communications, and expose confidential sources, putting press freedom and personal safety at risk. The IFJ warns that such surveillance is increasingly being used by both state and non-state actors to intimidate or silence reporters, undermining democratic accountability and investigative journalism. The statement urges governments to introduce stricter regulation of the spyware industry, improve accountability for abuses, and ensure stronger protections for journalists worldwide, including better legal safeguards and enforcement mechanisms - (15 May 2026). IFJ News

CENTRAL ASIA: ESCALATING DIGITAL REPRESSION THREATENS CIVIC SPACE AND FREE EXPRESSION

IMAGE SOURCE: EURASIA REVIEW

The article explains that Central Asia is facing increasing digital repression, with governments using tools such as internet shutdowns, surveillance technologies, cyberattacks, platform blocking, and restrictive laws to control online speech and limit civic freedom. Journalists, activists, and civil society groups are being targeted through monitoring, harassment, and prosecutions under vague charges like "false information" or "extremism," while AI-powered surveillance is further expanding state control over digital activity. The report warns that these developments are shrinking civic space and undermining freedom of expression across the region, and it calls for stronger legal protections, accountability, and international action to defend online rights - (11 May 2026). Eurasia Review

NEW CHINESE SURVEILLANCE LEAVES FOREIGNERS NOWHERE TO HIDE

IMAGE SOURCE: DW

A Deutsche Welle investigation reports that China is operating an advanced AI-powered surveillance system capable of tracking individuals—especially foreigners such as journalists—in real time by combining data from facial recognition cameras, travel records, mobile payments, transport systems, and other digital traces into detailed "holistic profiles." The system, revealed through a cybersecurity researcher's accidental access to a police dashboard, reportedly allows authorities to monitor movement down to precise train seats, ski resort check-ins, and daily activity patterns, while also mapping personal relationships through algorithmic analysis. Critics say the technology represents a shift from traditional surveillance to predictive, always-on social control with minimal oversight, raising concerns about privacy, press freedom, and the potential for abuse against foreign nationals and citizens alike - (24 May 2026). DW

SMART GLASSES AND AI PATROLS: CHINA EXPANDS REAL-TIME POLICE SURVEILLANCE

IMAGE SOURCE: MEZ HA

The article reports on China's continued rollout of AI-driven surveillance tools used by police, including smart glasses and advanced monitoring systems that integrate facial recognition, databases, and real-time analytics to identify and track individuals in public spaces. These wearable devices allow officers to scan crowds and instantly match faces against national records, helping them flag suspects, monitor movement patterns, and support policing tasks such as patrols and missing-person searches. The development is part of a broader expansion of "smart policing" infrastructure across Chinese cities, combining cameras, AI software, and connected databases to create highly automated surveillance networks. While authorities say the technology improves efficiency and public safety, critics argue it raises serious concerns about privacy, civil liberties, and the potential for mass monitoring and abuse of personal data - (27 May 2026). Mez Ha

LAWMAKERS CHALLENGE PALANTIR'S ROLE IN U.S. IMMIGRATION SURVEILLANCE

IMAGE SOURCE: DAN GOLDMAN

U.S. Representative Dan Goldman and a coalition of immigration advocates have intensified criticism of Palantir Technologies over its involvement in U.S. immigration enforcement, accusing the company of helping build a large-scale surveillance system used by the Department of Homeland Security (DHS) and ICE. During a rally outside Palantir's New York offices, advocates argued that the company's data-analysis platforms allow authorities to aggregate personal information, track individuals, and support deportation operations with minimal transparency or oversight. Goldman and other lawmakers have also formally demanded answers from DHS regarding the use of Palantir-developed tools alongside facial recognition, cellphone monitoring, and social media surveillance technologies, warning that such systems could threaten civil liberties, privacy rights, and lawful protest activity. The debate reflects growing national concern over how AI-driven surveillance and predictive analytics are being integrated into immigration enforcement and policing - (7 May 2026). Dan Goldman

INTELLIGENCE AGENCIES

SOUTH AFRICA TURNING INTO A PRIVATE SECURITY ESTATE

IMAGE SOURCE: MY BROADBAND

The article argues that South Africa is increasingly resembling a “private security estate” as crime, weak public policing, and declining municipal services push communities and businesses to rely on advanced private security technologies. A University of South Africa study highlighted how tools such as AI-powered surveillance, drones, biometric systems, IoT devices, and large-scale camera networks are rapidly expanding across suburbs and public spaces, often faster than regulations can keep up. Researchers warned that outdated laws, limited cybersecurity safeguards, and insufficient privacy protections could lead to abuse, surveillance overreach, and inequality, as wealthier areas gain access to sophisticated security systems while poorer communities remain underserved - (18 May 2026). My Broadband

SOUTH AFRICAN PROVINCE PUTS UP 960 CCTV CAMERAS TO KEEP AN EYE ON ITS RESIDENTS

IMAGE SOURCE: ST AUGUSTINE RECORD

The article reports that a South African province (Gauteng) has installed 960 CCTV cameras as part of a large-scale public surveillance and crime-prevention initiative costing over R124 million. The system is designed to monitor public spaces, support law enforcement, and improve response to crime across cities, townships, and major routes. However, the rollout has sparked political debate after it was revealed that a significant portion of the network is not fully operational, with reports that around one in four cameras or sites may be offline due to issues such as vandalism, water damage, and equipment failures. Critics argue that poor maintenance and rising upkeep costs weaken the effectiveness of the system, while government officials maintain that most cameras are still functioning and continue to assist policing efforts. The article highlights the broader tension between using large-scale surveillance for public safety and ensuring accountability, reliability, and proper governance of such systems - (14 May 2026). Business Tech

INTEL WATCH

Watching the watchers. Guarding the guardians.

CHINA'S SURVEILLANCE PUSH RAISES ALARM ACROSS AFRICA

IMAGE SOURCE: THE AFRICA REPORT

An investigation into China's growing export of facial recognition and AI-powered surveillance systems to Africa highlights how Chinese tech firms are helping governments across the continent build "smart city" networks that critics say risk enabling mass surveillance and political repression. Companies such as Huawei, ZTE, and Hikvision have supplied cameras, biometric systems, and monitoring platforms to countries including Kenya, Uganda, Zimbabwe, and South Africa, often funded through Chinese loans and infrastructure deals. Supporters argue the technology improves policing and urban management, but rights groups and researchers warn that weak privacy protections and authoritarian tendencies in some states could turn these systems into tools for tracking activists, journalists, and political opponents. Analysts also note concerns that African citizens' biometric data may be used to improve Chinese AI systems while expanding Beijing's geopolitical influence through digital infrastructure projects - (28 May 2026). The Africa Report

ISRAELI SPY-TECH COMPANY SIGNS SECRETIVE €32 MILLION DEAL WITH WEST AFRICAN COUNTRY

IMAGE SOURCE: BUSINESS INSIDER

The article reports that Israeli cyber intelligence company Mer Group has signed a secretive €32 million deal with a West African government to supply a package of homeland security, surveillance, and intelligence systems. The agreement reportedly includes technologies such as monitoring infrastructure, communications systems, and intelligence-gathering tools, although the exact country and full scope of deployment were not publicly disclosed. According to the report, the deal reflects a growing trend of African governments investing in advanced surveillance and cyber-capabilities to address security threats, including terrorism and organised crime. However, it also raises concerns from transparency and human rights perspectives, as critics warn that such technologies can enable increased state surveillance with limited public oversight and accountability. - (15 May 2026) Business Insider

INTEL WATCH

Watching the watchers. Guarding the guardians.

RIGHTS GROUPS URGE US APPEALS COURT TO UPHOLD SPYWARE BAN AGAINST NSO GROUP

IMAGE SOURCE: CADE PROJECT

A coalition of digital rights and press freedom organizations has urged a U.S. appeals court to uphold a permanent ban preventing Israeli spyware company NSO Group from targeting WhatsApp and its users with Pegasus spyware. The groups argue that weakening the injunction would endanger journalists, activists, and human rights defenders worldwide by allowing surveillance tools linked to serious abuses to continue operating unchecked. The case stems from WhatsApp's lawsuit accusing NSO of exploiting its platform to hack more than 1,400 devices globally, with courts increasingly rejecting NSO's attempts to avoid accountability through immunity claims. Advocacy groups say the ruling could become a landmark decision for protecting encryption, digital privacy, and freedom of expression against commercial spyware abuse - (25 May 2026). Cade project

CPJ, PARTNERS FILE AMICUS BRIEF TO PROTECT ENCRYPTION FROM PEGASUS SPYWARE

IMAGE SOURCE: CPF

The Committee to Protect Journalists (CPJ) and 10 partner organizations have filed an amicus brief in the U.S. Ninth Circuit Court of Appeals urging judges to preserve a permanent injunction against NSO Group, the maker of Pegasus spyware, arguing that weakening the ruling would threaten encrypted communication and expose journalists, activists, and human rights defenders to surveillance and abuse. The brief supports WhatsApp and Meta's long-running lawsuit accusing NSO of using WhatsApp servers to infect more than 1,400 devices across 20 countries with Pegasus spyware, which has repeatedly been linked to attacks on the press and civil society. CPJ says strong encryption is essential for protecting journalists' sources and safety, warning that allowing NSO to resume operations against WhatsApp users could undermine global digital rights and accountability efforts against commercial spyware companies - (22 May 2026). CPJ

CHINESE INITIATIVE NORMALIZES 'TECHNO-AUTHORITARIANISM'

IMAGE SOURCE: ADF

The article argues that a recent Chinese-led global governance push is helping to normalise "techno-authoritarianism", where governments use advanced digital tools—such as surveillance systems, AI monitoring, biometric tracking, and data-driven control—to manage and influence populations. It warns that this model risks spreading beyond China by offering developing countries affordable surveillance infrastructure that can be used for political control, censorship, and social monitoring, often under the banner of modernization and security. The piece highlights concerns that this trend could weaken democratic norms in Africa by embedding surveillance technologies into state systems without strong transparency or accountability safeguards. It also suggests that dependence on imported digital infrastructure may leave countries vulnerable to external influence over their data and governance systems, potentially reshaping how power is exercised in the digital age - (5 May 2026). ADF

BILL C-22 SPARKS FIERCE DEBATE OVER DIGITAL SURVEILLANCE POWERS IN CANADA

IMAGE SOURCE: JUNO NEWS

Canada's proposed Bill C-22, the Lawful Access Act, has triggered widespread controversy as critics warn it could significantly expand state surveillance capabilities by requiring digital service providers to retain user metadata, enable lawful access to communications, and potentially build technical systems that could weaken or bypass encryption. Civil liberties groups, privacy experts, and major tech companies like Apple and Google argue the bill risks undermining end-to-end encryption and could allow secret government orders to access data without sufficient judicial oversight, effectively creating a surveillance infrastructure across messaging apps, cloud services, and telecom networks. The Canadian government insists the legislation is intended to improve law enforcement's ability to investigate serious crimes and denies that it mandates "backdoors" or mass surveillance, saying safeguards exist to prevent systemic security vulnerabilities - (27 May 2026). Juno News

INTEL WATCH

Watching the watchers. Guarding the guardians.

AI SURVEILLANCE WITHOUT RULES: EXPERTS WARN CANADA'S POLICING LAWS ARE LAGGING BEHIND TECHNOLOGY

IMAGE SOURCE: LAW 360

A legal commentary in Law360 Canada argues that Canadian legislation has not kept pace with the rapid rise of modern police surveillance tools, including spyware, facial recognition, and advanced data analytics that can deeply intrude into personal digital lives. The article highlights concerns that technologies now being explored or used by law enforcement can access nearly all aspects of a person's smartphone activity—messages, location data, camera feeds, and microphone access—far beyond what traditional wiretap laws were designed to regulate. It also points to allegations involving Ontario police and commercial spyware, warning that current oversight frameworks are fragmented, outdated, and lack clear rules on transparency, data retention, and accountability. The author argues that without updated laws, Canada risks allowing powerful surveillance systems to expand with limited democratic control or meaningful safeguards, raising serious constitutional and privacy concerns under the Charter - (20 May 2026). Law 360

DO AI RISKS REQUIRE EXTRAORDINARY GOVERNMENT INTERVENTION?

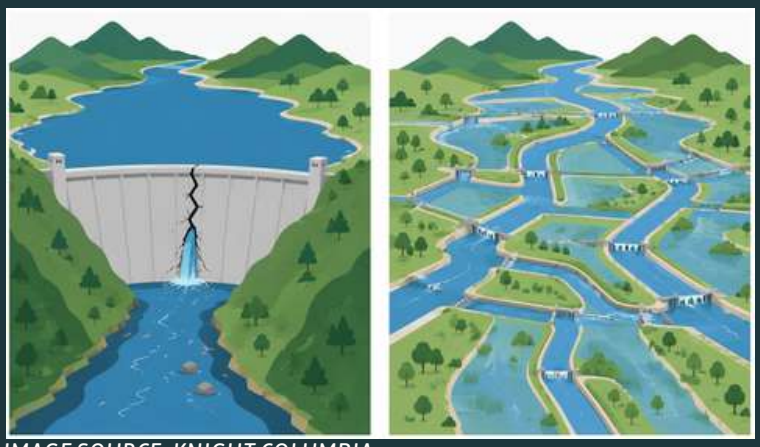

IMAGE SOURCE: KNIGHT COLUMBIA

The essay argues against the idea that AI's risks justify "extraordinary" government intervention such as strict pre-release restrictions, emergency powers, or heavy centralized control over AI development. The authors agree that AI can create serious risks like misuse, cyberattacks, biosecurity threats, and social disruption, but they argue these are better handled through "resilience" rather than sweeping top-down controls. Resilience means strengthening society's ability to detect, absorb, and respond to harms—such as improving cybersecurity systems, expanding oversight tools, and investing in public-sector capacity—rather than trying to tightly restrict AI companies or model releases. They warn that extraordinary interventions are hard to enforce, risk concentrating government power, and may fail in a fast-moving, widely distributed technology environment. Instead, they suggest treating AI more like other general-purpose technologies and focusing on normal democratic policymaking, institutional improvement, and layered defenses that make society safer regardless of how AI evolves - (21 May 2026). Knight Columbia

SHIVA'S EYE: INDIA'S RISE IN THE GLOBAL SPYWARE ECONOMY

IMAGE SOURCE: IN CYBER

The article argues that India has evolved from being primarily a consumer of surveillance tools like Pegasus into a significant global hub for the commercial spyware industry, often described as "spyware-as-a-service." It explains how a mix of government digitalisation efforts, a large pool of skilled cybersecurity talent, and weak regulatory oversight has enabled the growth of private firms offering hacking, surveillance, and data extraction services to a wide range of clients. These companies operate in a grey zone where tools marketed as cybersecurity or intelligence solutions are also used for intrusive spying, including zero-click phone hacks, data interception, and targeted surveillance. The piece highlights how this ecosystem has expanded beyond government clients to private actors such as corporate investigators and law firms, creating an international supply chain for digital espionage. While supporters frame it as part of India's tech and security growth, critics warn it normalises surveillance practices that can be misused against journalists, activists, and private individuals - (20 May 2026). In Cyber

---

THE BORDER SURVEILLANCE TOWER LINKING THE U.S. AND MEXICO

IMAGE SOURCE: DROPSITNEWS

The article reports that U.S. federal agencies—including the FBI, DEA, ATF, Homeland Security Investigations, and Customs and Border Protection—are set to operate from a new high-tech surveillance hub inside the Centinela Tower in Ciudad Juárez, Chihuahua, deepening cross-border intelligence cooperation with Mexican authorities. The tower is part of Chihuahua's "Plataforma Centinela" system, which integrates thousands of surveillance cameras, drones, license-plate readers, facial-recognition tools, and other AI-driven monitoring technologies to track criminal activity along the border. Despite a recent political scandal involving unauthorized CIA participation in a Mexican anti-drug operation that resulted in multiple deaths and diplomatic tension, officials are moving ahead with formalised intelligence-sharing arrangements focused on drug trafficking, weapons smuggling, immigration enforcement, and organised crime. Supporters say the system improves coordination and security, while critics warn it reflects growing concerns over transparency, sovereignty, and the expansion of cross-border surveillance infrastructure - (15 May 2026). DropsitNews

INTEL WATCH

Watching the watchers. Guarding the guardians.

HAVE YOUR SAY!
LETTER TO THE EDITOR

Dear Readers:

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

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

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

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

Warm regards
The Intelwatch Team

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

INTEL WATCH

Watching the watchers. Guarding the guardians.

GET INVOLED!

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

FIND US ON SOCIAL MEDIA

@IntewatchNews

HAVE ANY QUESTIONS?

info@intelwatch.org.za

The Reynolds Foundation Now for tomorrow

Global Dialogue

Luminate

Funded by the European Union

We are grateful for the support of our donors!