Inaugural edition

INTEL WATCH

May 2025

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 REPORTS & RESEARCH

INTELWATCH UPDATES & SURVEILLANCE UPDATES

REPRESSION MONITOR

INTELLIGENCE AGENCIES

Watching the watchers. Guarding the guardians.

WELCOME TO INTELWATCH: THE DAWN OF ACCOUNTABILITY!

DEAR READERS:

Today, we embark on a transformative journey together. With immense pride and purpose, Intelwatch introduces its first-ever newsletter–a monthly beacon for truth, transparency, and the defense of human rights in the digital age. Intelwatch was founded with a singular mission: to shine a light on the shadowy practices of state and private intelligence agencies. As a research and advocacy organization rooted in the global South, we are committed to empowering citizens, informing policymakers, and strengthening democratic oversight over surveillance systems that shape our lives.

WHAT INTELWATCH STANDS FOR:

- **Research:** We investigate the hidden mechanisms of surveillance and intelligence operations.
- **Policy Work:** We advocate for laws and regulations that protect privacy and uphold human rights.
- **Activism:** We support grassroots movements fighting for transparency and accountability.

In an era where technology is increasingly weaponized against individuals, Intelwatch exists to ask the critical question: ***Do you know who's watching you?***

This newsletter is more than just a publication–it's a call to action. Together, we can challenge systems of unchecked power and build a future where privacy is not a privilege but a right.

EDITORIAL TEAM

EXECUTIVE DIRECTOR	PAULA CRISTINA ROQUE
EDITOR & HEAD OF ADVOCACY AND CAPACITY BUILDING	HERBERT MOYO
CONTENT, DESIGN AND LAYOUT	SISIPHO MBALO

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

BENEATH THE SURFACE: SOUTH SUDAN'S INTELLIGENCE SERVICES' REIGN OF TERROR

BY REMEMBER MIAMINGI

DOWNLOAD REPORT

Key findings:

This report exposes the National Security Service (NSS) of South Sudan as a principal instrument of repression, democratic regression, and instability. Established to safeguard national security, the NSS has instead evolved into a 40,000-strong personalised political militia with unchecked power. The NSS is fundamentally instrumentalised to retain President Salva Kirrs' centralised power of the state, society, the economy and international partners. Its activities have not only undermined efforts to achieve peace, democratic governance, civil liberties, and the rule of law within the country but have also extended its reach beyond South Sudan's borders.

The NSS operates like a state within a state, a driver of political control, fear-based loyalty, repression and a counterweight to neutralise any dissent, military threats or coup attempts against President Salva Kiir. Allegations of shadow networks, including groups carrying out extrajudicial killings at the behest of senior officials, underscore the agency's role in consolidating regime power. The NSS has also neutered freedom of expression, assembly, political pluralism, the press and civil society with the use of a wide system of surveillance, censorship mecahnisms and bureaucratic restrictions.

Central to the NSS's pervasive influence lies the extensive powers granted through the 2014 National Security Service Act and its subsequent amendments. These powers include arbitrary detention, surveillance, and property seizure, all carried out with minimal legal oversight. The NSS consistently exceeds constitutional limits, engaging in policing and other extra-legal activities far surpassing its officially mandated intelligence gathering role, and is frequently implicated in arbitrary detentions, torture, extrajudicial killings, and enforced disappearances.

This unfettered authority has directly facilitated a wide range of human rights abuses, in line with the ruling party's intolerance for dissent , public scrutiny, accountability and criticism. Detention centres, such as the notorious 'Blue House', serve as grim sites where detainees face harsh conditions without trial, enduring physical abuse and other inhumane treatment. Such practices erode the principles of justice and public trust in the rule of law, creating an environment of systemic rights violations and impunity. The cumulative effect of these practices has profoundly undermined democracy and governance in South Sudan. By suppressing dissent, the NSS erodes political pluralism, weakens judicial institutions, and stifles the emergence of alternative political voices. Civil society and media freedom are severely restricted, as organisations are subjected to surveillance, harassment, and financial reprisals.

In addition to direct abuses, an extensive surveillance apparatus bolsters the NSS's repressive tactics. The agency targets political opponents, journalists, and civil society organisations by employing phone tapping, informant networks, and digital monitoring. This pervasive surveillance infrastructure generates an ubiquitous climate of fear that stifles free expression, discourages public political engagement, and effectively silences dissenting voices. Consequently, opposition becomes fragmented and civic participation is curtailed, further entrenching authoritarian control.

The NSS's capacity to repress dissent does not stop at South Sudan's borders. The agency's cross-border operations, often conducted with the complicity of neighboring states, target dissidents abroad. These transnational repressive practices demonstrate a willingness to violate international norms, further extending its destabilizing influence beyond its home territory.

Despite mounting evidence and numerous calls for accountability, the leadership of the NSS continues to operate with impunity. While some individuals and institutions in South Sudan have faced sanctions–often with lesser criminal culpability–international actors have failed to hold NSS leaders accountable.

This lack of meaningful action has emboldened the agency and its leadership to persist in their abuses. It is imperative that the silence surrounding these violations ends and that decisive measures are taken against both past and present leaders of the NSS, thereby confronting impunity and upholding justice in South Sudan. The report underscores the need for comprehensive reform of the NSS as part of a broader strategy to dismantle South Sudan's militarised and exclusionary governance structures.

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

RUSSIAN SECURITY ASSISTANCE IN AFRICA: SOVIET IN STYLE; EXTRACTIVE IN SUBSTANCE; DESTABILISING IN IMPACT

BY LIAM O'SHEA

DOWNLOAD REPORT

Key findings:

Russia provides a variety of forms of security assistance to African countries, formally, via military agreements and arms sales, and informally by using private military companies (PMCs) to bolster regimes' security. The distinction between the two is often unclear.

Multiple Russian state and state-affiliated actors and networks use a wide variety of tools and techniques to further both the Russian state's and their own political, economic and security interests. Though the picture is murky, it is possible to isolate several components of a Russian security assistance 'playbook'.

This report sets out the elements of this 'playbook.' It provides an overview of the range of techniques and tools deployed by Russian actors, which include the formal components, described above, and 'assistance' delivered by PMCs. This includes directing and supporting combat operations, training local security forces, protecting regimes' personnel and assets, and coupling these with the provision of political disinformation campaigns. In recent years, the informal component had predominated, primarily through the Wagner Group.

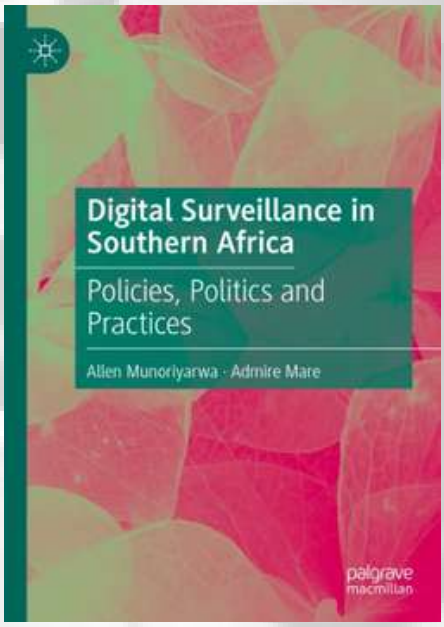
Russian assistance comes at a cost. The model of counter-insurgency provided by Russian PMCs is highly violent and encompasses collective punishment. For all Russia's talk of enhancing stability and supporting decolonisation, what it actually does is support regimes to exert their power, often with grave violations of human rights. For elites costs are quite literal. In some contexts, such as the Central African Republic (CAR), regime security is provided in exchange for lucrative contracts, mostly for 1 resource extraction. Costs may also become political as elites become dependent on an unstable partner.

The model is however likely to remain attractive. Overall, Russian security assistance provides regimes' elites with a means to enhance their security using resources otherwise unavailable to them, and without some of the restrictions that can come with Western security assistance (e.g. around human rights). Globally, and in Africa, Russia has framed itself as a reliable security partner to authoritarian regimes. Rather than simply providing regime survival packages, Wagner has helped governments address various security challenges, including conducting brutal counterinsurgency operations that other actors avoid; and to helping regimes assert their sovereign authority against external interference. There is likely to remain a demand for the violence and force Russian security assistance can provide.

Although the Russian state has sought to gain more direct control over Wagner institutions following the June 2023 Prigozhin mutiny, it remains reliant on the flexibility afforded by the Prigozhin model. This remains attractive to some African countries (e.g. Mali), which have sought to resist the extractive costs associated with Wagner deployments and prefer assistance provided by units with a degree of autonomy from the Russian state.

EXCLUSIVE INTELWATCH REPORTS & RESEARCH

CYBERSECURITY LAWS ENABLE STATE OVERREACH



BOOK COVER: SPRINGER NATURE

This book by Allen Munoriyarwa - a board member of Intelwatch - and Admire Mare "critically examines the manifest and latent practices of surveillance in the southern African region, using case studies from South Africa, Zimbabwe, Zambia, Namibia, Botswana and Mozambique. The book demonstrates the growing role of super-powers in the construction and normalization of the surveillance state. It traces the digitization of surveillance practices to the rapid adoption of smart CCTV, facial recognition technologies and EMSI catchers. Through predictive policing mechanisms, state security agencies have appropriated digital media technologies for sentiment analysis, constant monitoring of digital footprints of security targets, and even deploying cyber-troops on popular social media platforms.

The authors argue that surveillance practices have thus been digitized with deleterious impact on the right to privacy, peaceful assembly and freedom of expression in the region. Furthermore, they argue that specific laws and regulations governing surveillance practices in the region are lagging behind. Finally, the book demonstrates how digital surveillance have significantly infiltrated the political, economic and social fabric of Southern Africa.

This book provides much needed systematic, cutting-edge research into the trends, practices, policies and geo-political interests at the center of surveillance practices in the region, providing a crucial link between human rights, such as freedom of privacy and expression, and political authoritarianism - Springer

Watching the watchers. Guarding the guardians.

INTELWATCH UPDATES:
MEDIA RESILIENCE IN SOUTHERN AFRICA PROJECT
MEDIA DEFENSE TRAINING

In light of the proliferation of repression and threats against journalists in Africa, Intelwatch hosted a powerful and intensive 8-day (3 overlapping 4 day trainings) Media defense training from 30 April - 7 March 2025 in South Africa, bringing together 60 high-risk investigative journalists and media practitioners from 7 Southern African countries with the aim of strengthening their investigation and reporting capacities and safety through digital, physical, and psychological threat mitigation strategies, capacity building, advocacy and awareness campaigns.

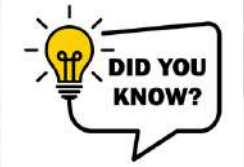
The training was designed to equip these frontline journalists and media practitioners with essential skills and knowledge to carry out their work safely and effectively under threat. With the support of leading experts, participants received extensive training on Cybersecurity essentials for journalists, how to conduct investigations safely, First Aid protocols, how to respond to cyber threats targeting journalists, digital security protocols, preventative physical safety measures, legal recourse strategies, and gender harassment mitigation.

This training represents a vital step in empowering journalists who face significant risks due to their courageous work exposing corruption, human rights abuses, and other sensitive issues. By strengthening their safety, resilience, and legal protections, Intelwatch is advancing the important cause of Defending Human Rights, Protecting Civic Space in the digital age, amplifying the need for transparency and accountability and holding power accountable across the Global South and beyond.

Funded by the European Union

The training is an integral component of what is envisaged to be a two year project, running from January 2025 to January 2027, that aims to help strengthen the operational environment for media practitioners in 7 Southern African countries. This project comes against the backdrop of the reality of cyber control, surveillance, and manipulation of the truth is rapidly becoming the next frontline of an invisible war on democracy and those protecting the civic space, including journalists and media practitioners. In addition, gender based harassment of female journalists is rife in the region.

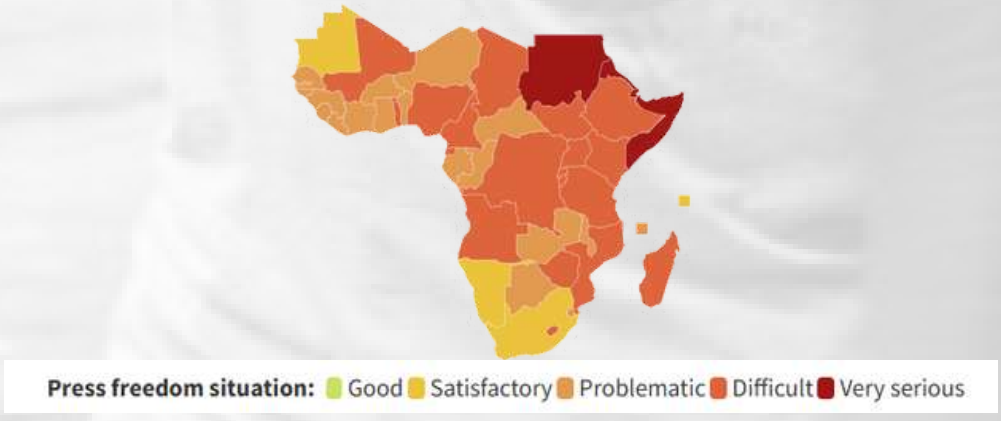
Intelwatch hopes that the training and the two year project in its entirety will ensure a media sector that is technically capacitated to mitigate various safety risks, ranging from digital security risks, to gender harassment. This training as well as the project was made possible by the generous support of the European Union.



ACCORDING TO THE 2025 RSF WORLD PRESS FREEDOM INDEX, ECONOMIC FRAGILITY IS A LEADING THREAT TO PRESS FREEDOM:

The 2025 World Press Freedom Index by Reporters Without Borders (RSF) reveals that global press freedom has reached a historic low, with the economic conditions for journalism now classified as a "difficult situation" for the first time. The report highlights that concentrated media ownership, lack of transparent public support, and reliance on advertisers have forced news organizations into financially precarious positions, undermining quality reporting and editorial independence. Nearly one-third of countries have seen media outlets close for economic reasons, and even democracies like New Zealand and South Africa are struggling. The dominance of tech giants in online advertising has further strained media revenues. Conflict zones and authoritarian states face catastrophic conditions, with mass closures and journalist exiles. RSF calls for urgent government action to ensure transparent, stable funding and protect media pluralism, warning that without economic independence, press freedom-and thus democracy-is at serious risk - RSF

PRESS FREEDOM SITUATION IN AFRICA:



MAP SOURCE: REPORTERS WITHOUT BORDERS

SURVEILLANCE UPDATES

DEEPFAKE POLITICAL UNREST WARNING IN SOUTH AFRICA

IMAGE SOURCE: DAILY INVESTOR

Deepfakes pose a significant threat to South Africa, potentially leading to political unrest, financial fraud, and reputational damage, particularly with local government elections approaching. Accenture Africa's security lead, Boland Lithebe, warns that manipulated videos and audio created using AI could spread misinformation, erode trust in institutions, and be used to discredit political figures or trigger financial panic. He suggests using AI-powered verification tools, public education campaigns, regulatory reforms, and increased social media platform responsibility to mitigate the impact of deepfakes, emphasizing the need to prepare defenses before a major deepfake crisis occurs. The FSCA has already dealt with a case involving deepfake ads promising profits and featuring Elon Musk, Johann Rupert, and Nicky Oppenheimer, which led to investors losing millions - Daily Investor

14% INCREASE IN SPYWARE ATTACKS ON AFRICAN BUSINESSES

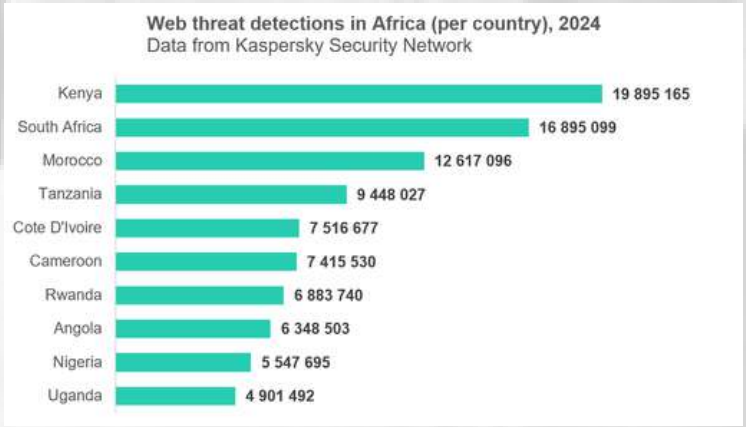


IMAGE SOURCE: KASPERSKY

Kaspersky's recent cyberthreat analysis at GITEX Africa reveals a rise in cyberattacks targeting African businesses. The report indicates a 1.2% increase in web threats, a 4% increase in local threats, and a significant 14% surge in spyware attacks from 2023 to 2024. Password stealers also saw a 26% increase, with Kenya, Morocco, and South Africa being the most targeted countries. Kaspersky recommends that organisations prioritise cybersecurity investments, training, and digital literacy to combat these rising cyber threats, while individual users should use strong passwords, update software, and avoid suspicious links - Kaspersky

WHY NIGERIA MUST PRIORITIZE CYBERSECURITY

IMAGE SOURCE: CIO AFRICA

Nigeria's rapid digital transformation has outpaced its investment in cybersecurity, leaving critical public sector systems-such as tax, identity, and electoral platforms-vulnerable to breaches like the recent Gombe State IRS hack. Chronic underfunding, a shortage of skilled personnel, outdated software, and weak security practices have created fertile ground for cybercriminals, undermining public trust and threatening national security. Despite having robust cybersecurity policies on paper, implementation is lacking due to insufficient leadership accountability, inadequate training, and a lack of independent audits and incident response plans. The article calls for urgent, top-level government action: mandating compliance, properly funding cybersecurity, building internal expertise, regularly testing response plans, and holding leaders accountable to safeguard Nigeria's digital future - CIO Africa

COMBATING DIGITAL THREATS TO SAFEGUARD PRESS FREEDOM

IMAGE SOURCE: ACCESS NOW

The article highlights that World Press Freedom Day 2025 comes amid a crisis for global journalism, with 2024 being one of the deadliest years for journalists in decades. Press freedom faces escalating digital threats: the unchecked rise of spyware targeting journalists worldwide, persistent attacks on encryption that endanger source protection, increasing disinformation and online abuse, and the weaponization of cybercrime laws to silence dissent. Governments are exploiting national security narratives to justify censorship and repression, while shrinking civic space and funding cuts further undermine independent media. The article calls for urgent, coordinated action to address these threats, safeguard journalist safety, and defend press freedom in the digital age - Access Now

INTEL WATCH

Watching the watchers. Guarding the guardians.

HOW GHANA'S PEGASUS PURCHASE IGNITES PRIVACY CONCERNS ACROSS AFRICA

IMAGE SOURCE: UNITE AI

Ghana's acquisition of the Pegasus spyware, developed by Israel's NSO Group, has sparked global concerns about privacy, democracy, and ethical surveillance practices. Purchased for $5.5 million in 2015 under dubious circumstances, Pegasus enables invasive monitoring of smartphones, granting access to calls, messages, GPS data, and microphones with minimal user interaction. Legal challenges arose in 2020 when Ghana's High Court deemed the procurement illegal, citing misuse by officials and lack of accountability. The case highlights broader issues of surveillance overreach and Israel's growing influence in Africa through advanced technologies, mirrored by similar practices from Chinese firms like Huawei. Globally, Pegasus has prompted regulatory scrutiny, with the U.S. restricting NSO Group's market access and the EU calling for stricter oversight of spyware technologies. This controversy underscores the urgent need for international frameworks to balance national security interests with individual privacy rights in the digital age - Unite AI

ISC HOLDINGS LTD NAMED IN GHANA SPYWARE CORRUPTION SCANDAL

IMAGE SOURCE: GHANA BUSINESS NEWS

Another Israeli company, ISC Holdings Ltd, is implicated in a corruption scandal in Ghana involving the former Director-General of the National Signals Bureau (NSB), Kwabena Adu-Boahen. Adu-Boahen allegedly diverted GH¢49 million (about $7 million) meant for "cyber defence systems" to a private company co-owned with his wife, with only $1.75 million reaching ISC Holdings. The remaining funds were reportedly used for private investments and properties. This scandal follows a previous one involving the NSO Group's Pegasus spyware, raising concerns about corruption and misuse of surveillance technology in Ghana. The NSB, established in 2020, is meant to provide secure signal systems for national security and protect Ghana's cyberspace - Ghana Business News

APPLE SENDS NEW SPYWARE WARNING, JOURNALISTS AND ACTIVISTS AMONG THOSE TARGETED

IMAGE SOURCE: JAGRAN

In April 2025, Apple issued new threat notifications to iPhone users in over 100 countries, warning journalists, activists, and other high-profile individuals that they were being targeted by sophisticated mercenary spyware attacks similar to previous Pegasus incidents. These targeted attacks aim to remotely compromise devices based on users' identities or activities, often linked to government or state-sponsored surveillance. Apple urged affected users to enable Lockdown Mode and follow strict security practices, emphasizing that while such attacks are rare and highly advanced, they pose serious risks to those in sensitive professions. The company has been sending such alerts since 2021 and remains committed to protecting at-risk users through timely notifications and security guidance - Jagran

NEW YORK'S SUBWAY AI SURVEILLANCE PLAN SPARKS PRIVACY ALARMS

IMAGE SOURCE: WIN BUZZER

New York's Metropolitan Transportation Authority (MTA) is advancing plans to use AI-powered surveillance across its subway system to detect "problematic behavior" in real time, aiming for "predictive prevention" to alert police before crimes occur. While the MTA insists the technology focuses on behaviors-not individuals-and excludes facial recognition, civil liberties groups warn the system risks reinforcing bias, expanding mass surveillance, and disproportionately targeting marginalized communities. The initiative involves partnerships with major tech companies like Google and Amazon, raising concerns about data privacy, corporate influence, and ethical implications amid broader controversies over AI surveillance. Despite existing state laws limiting biometric use and some AI policy guidelines, regulatory oversight remains weak, fueling debate over balancing public safety with protecting civil rights and transparency. - Win Buzzer

INTEL WATCH

Watching the watchers. Guarding the guardians.

MILITARY-GRADE SPYWARE IN CONSUMER STALKERWARE APPS

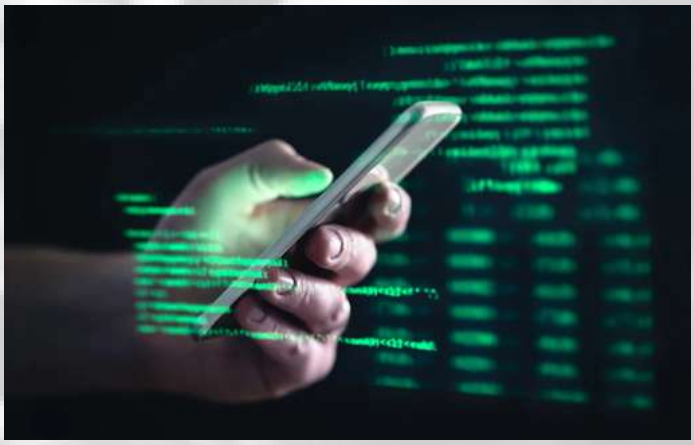


IMAGE SOURCE: CYBERSNOWDEN

Consumer stalkerware apps, marketed as parental monitoring tools, increasingly contain military-grade spyware, raising serious ethical and security concerns. These apps, like mSpy and FlexiSpy, enable unauthorized tracking of location, calls, messages, and social media activity, exploiting vulnerabilities and collecting vast amounts of personal data. Despite efforts by Google, Apple, and the FTC to regulate and remove such apps, many continue to thrive, posing risks of stalking, harassment, and corporate espionage. Individuals can protect themselves by monitoring device activity, reviewing app permissions, using anti-spyware scans, and keeping software updated, while stronger regulatory measures and public awareness are crucial to combating the dangers of invasive surveillance software - Cyber Snowden

SIGNAL ISN'T INFALLIBLE, DESPITE BEING ONE OF THE MOST SECURE ENCRYPTED CHAT APPS

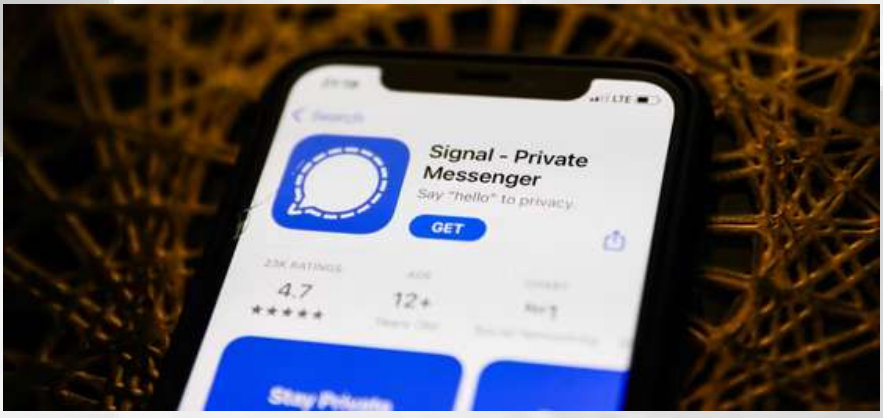


IMAGE SOURCE: JAKUB PORZYCKI / NURPHOTO VIA GETTY IMAGES FILE

The Signal messaging app, widely regarded for its encryption, has faced scrutiny following incidents that exposed vulnerabilities in its use for sensitive communications. Notably, Defense Secretary Pete Hegseth accidentally disclosed U.S. military plans in a Signal group chat before strikes on Houthi militia in Yemen. The NSA had previously issued a bulletin warning employees of Signal's vulnerabilities, emphasizing its susceptibility to surveillance and espionage targeting high-profile users. Concerns include phishing attacks and potential exploitation by adversaries like Russia and China. While Signal remains secure overall, these incidents highlight risks when used for critical government or military discussions - NBC News

CHINESE FACIAL RECOGNITION DATABASE LEAK RAISES GLOBAL ALARM OVER MASS SURVEILLANCE, PRIVACY, AND IDENTITY VULNERABILITY

IMAGE SOURCE: NEWSWIRE NETWORK

A massive security breach in April 2025 exposed a Chinese facial recognition database containing sensitive personal data of over 2.5 million individuals, including names, ID numbers, photos, locations, and employer details. The leak, involving SenseNets-a major AI firm specializing in facial recognition-highlighted the risks of mass surveillance, privacy violations, and identity theft inherent in centralized biometric systems. This incident underscores China's extensive surveillance infrastructure, including its Social Credit System, which monitors citizens' behavior and enforces social control through rewards and punishments. The breach has global implications, especially for vulnerable groups like ethnic minorities, dissidents, and journalists, who face heightened risks of wrongful targeting and repression. Experts warn that biometric data breaches are particularly dangerous since faces and fingerprints cannot be changed, fueling calls for stronger international regulation and privacy protections - NEWSWIRE NETWORK

CELLEBRITE HALTS PRODUCT USE IN SERBIA

IMAGE SOURCE: AMNESTY INTERNATIONAL

Following an Amnesty International report on the misuse of spyware and mobile forensic products by Serbian authorities to unlawfully target activists and journalists, Cellebrite has announced it will stop the use of its digital forensic equipment for some of its customers in Serbia. Amnesty International's investigation revealed that Serbian police and intelligence routinely misused Cellebrite's equipment outside legally sanctioned processes to target civil society activists and independent journalists critical of the government. Amnesty International is calling for Serbian authorities to conduct thorough investigations, hold those responsible to account, and establish safeguards to prevent future abuse, while also urging Cellebrite to revamp its due diligence processes - Amnesty International

NEW LIGHTSPY SPYWARE VARIANT COMES WITH ENHANCED DATA COLLECTION FEATURES TARGETING SOCIAL MEDIA PLATFORMS

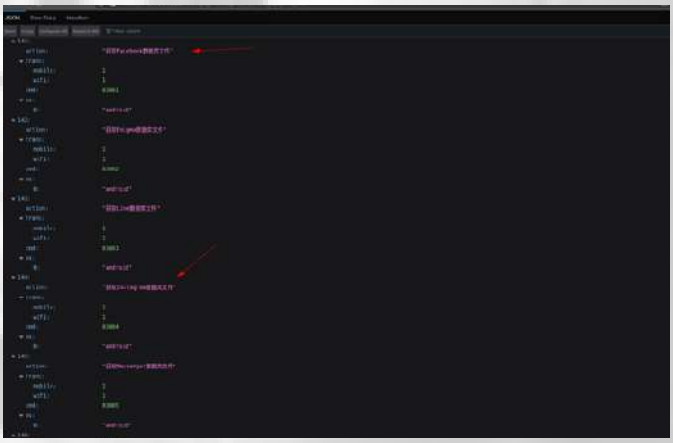


IMAGE SOURCE: SECURITY AFFAIRS

The latest version of LightSpy spyware has significantly expanded its capabilities, targeting social media platforms like Facebook and Instagram to extract private messages, contact lists, and metadata. Originally discovered in 2020, LightSpy is a modular surveillance tool capable of infecting devices across multiple platforms, including Windows, macOS, Linux, and mobile systems. Recent updates include over 100 commands and new plugins for enhanced data collection and operational control. The spyware also incorporates destructive features, such as preventing infected iOS devices from booting up, while adding plugins for Windows systems focused on surveillance. Researchers have identified infrastructure details, such as admin panels and endpoints, revealing insights into how operators manage compromised devices. LightSpy's evolving framework highlights increasing threats to privacy and cybersecurity across platforms - Security Affairs

META'S UK FACIAL RECOGNITION APPROVED, CRITICS WARN OF CHINESE-STYLE SURVEILLANCE

IMAGE SOURCE: PEXELS

Meta's facial recognition technology has been approved for use in the UK, aiming to combat celebrity deepfake scams by matching images against verified profiles and ensuring data is encrypted and deleted after use. Critics warn this development could pave the way for surveillance systems resembling China's, where extensive facial recognition and AI-driven monitoring are used to predict threats and detain individuals based on behavior. Privacy advocates in the UK have expressed concerns over increasing government reliance on facial recognition, including proposals to create a national database and expanded use by police, which they argue risks misidentifications and undermines civil liberties. Additionally, social media platforms may soon be required to adopt facial recognition for age verification, raising further debates about privacy and surveillance - CCN

REPRESSION MONITOR

SAHRAWI ACTIVIST CONDEMNS MOROCCO'S USE OF PEGASUS SPYWARE IN WESTERN SAHARA

IMAGE SOURCE: BURAK AKBULUT – ANADOLU AGENCY

Sahrawi activist Ghalia Abdallah Djimi condemned Morocco's use of Pegasus spyware to monitor and intimidate journalists and activists in Western Sahara, speaking at the UN Human Rights Council. She highlighted that Moroccan authorities exploit this technology to violate human rights, particularly targeting women with defamation and intimidation to silence free voices. Djimi called for a comprehensive investigation into the use of Pegasus in Western Sahara and urged the international community to take urgent action to protect privacy and freedom of expression - Middle East Monitor

ACTIVIST ALERTS ICC TO SPYWARE ATTACK

IMAGE SOURCE: REMO CASILLI / REUTERS

David Yambio, the founder of Refugees in Libya, has alerted the International Criminal Court (ICC) about a spyware attack on his mobile phone while he was providing evidence on human rights abuses in Libya. Yambio, a vocal critic of Italy's migrant pact with Libya, has been targeted with Paragon's Graphite spyware, which is capable of accessing sensitive data. This incident highlights the misuse of surveillance technology against human rights defenders and journalists in Italy, with several activists and journalists, including Luca Casarini and Francesco Cancellato, also being targeted. The Italian government has denied involvement, but Paragon Solutions terminated its contract with Italy due to alleged misuse. The situation underscores Europe's broader spyware crisis, with Amnesty International calling for stricter regulations to protect civil society from such invasive surveillance tools - The Guardian

NGE, SERAP, DEMAND END TO ABUSE OF CYBERCRIMES ACT AGAINST JOURNALISTS

IMAGE SOURCE: FOREFRONT NG

The Nigerian Guild of Editors (NGE) and the Socio-Economic Rights and Accountability Project (SERAP) have condemned the continued misuse of the Cybercrimes Act, particularly its 2024 amendment, to repress journalists, activists, and peaceful critics in Nigeria. They argue that section 24 of the Act, which criminalizes "cyberstalking," is vague, inconsistent with Nigeria's Constitution and international human rights standards, and has been used to arbitrarily arrest and intimidate media professionals and social media users. Both organizations call for the immediate release of those detained, an end to harassment under the Act and related broadcasting regulations, and urgent reforms to align the law with constitutional guarantees and press freedom. They urge President Tinubu, state authorities, and the National Assembly to respect freedom of expression, protect journalists, and revise repressive laws to uphold democracy and human rights. - Forefront NG

2ND ITALIAN INVESTIGATIVE JOURNALIST TARGETED WITH SMARTPHONE SPYWARE

IMAGE SOURCE: CPJ

In 2025, two investigative journalists from Italy's Fanpage.it-known for probing corruption and organized crime-were targeted with sophisticated smartphone spyware, raising serious concerns about surveillance aimed at intimidating the press. Reporter Ciro Pellegrino received an Apple alert confirming spyware targeting, following a similar attack on editor-in-chief Francesco Cancellato earlier in the year involving Paragon spyware via WhatsApp. Despite an ongoing investigation by Rome's prosecutor into unauthorized surveillance, questions remain about government involvement and the legality of such operations, especially after leaks suggested some spyware use was authorized against migrant rights activists but not journalists. The Committee to Protect Journalists (CPJ) urges Italian authorities to conduct a transparent probe, hold perpetrators accountable, and safeguard journalistic freedom from digital threats. - biometric CPJ

GREEK DEMOCRACY IS BEING DISMANTLED

IMAGE SOURCE: INDEX ON CENSORSHIP

The article exposes how Greek democracy is being systematically undermined following the 2022 "Greek Watergate" spyware scandal, where government-linked officials, including associates of Prime Minister Kyriakos Mitsotakis, used Predator spyware to surveil political opponents, journalists, and even ministers. Despite widespread evidence, the government denies involvement, obstructs investigations, and uses strategic lawsuits (SLAPPs) to intimidate the press. Mitsotakis's administration has been accused of media manipulation, selective funding favoring pro-government outlets, and deploying coordinated online troll campaigns to suppress dissent. These actions mirror illiberal tactics seen elsewhere in Europe, contributing to democratic backsliding, erosion of press freedom, and weakening of transparency and accountability in Greece. The article warns that without urgent reforms, Greece risks further entrenching authoritarian practices that threaten the foundations of its democracy - Index on Censorship

GREECE: INVESTIGATIVE MEDIA WIN LATEST VICTORY IN SPYWARE SLAPP RULING

IMAGE SOURCE: INTERNATIONAL PRESS INSTITUTE

A Greek court has overwhelmingly dismissed lawsuits against journalists from Reporters United and Efimerida ton Syntakton, who had reported on the Prime Minister's nephew, Grigoris Dimitriadis, and his connection to a spyware scandal. The court found the journalists' reporting-detailing how Dimitriadis' phone number was used to target 11 individuals with spyware-was accurate and contained no defamatory content. Dimitriadis, who sought nearly €1 million in damages, was ordered to pay legal costs, though the court did rule that a single headline by EfSyn constituted simple defamation, resulting in a minor penalty. Press freedom groups welcomed the ruling as a victory against abusive SLAPP lawsuits intended to silence public interest journalism, even as concerns remain over the lack of legal recognition for SLAPPs in Greece - biometric International Press Institute

CHINA-LINKED SPYWARE TARGETING COMMUNITIES DEEMED THREAT TO CCP

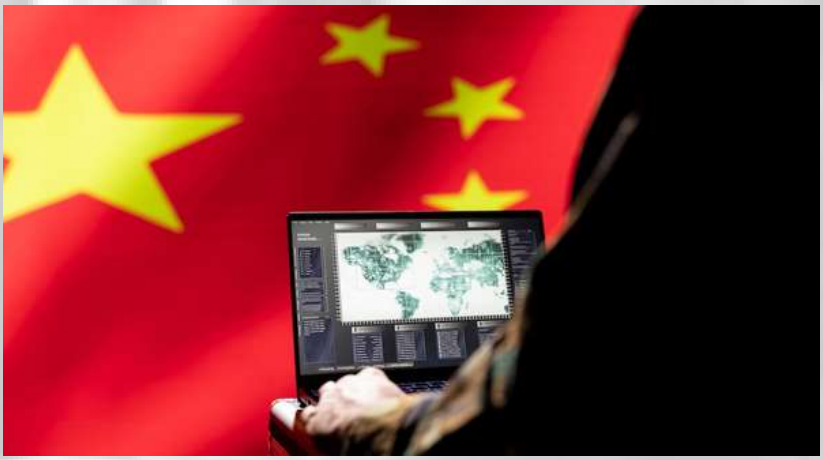


IMAGE SOURCE: PHAYUL

A joint advisory issued on April 9, 2025, by cybersecurity agencies from the UK, US, Australia, Canada, Germany, and New Zealand warns that sophisticated spyware-specifically 'Badbazaar' and 'Moonshine'-is being used to target communities considered a threat to the Chinese Communist Party, including Tibetans, Uyghurs, Taiwanese, and Falun Gong practitioners. These spyware tools, embedded in seemingly legitimate apps tailored to these groups, covertly collect sensitive data such as location, audio, messages, and photos, serving Chinese state interests. The advisory urges at-risk individuals to use only trusted app stores, avoid jailbreaking devices, and remain vigilant, while app stores and developers are given technical mitigation advice. This warning follows a series of reports documenting ongoing Chinese-linked cyber espionage against Tibetan organizations and other dissident groups worldwide - Phayul

RIGHTS CONCERNS TRIGGER FACIAL RECOGNITION REVIEWS IN PARAGUAY, BALKANS AND HUNGARY

IMAGE SOURCE: BIOMETRIC UPDATE

The article highlights growing rights concerns over the deployment of facial recognition technology in Paraguay, the Balkans, and Hungary. In Paraguay, a report by TEDIC reveals that since 2018, the national police have significantly expanded the use of facial recognition cameras without an adequate legal framework, raising serious issues around privacy, data security, lack of transparency, and potential corruption. The technology's use is criticized for exposing citizens to mass surveillance and discrimination, with calls for robust data protection laws and oversight. Similar concerns are raised in the Balkans, where biometric surveillance is reportedly being used to stifle dissent, and in Hungary, where the EU is reviewing plans to use facial recognition at Pride parades for compliance with strict AI and privacy laws. Across these regions, the article underscores the tension between public security and the protection of civil liberties in the face of expanding invasive surveillance technologies - biometric update

ITALIAN PRIEST CLOSE TO POPE TOLD HE WAS TARGET OF SURVEILLANCE TOOL USED BY A GOVERNMENT

IMAGE SOURCE: ALESSANDRO SERRANÒ/REX / SHUTTERSTOCK

An Italian priest, Father Mattia Ferrari, closely associated with Pope Francis, has been targeted by sophisticated government-backed surveillance. Ferrari, a chaplain for the migrant rescue vessel Mediterranea Saving Humans, received a notification from Meta in February 2024 that his devices had been compromised by a "sophisticated attack" linked to unidentified government actors. This revelation follows a private meeting between Ferrari, NGO founder Luca Casarini, and activist David Yambio with Pope Francis at the Vatican, where they discussed humanitarian issues. The incident has raised concerns about state-sponsored surveillance and its implications for civil liberties, with opposition leaders demanding accountability from Italy's government, which has denied involvement. The spyware used was developed by Israel-based Paragon, which has since severed ties with Italy - The Guardian

SERBIAN POLICE HACK PROTESTER'S PHONE WITH CELLEBRITE EXPLOIT CHAIN

IMAGE SOURCE: DEJAN KRSMANOVIC VIA ALAMY STOCK PHOTO

Serbian police exploited a Cellebrite exploit chain to hack a protester's phone, raising concerns about surveillance and ethical responsibility. The incident involved tracking dissent using spyware and highlights vulnerabilities in mobile security. It also underscores the need for Cellebrite to address cyber-ethical considerations in its technology deployment - Dark Reading

ITALIAN GOVERNMENT MUST EXPLAIN SPYWARE SURVEILLANCE OF JOURNALIST FRANCESCO CANCELLATO

IMAGE SOURCE: RSF STUDIO

Reporters Without Borders (RSF) is urging the Italian government to investigate and explain the surveillance of Francesco Cancellato, editor-in-chief of FanPage, and several activists, after complaints have multiplied. The Italian government's response has been inconsistent, and RSF is calling for them to identify who was responsible for the attack on press freedom and clarify how and why the spyware Graphite was used within Italy - Reporters Without Borders

GOVERNMENT MONITORING OF IMMIGRANTS' SOCIAL MEDIA

IMAGE SOURCE: BOUNDLESS

Starting in 2025, the White House will require millions of immigrants applying for various benefits, including green cards and citizenship, to provide social media information as part of enhanced screening measures under Executive Order 14161. USCIS will collect social media handles to verify identities, assess security and public safety risks, and detect fraud, potentially affecting over 3.5 million applicants annually. This formalizes and expands social media monitoring, raising concerns about mass surveillance, data storage, and the potential for even naturalized citizens to be subject to ongoing government scrutiny, despite limited legal protections for social media privacy in immigration-related contexts - Boundless

IRAN DEPLOYS DRONES AND SURVEILLANCE IN CRACKDOWN ON WOMEN - UN REPORT

IMAGE SOURCE: VOLANT MEDIA

A UN report reveals Iran is intensifying its crackdown on women, minorities, and activists using drones, facial recognition, and tracking apps to monitor and suppress dissent. The government leverages technology, like the Nazer mobile app, to enforce strict hijab laws, criminalize activism, and expand surveillance beyond its borders, targeting Iranian activists and journalists abroad. The UN's Fact-Finding Mission collected over 38,000 evidence items, reaffirming gross human rights violations and crimes against humanity, and urging the Human Rights Council to support victims and continue investigating these abuses, as well as appointing a new independent body to continue investigating human rights violations in Iran - Volant Media

ESSEX POLICE FORCE DEPLOYS FACIAL RECOGNITION TECHNOLOGY LINKED TO OPPRESSIVE SURVEILLANCE IN GAZA

IMAGE SOURCE: AVISHAY MOHAR / ACTIVESTILLS

The Israeli army, specifically Unit 8200, is developing a ChatGPT-like AI tool trained on millions of Arabic conversations obtained through surveillance of Palestinians in the occupied territories. This Large Language Model (LLM) aims to rapidly process vast quantities of surveillance data to "answer questions" about specific individuals, potentially expanding Israel's incrimination and arrest of Palestinians. Experts warn this constitutes a severe violation of Palestinian rights, enabling population control and raising concerns about accuracy and biases inherent in AI-driven intelligence, potentially leading to wrongful accusations and increased arrests based on vague suspicions - +972 Magazine

NATION-STATE 'PARAGON' SPYWARE INFECTIONS TARGET CIVIL SOCIETY

IMAGE SOURCE: ASCANNIO VIA ALAMY STOCK PHOTO

Paragon Solutions, an Israeli spyware firm founded in 2019, has come under scrutiny for its invasive Graphite spyware, which targets instant messaging apps rather than taking complete control of devices. Citizen Lab's investigation mapped Paragon's infrastructure and revealed deployments in countries like Italy, Canada, and Cyprus. Notably, WhatsApp mitigated a zero-click exploit linked to Paragon and notified over 90 individuals targeted by the spyware, including Italian journalists and activists such as Francesco Cancellato and Luca Casarini. Forensic analysis confirmed infections in WhatsApp and other apps on Android devices, while a related iPhone case showed attempted infection with novel spyware. Amnesty International highlighted the misuse of Graphite against human rights defenders and sea rescue organizations in Italy, emphasizing Europe's growing spyware crisis fueled by lax regulation. These findings underscore the urgent need for stricter oversight of surveillance technologies globally - Dark Reading

UYGHUR LANGUAGE SOFTWARE HIJACKED TO DELIVER MALWARE

IMAGE SOURCE: BELINDA JIAO/SOPA IMAGES/LIGHTROCKET / GETTY IMAGES

In March 2025, senior members of the World Uyghur Congress (WUC) in exile were targeted by a sophisticated spearphishing campaign delivering malware via a trojanized version of a legitimate Uyghur language word processing tool, UyghurEditPP. This malware, designed to remotely surveil victims by collecting system information and enabling further malicious commands, exemplifies China's ongoing digital transnational repression against the Uyghur diaspora. The attackers exploited trusted software to infiltrate and monitor Uyghur activists advocating against human rights abuses in Xinjiang, continuing a pattern of state-backed cyberattacks aimed at silencing and intimidating diaspora communities. The campaign's infrastructure and tactics highlight the persistent and evolving threat faced by Uyghurs abroad - Citizen Lab

TWO SERBIAN JOURNALISTS REPORTEDLY TARGETED WITH PEGASUS SPYWARE

IMAGE SOURCE: VOICE OF AMERICA VIA WIKIMEDIA COMMONS

Two Serbian investigative journalists from the Balkan Investigative Reporting Network (BIRN), Bogdana (not her real name) and Jelena Veljkovic, were targeted with Pegasus spyware, as revealed by Amnesty International. The attack involved suspicious messages sent via Viber from a number linked to Telekom Srbija, containing hyperlinks associated with Pegasus spyware domains. Amnesty's forensic analysis confirmed the use of a one-click infection method, requiring victims to click on malicious links to activate the spyware. This incident marks the third documented Pegasus attack on Serbian civil society in two years, following previous cases targeting activists ahead of national elections. Amnesty International and other organizations have highlighted Serbia's recurring use of invasive surveillance tools against journalists and activists, calling for accountability and stricter regulations to prevent further abuses - The Record

ITALIAN GOVERNMENT APPROVED USE OF SPYWARE ON MEMBERS OF REFUGEE NGO, MPS TOLD

IMAGE SOURCE: THE GUARDIAN; OLMO CALVO / AP

The Italian government has been accused of approving the use of spyware against members of refugee NGOs, raising concerns about surveillance abuse and human rights violations. Activists and journalists linked to Mediterranea Saving Humans and other organizations were reportedly targeted with Paragon's Graphite spyware, capable of extracting sensitive data from mobile devices. This revelation follows broader allegations of invasive surveillance practices in Italy, including targeting human rights defenders and critics of migration policies. Amnesty International and other groups have called for accountability and stricter regulations to prevent further misuse of spyware technologies, emphasizing the need to protect civil society from such invasive measures - The Guardian

INTELLIGENCE AGENCIES

SOUTH AFRICA'S MULTI-AGENCY DIGITAL ID DEAL SPARKS PRIVACY CONCERNS

IMAGE SOURCE: BIOMETRIC UPDATE

South Africa's government recently signed a multiparty agreement to integrate digital ID systems across agencies like SARS and Home Affairs, aiming to streamline services and combat fraud. However, civil society groups warn the move could centralize biometric data access for law enforcement without adequate privacy safeguards. The upgraded Home Affairs verification system (announced March 24, 2025) raises parallel concerns about expanded state access to citizen data - Biometric Update

PROPOSED CYPRUS BILL ALLOWING JOURNALIST SURVEILLANCE SPARKS OUTCRY

IMAGE SOURCE: OCCRP

A proposed bill in Cyprus that would permit surveillance of journalists, including searches of their homes, offices, and electronic devices, has sparked widespread condemnation from press freedom groups, legal experts, and media advocates. Critics argue the draft law, intended to align with the European Media Freedom Act, instead grants excessive powers to state authorities, potentially allowing spyware use and surveillance of journalists' contacts without adequate safeguards. The bill lacks key protections such as requiring restrictions to be justified by overriding public interest and proportionate measures, raising fears it could suppress investigative journalism and source protection. Despite strong opposition and warnings that it threatens democratic principles and press freedom, the government plans to revise but not withdraw the bill, prompting concerns about increased censorship and self-censorship in Cyprus - OCCRP

INCOME TAX BILL: ‘NO WARRANT, NO NOTICE, THIS IS SURVEILLANCE’, CONG SLAMS GOVT ON 'UNRESTRICTED ACCESS' TO EMAILS, SOCIAL MEDIA POSTS

IMAGE SOURCE: BUSINESS TODAY

The recently introduced Income Tax Bill 2025 in India has sparked significant controversy due to its provisions granting tax officials access to citizens' digital and financial spaces. Introduced in Parliament by India's Finance Minister Nirmala Sitharaman on February 13 2025, the bill has been criticized for allowing tax authorities to access emails, social media accounts, bank details, and trading transactions without a warrant or prior notice, solely based on suspicion, therefore arguably potentially turning India into a "surveillance state" - Business Today

REVEALED: ISRAELI MILITARY CREATING CHATGPT-LIKE TOOL USING VAST COLLECTION OF PALESTINIAN SURVEILLANCE DATA

IMAGE SOURCE: THE GUARDIAN; ANGELICA ALZONA/GUARDIAN DESIGN; PHOTOS VIA GETTY IMAGES

Israel's military, particularly Unit 8200, is developing an AI tool similar to ChatGPT by training it on millions of intercepted Arabic conversations from Palestinians. This AI aims to rapidly process surveillance data to gather information about specific individuals, enhancing the military's ability to monitor and control activities in the occupied territories. The use of AI in military operations raises concerns about privacy violations and the weaponization of surveillance technology. Additionally, Israel has been leveraging AI systems from U.S. tech giants like Microsoft and OpenAI to analyze intelligence and surveillance data, which has been criticized for its role in warfare and potential civilian casualties. Microsoft recently faced internal protests over its AI supply to the Israeli military, leading to the dismissal of two engineers who criticized the company's involvement - The Guardian

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

Global Dialogue

Funded by the European Union

We are grateful for the support of our donors!