Global Surveillance of Journalists: A Technical Mapping of Tools, Tactics, and Threats

An investigative study on the technologies and methodologies used to monitor, target, and intimidate members of the press worldwide.

Prepared by
Samar Al Halal
Computer & Communication Engineer | Digital Security & Digital Rights Expert

Revised by
Lukasz Olejnik

Commissioned by
International Federation of Journalists (IFJ)

brave media
SUPPORTING INDEPENDENT MEDIA WORLDWIDE

IFJ International Federation of Journalists

Co-funded by the European Union

Disclaimer: *This publication was co-funded by the European Union. Its contents are the sole responsibility of the International Federation of Journalists and do not necessarily reflect the views of the European Union.*

March 2026

This report aims to shed light on the evolving technological threats facing journalists, and to strengthen collective resilience through technical understanding and practical countermeasure

Executive summary

Over the past decade, digital surveillance targeting journalists has shifted from scattered, state-run monitoring to a full-fledged commercial industry that spans continents.

This study, commissioned by the International Federation of Journalists (IFJ), investigates the technical infrastructure behind this transformation and the human consequences it produces. Drawing on interviews with cybersecurity experts, forensic analysts and journalists from diverse parts of the world, as well as technical documentation and verified investigations between 2021 and 2025, it paints a detailed picture of how the act of reporting has become intertwined with the risk of being watched, tracked or hacked.

The findings show that surveillance against journalists is now industrial in scale. Sophisticated spyware, once reserved for military intelligence – such as Pegasus, Predator and Graphite – has been repackaged as 'lawful intercept' technology and marketed to governments around the world. These tools give their operators the power to penetrate phones and computers silently, reading encrypted conversations, listening through microphones, and extracting data in real time. Pegasus, developed by Israel's NSO Group, and Predator, a product of the European Intellexa alliance, are among the most well-known examples, but they are only part of a broader ecosystem. Surveillance programmes have been deployed against journalists in democracies and authoritarian states alike. The reasons invoked for these actions are often vague, insufficiently substantiated, or not made public.

At the same time, low-cost methods have proliferated. Ordinary phishing emails, fake websites, and 'off-the-shelf' stalkerware now coexist with state-grade spyware, creating a continuum of threats. Telecommunications engineers have been bribed, forced or coerced to provide access to call data[1]; fake cell towers can be used to track reporters[2] during protests; and entire social media profiles have been scraped to build behavioral maps of journalists before any direct attack occurs. The combined result is a new normal in which surveillance is constant, often invisible, and increasingly normalised.

Technically, the ecosystem is layered and global. Spyware vendors exploit vulnerabilities in phones and messaging apps, bypassing encryption entirely by taking control of the device itself. Telecom infrastructure adds another dimension: weaknesses in the SS7 and Diameter protocols make it possible to locate, intercept and clone mobile communications without a trace. Deep Packet Inspection and network-injection systems allow service providers or governments to tamper with web traffic, redirecting users to malware-laden sites or filtering entire categories of information. Forensic tools such as Cellebrite and Oxygen Forensics, commonly used in police work, can clone a seized device within minutes, sometimes before reinstalling spyware to maintain long-term access. Increasingly, the data harvested through these mechanisms is fed into artificial intelligence (AI) dashboards that correlate calls, messages, geolocation data, and online activity –automating surveillance at a scale once unimaginable. In conflict zones, AI systems now fuse telecom and drone feeds to identify and track journalists, blurring the line between observation and physical targeting.[3] [4]

Across the case studies examined, a similar pattern emerges: the convergence of commercial spyware, state intelligence and weak oversight – a lack of transparency, judicial oversight, legislative or parliamentary accountability and/or independent bodies with the power to investigate and audit.

The study shows the vast reach of these operations, and the immense human cost of this technological apparatus.

Most journalists don't realise they have been targeted until a forensic laboratory confirms an infection, often months after the fact, when evidence has decayed. Only a handful of organisations worldwide – including Citizen Lab, Amnesty International's Security Lab and Access Now – have the expertise to perform such analyses, and their resources are stretched thin. This scarcity of technical support leaves journalists in the Global South particularly vulnerable. Many learn about digital security only after an incident, when their sources are already compromised. The sense of exposure produces psychological exhaustion and widespread self-censorship; reporters avoid sensitive topics or drop investigations altogether, undermining public trust in the press and the confidence of crucial sources.

Behind this lies a deeper governance vacuum – a world in which spyware exports are often unregulated, legal, parliamentary and/or independent oversight is absent, and accountability for abuses becomes almost impossible. Even where there is some form of, or attempt at, regulation, oversight is frequently uneven, incomplete or inconsistently enforced across jurisdictions, and these existing mechanisms may be inadequate to prevent abuse or ensure accountability. Meanwhile, digital safety resources for journalists are fragmented, underfunded, and rarely institutionalised within newsrooms.

This research concludes that surveillance of journalists is not a collection of isolated incidents but a systemic infrastructure of control. Counter-measures – such as encrypted messaging, VPNs and secure storage – remain essential but are insufficient without political and legal accountability for the actors who enable these abuses. Defending journalism now requires not only technical resilience but also collective advocacy: demanding transparency in spyware exports and accountability in its use, investing in regional forensic capacity, integrating digital safety training into journalism education, and safeguarding encryption and anonymity as fundamental press freedom rights.

Unless these steps are taken, the ability of journalists to investigate power – and of societies to know the truth – will continue to erode quietly, line by line, byte by byte.

Table of contents

'This publication was co-funded by the European Union. Its contents are the sole responsibility of the IFJ and do not necessarily reflect the views of the European Union'

Introduction: context and goals of the study

'Anna' was covering government corruption as an investigative journalist when her phone began to behave strangely – the battery drained rapidly, messages lagged, and calls dropped mid-sentence. Weeks later, forensic analysis confirmed her worst fear: her device had been infected with Pegasus spyware, the same tool used by intelligence agencies worldwide to infiltrate dissidents' phones. She asked to remain anonymous, fearing renewed targeting. Her story mirrors that of hundreds of journalists across the world – who are silently surveilled not for crimes, but for doing their job.[5]

This study begins from that shared reality: digital surveillance has become one of the most insidious threats to journalism in the 21st century. Once the preserve of sophisticated intelligence operations, it is now a commercially available service – global, profitable, and largely unregulated. The Pegasus Project revelations of 2021[92], which exposed that at least 180 journalists were selected for targeting by Israel's NSO Group, forced the world to confront this systematic and targeted attack on journalists and journalism. Since then, new players – such as Intellexa's Predator and Paragon's Graphite – have expanded the spyware market, offering 'lawful intercept' tools that are routinely turned against reporters.

For journalists, this is not a hypothetical risk. Surveillance compromises source protection, erodes confidentiality, and breeds self-censorship. In multiple interviews conducted for this study, technical experts and digital rights defenders underscored that the threat is now systemic: journalists' devices are part of a contested battleground of exploits, phishing operations, and network injections. Their insights shaped both the methodology and the recommendations of this research. Expert interviewees highlighted the crucial role of education and building local capacity.

The implications for press freedom and democracy are profound. When journalists suspect that every call, message or movement may be watched, they begin to withdraw from investigative reporting. The Reporters Without Borders (RSF) Press Freedom Index 2025 notes that surveillance is now one of the top three threats to journalists' safety worldwide. Yet in many parts of the Global South, technical investigations remain rare; infections are hard to prove, and support for affected journalists is limited.

To address this gap, the International Federation of Journalists (IFJ) commissioned this study to analyse the technical aspects of journalist surveillance – focusing on how these attacks occur, which tools and infrastructures enable them, and what responses are needed. The research was designed to complement parallel work on legal and policy frameworks, forming the technical backbone of IFJ's broader initiative on journalist safety.

The objectives of the study are as follows:

1. Document the digital tools, techniques and surveillance technologies deployed against journalists

2. Identify regional and global patterns in spyware use and digital monitoring

3. Analyse how journalists and media organisations detect, respond to, or mitigate these threats

4. Recommend technical and policy interventions to strengthen protection and accountability

The scope is global, drawing on 10 primary countries – India, Pakistan, Kenya, Italy, Serbia, Brazil, Mexico, El Salvador, Lebanon and Jordan – alongside technical insights from Israel/Palestine and Russia/Belarus. These case studies illustrate a spectrum of contexts, from democratic states experimenting with 'lawful interception' to authoritarian regimes using imported spyware to suppress dissent and control the press.

In this report, 'surveillance' refers to digital or electronic monitoring, including hacking of devices, interception of data or communications, geolocation tracking, and remote exploitation through spyware or malware. Physical intimidation, censorship and harassment are discussed only when they directly intersect with these digital tactics.

The urgency of this work stems from a widening asymmetry; the balance of power keeps shifting. Spyware is becoming cheaper, stealthier and easier to deploy, while journalists' access to detection tools and technical expertise remains scarce. As the experts interviewed for this report emphasised, journalists are unable to fight back. Without sustained investment in education and regional capacity, the press will remain reactive rather than resilient. This report seeks to change that, offering both a technical map of the threat landscape and a practical roadmap for protection.

The intended readership includes journalists, media institutions, digital rights organisations and policymakers. It is written in accessible language while maintaining technical depth for practitioners and researchers in cybersecurity.

Following this introduction, the report goes on to provide a global overview of surveillance tools and tactics, a detailed examination of the technical ecosystem, country case studies drawn from multiple regions, and an analysis of challenges and detection gaps. It concludes with recommendations for journalists, media organisations, and policymakers, and is accompanied by an annex of sources and references.

Ultimately, this study aims to expose not only the mechanisms of surveillance but also the resilience of those who continue to report under it. Protecting journalism in the digital age demands more than encryption — it calls for technical understanding and coordination, and the political will to confront the surveillance industry itself.

This report has been published as part of the Brave Media project – a global project supporting independent media and public interest journalism.

Public interest media play a vital role in democracy and development – yet in 2025, press freedom reached a historic low, with conditions for journalism now rated "difficult" or worse in more than half the world's countries, amid intensifying political, legal and economic pressure. Across countries, journalists face political and security threats, financial strain, rising mis- and disinformation, and a deepening crisis of trust – which together pose an existential threat to independent media and to democracy itself.

Brave Media responds to these by supporting locally-led solutions that help media outlets and networks operate safely, build resilience, and continue delivering trusted information to communities in the face of growing political, financial and digital threats.

The project – co-funded by the European Union – is led by BBC Media Action, working in a consortium with eight other organisations: Arab Reporters for Investigative Journalism (ARIJ), Equal Rights and Independent Media (ERIM), the International Federation of Journalists (IFJ), Fondation Hirondelle, the Media Institute of Southern Africa (MISA), the Samir Kassir Foundation, SembraMedia, and the World Association of News Publishers (WAN-IFRA).

Methodology: research design, tools and sources

This study adopts a qualitative, multi-method research design combining in-depth expert interviews, case study analysis, and extensive desk research. The goal was to document how journalists are targeted by digital surveillance technologies and to map both the technical and human factors that enable or resist these operations.

Research approach

The research approach integrated three complementary strands:

1. Interviews with digital and security technical and journalistic experts
2. In-depth analysis of documented surveillance incidents
3. Secondary research using technical and NGO data sources

This ensured both qualitative depth and empirical verification. The study focused primarily on the technical aspects of surveillance rather than legal frameworks, filling a crucial gap in understanding how these attacks are executed.

Interviews conducted

Between August and September 2025, nine interviews were conducted with digital security experts, forensic analysts and journalists (interview questions are listed in the annex section).

Interviewees included three cybersecurity experts: one affiliated with a global digital rights organisation with a particular focus on the Middle East; one with expertise in southwest Asia and North Africa digital security and cyber weapons; and one from a non-profit focused on digital technology and information with expertise in Latin American cybersecurity. Their insights included: reported widespread use of data to target individuals, including journalists, specifically in Israel's war in Gaza; shifts from targeting individuals to mass surveillance using specially designed AI systems; surveillance being carried out using not just elite spyware, but also via insider information and bribery.

Interview questionnaires were designed to ensure consistency while allowing for personal experience and regional context. Themes included device compromise, threat detection, infrastructure vulnerabilities, and the human consequences of surveillance.

Expert testimonies demonstrated both the level of sophistication and the normalisation of surveillance practices, from high-end spyware to systemic data exploitation.

Data collection tools and technical sources

The study combined secure data collection practices with triangulation of trusted forensic and investigative sources:

- **Encrypted communications:** all interviews were conducted via Signal, with transcripts stored

securely on local drives

- **Verification sources:** findings were cross-checked against Amnesty International's Security Lab, Citizen Lab and Access Now
- **Spyware intelligence:** OSINT and technical indicators were drawn from the Pegasus Project, the Predator Files, TechCrunch SS7 tracking investigations, and Privacy International's archives
- **Case validation:** Incidents from RSF, the IFJ and SMEX were reviewed to identify technical overlaps across countries

Secondary research

More than 70 external sources were reviewed to contextualise the findings. Key references included:

- Citizen Lab investigations into Pegasus, Predator and Graphite spyware
- Access Now's Digital Security Helpline case analyses
- Privacy International and Amnesty International Security Lab reports on network interception and lawful access systems
- IPI and Freedom House publications on media freedom and digital repression

This combination of sources provided both empirical validation and geopolitical framing for understanding the evolving surveillance ecosystem.

Timeline and outputs

The research was conducted between July and October 2025. It directly informed the:

- global overview of surveillance tools and tactics
- technical ecosystem of spyware vendors and attack vectors
- country and regional case studies
- recommendations framework for journalists, media institutions and policymakers

Supporting materials – including the interview guide – are listed in the annex.

Global overview of surveillance tools and tactics

Journalists around the world are increasingly targeted by sophisticated surveillance systems that were once reserved for state intelligence agencies. The spread of commercial spyware, weaknesses in global telecommunications, and the exploitation of human vulnerabilities have converged to create a hostile environment for press freedom worldwide. One of the most well-known examples is NSO Group's Pegasus spyware, which a 2021 investigation found on the devices of at least 180 journalists across the globe.[6] [7] [8] Other spyware families such as Predator, Graphite, Hermit, as well as older tools like FinFisher, continue to be deployed against reporters. These implants compromise devices silently: extracting messages, call audio, and photos, and even activating microphones or cameras. They essentially turn a phone or laptop into a 24-hour surveillance device.

Beyond device infection, journalists are exposed to exploits of telecom infrastructure. Attackers routinely leverage flaws in global signaling systems (SS7/SIGTRAN) to intercept calls and SMS texts or to geolocate phones without any physical access.[9] In parallel, many governments deploy IMSI catchers that masquerade as cell towers, forcing nearby phones to connect through them. This allows identification of a journalist's handset in a crowd and can enable eavesdropping or injection of spyware over the air. Meanwhile, cheaper but pervasive tactics like email phishing, social media 'honey traps', and even off-the-shelf stalkerware are widely used as entry points. Such methods rely on social engineering rather than zero-day exploits, yet remain highly effective – a reminder that sophisticated surveillance often begins with simple deception.

Increasingly, these technical attacks are augmented by open-source intelligence (OSINT) scraping and AI-driven analytics. Governments and private operators harvest journalists' digital footprints – such as social media, public data, and leaked databases – to map their networks and habits. AI-enabled platforms then fuse this data with telecom metadata or hacked device logs to profile entire newsrooms in real time. In conflict zones, such as Gaza and Ukraine, experts warn that such AI-integrated surveillance enables not only monitoring but also physical targeting – for instance by flagging a reporter's location or contacts for military action. In sum, a diverse arsenal of tools and tactics – from zero-click malware to network interception to psychological manipulation – is being used to surveil and intimidate journalists globally. These methods are often invisible to the target and thus extremely difficult to detect or prove, underscoring the urgent challenge this paper addresses.

Technical ecosystem of surveillance tools

The ecosystem of surveillance targeting journalists consists of multiple layers of actors and technologies working in tandem. This section outlines four key layers of that technical ecosystem and how they interconnect.

1. Commercial spyware (zero/one-click spyware)

Pegasus, Predator, and Graphite (Paragon) – 'the 3 Ps' – dominate the commercial spyware market, offering capabilities once found only in state intelligence agencies. These 'premium' spyware suites provide zero-click exploits (remote-code execution tools or exploit chains enabling compromise of a device and control over its functions without requiring any user action), modular implants (malware payloads that can be updated or customised), and sophisticated anti-forensics to avoid detection. Although marketed as lawful intercept tools for fighting crime, their repeated use against journalists and civil society demonstrates systemic abuse of these technologies.

- **Pegasus (NSO Group, Israel)**

According to investigations by the Guardian and the Pegasus Project, NSO Group was established in 2010 in Israel by Shalev Hulio, Omri Lavie, and Niv Carmi – the company's name being an acronym of their first initials.[10] Reports from Citizen Lab and the New York Times detail how Hulio and Lavie pivoted from their previous startup CommuniTake (a remote device management firm) to collaborate with Carmi, a former Mossad operative, to develop Pegasus.[11] Finalised in 2011, this first iteration was designed as a lawful interception tool sold exclusively to government agencies for the unauthorised remote surveillance of mobile devices.[12] Pegasus is perhaps the most infamous spyware, capable of infiltrating both iPhones and Androids without any clicks by the target.[13] It exploits vulnerabilities in widely used communication software, often zero-day vulnerabilities not yet disclosed to the vendor, to remotely install a spyware agent on the phone that can steal messages, call audio and photos, and activate the microphone or camera without the user's knowledge.[14] In 2021, Pegasus was found on the devices of at least 180 journalists across more than 20 countries.[15] The spyware often leveraged zero-click iMessage exploits – for example, the FORCEDENTRY exploit sent a hidden malicious image file via iMessage to instantly compromise an iPhone. Pegasus is licensed exclusively to governments (NSO claims 60 military, intelligence, and law enforcement agencies in 40 countries) and has been linked to surveillance abuses in countries ranging from Mexico to India to Saudi Arabia. Once Pegasus penetrates a device, it establishes a covert connection to a command-and-control server to exfiltrate data in real time, effectively turning the phone into a pocket spy device.

- **Predator (Cytrox/Intellexa, Europe)**

Predator spyware was originally developed by Cytrox, a company founded in 2017 with origins in North Macedonia and affiliated entities registered in Israel and Hungary. Cytrox was later acquired by Intellexa, a Cyprus-registered company owned by Tal Dilian, a former senior officer in Israeli military intelligence with 24 years of service.[6] [16] Predator first came to light when Citizen Lab found it had infected two Egyptian dissidents' phones in 2021.[17] Unlike Pegasus's frequent zero-click attacks, Predator has often been deployed via one-click methods – targets receive a malicious link by SMS, WhatsApp, or email, and a single click triggers a malware installation.[18] Former Egyptian MP Ahmed Eltantawy had his phone

targeted with Predator spyware through SMS/WhatsApp links after he announced plans to run for president.[18] Predator can infect both Android and iOS; Google's Threat Analysis Group uncovered Predator exploits for Chrome and Android in 2021,[19] and in 2023 Citizen Lab uncovered an attempted network injection attack in which Predator was injected into Eltantawy's web traffic by a device inside an ISP – without any clicks.[18] The corporate entities behind Predator operate from various jurisdictions (including North Macedonia, Greece and Ireland) and sell this spyware to governments. Predator's clients include at least sixteen countries in Europe, Asia, and Africa.[20] Technical analysis indicates that Predator has capabilities similar to Pegasus – such as accessing messages, microphones and cameras. It even uses its own sophisticated exploits to maintain persistence on updated phones.[18]

- **Graphite (Paragon Solutions, Israel/US)**

Graphite is a newer player, developed by Paragon Solutions – a startup founded in Israel in 2019 by former Israeli prime minister Ehud Barak and ex-Unit 8200 commander Ehud Schneorson, among others.[21] Paragon markets itself as a more 'responsible' spyware vendor after the NSO scandals.[21] Graphite's design is often described as focusing on extracting data from instant messaging applications, such as WhatsApp. However, achieving this objective in practice may still require deep access to the device. Evidence of Graphite infections, including zero-click exploits delivered via WhatsApp, indicates that the spyware is capable of fully compromising targeted phones. Meta reported in January 2025 that approximately 90 users, including journalists and activists, were notified of such targeting, with subsequent forensic investigations further supporting this attribution.[22] Citizen Lab's 2025 investigation confirmed Graphite infections on both Android and iPhones belonging to journalists in Italy.[23] Paragon, which received backing from US investors, has also secured a $2 million contract with US Immigration and Customs Enforcement (ICE), which is the first known instance of a US law enforcement agency buying such spyware.[20] Graphite employs zero-click techniques similar to Pegasus (WhatsApp had to patch an exploit after Paragon's activity was discovered) and, once deployed, the spyware can access communications on encrypted applications at the endpoint, including message content after decryption. As with Pegasus and Predator, Graphite's operations are covert: the spyware runs an implant on the phone that funnels data out to Paragon's servers. Researchers have mapped suspected Graphite servers on multiple continents, indicating Paragon has a growing customer base in Europe, the Middle East and Asia, as well as in Canada.[21]

How these spyware suites work:

All of 'the 3 Ps' function as end-to-end attack platforms.

- First, an exploit (or exploit chain) is delivered to the target device – either via network injection, a zero-click message, or a malicious one-click link – which leverages one or more vulnerabilities to gain code execution on the phone.
- Upon successful exploitation, a spyware agent (implant) is installed. This agent runs with high privileges, allowing it to surveil the device comprehensively.[16] It can secretly copy call logs, emails, contact lists, and message content from encrypted messaging applications being captured at the endpoint (for example through access to the device interface, stored data, or user activity), as well as being able to activate sensors like the microphone or camera.[14]
- The agent then encrypts and sends the collected data to a remote command-and-control (C2) server operated by the spyware platform, all while attempting to erase forensic traces (for examples, Pegasus now scrubs iPhone logs to disrupt investigators).

These spyware suites are highly adaptable and receive updates from the vendor enabling new exploits as phone manufacturers patch old vulnerabilities. Notably, in 2022 Pegasus operators deployed at least three distinct iOS 15/16 exploit chains (codenamed LATENTIMAGE, FINDMYPWN, PWNYOURHOME) in quick succession, illustrating the constant evolution of such tools. [26] The zero-click nature of many of these attacks means journalists may have no warning. For example, a phone can be penetrated by an invisible iMessage or missed call, with no user interaction at all, making it extremely difficult to detect or prevent.[14] This high-end commercial spyware layer represents the most direct and invasive threat – a successful infection essentially hands over a journalist's digital life to the attacker. As evidenced by the Pegasus Project disclosures, many governments (including authoritarian regimes and some democracies) have been willing to purchase these capabilities despite the backlash.[13] The result is a growing commercial surveillance industry under which journalists cannot safely do their jobs without endangering themselves and their sources.[13]

The forensic response:

When Pegasus was first exposed, researchers sought to make its inner workings transparent to the world. In July 2021, Amnesty International's Security Lab published its *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, a landmark investigation that detailed how the spyware leaves traces on iOS and Android devices. Alongside this report, Amnesty released an open-source detection tool, the mobile verification toolkit (MVT), allowing journalists, NGOs and forensic experts to scan phones for signs of infection using known indicators of compromise (IOCs).

The MVT represented a breakthrough for civil society: it was the first time a credible, replicable method for confirming Pegasus infections was made publicly available. The toolkit automated complex forensic steps – parsing system logs, scanning backups, and cross-checking domain indicators tied to NSO Group's infrastructure – and quickly became the foundation of digital rights investigations around the world.

Citizen Lab later peer-reviewed Amnesty's methodology, validating its accuracy and confirming infections that had previously only been suspected.

However, transparency came at a cost. By revealing forensic patterns to the public, the report also exposed them to NSO and its clients. Within months, researchers observed that newer Pegasus versions had learned from this scrutiny; erasing log entries, randomising process names, and deploying stronger anti-forensic features designed to defeat tools like the MVT. What was meant as empowerment for defenders inadvertently helped spyware operators refine their stealth.

Since then, no equally public or comprehensive forensic methodology has been released. Detection work continues, but most discoveries now occur quietly within specialised labs, shared privately among trusted researchers rather than published openly. The result is a deepening asymmetry: Pegasus and similar spyware continues to evolve in secrecy, while those defending journalists are left with fewer visible tools to confirm infections. The brief moment of visibility that MVT created underscored both the potential and peril of openness in the surveillance age – knowledge remains our best weapon, but it can also become the adversary's map.

It is important to highlight that, in addition to 'the 3 Ps', several other commercial spyware products offer zero-click or highly intrusive one-click capabilities:

- **Reign (by QuaDream)**
    - **Company:** Israeli firm founded by former NSO employees**Created:** 2016 (operations expanded significantly in 2019)
    - **Founders:** Ilan Dabelstein (former Israeli military official), Guy Geva, and Nimrod Reznik (both former NSO Group employees)[27]
    - **Circumstances:** Born out of the competitive Israeli cyber-intelligence scene, QuaDream was founded by veterans who left NSO Group. Designed to be even more secretive than NSO, operating without a website and under strict non-disclosure agreements. Became notorious for finding a 'screencast' zero-click exploit that bypassed Apple's security via iCloud calendar invites. Reportedly shut down in 2023 after its operations were exposed by Citizen Lab and Microsoft.[28] [29]

- **DevilsTongue (Candiru/Saito Tech)**
    - **Company:** Secretive Israeli firm that primarily targets desktop operating systems (Windows) but has expanded to mobile
    - **Created:** 2014
    - **Founders:** Eran Shorer and Yaakov Weizman
    - **Circumstances:** Candiru (now known as Saito Tech) was founded as a high-end 'mercenary' firm catering to governments that needed to hack Windows computers as well as mobile devices. Received significant early funding from Isaac Zack, an original investor in NSO Group. Known for its extreme 'stealth' business model, it has changed its name multiple times (Grindavik, Taveta, Saito Tech) to evade public and regulatory scrutiny. Blacklisted by the US in 2021 alongside NSO.[30][31]

- **Subzero (by DSIRF)**
    - **Company:** Austrian firm (Decision Software International Research Forum).
    - **Created:** 2016 (spyware branch); parent company active since the mid-2000s
    - **Founders:** Stefan Musil (and associated Austrian investors)
    - **Circumstances:** Based in Vienna, DSIRF presented itself as a risk-analysis and business-intelligence firm. However, Microsoft and security researchers discovered they were selling a sophisticated spyware tool called Subzero. The circumstances of its creation reflect a growing trend of European 'boutique' firms entering the cyber-arms market, offering high-end zero-day exploits (especially for Windows and Adobe software) to a select group of government clients. Microsoft has specifically called out this vendor for providing 'spyware as a service' to government clients.[32]

Note on zero-click availability: Because zero-click exploits (like NSO's FORCEDENTRY) are extremely expensive to develop and fragile (they break when Apple/Google release patches), many of these companies fluctuate between offering true zero-click and one-click capabilities.

2. Everyday surveillance

Not all threats to journalists require such advanced malware. In fact, many reporters are compromised through everyday surveillance tactics that are far cheaper and more common. Journalists are routinely exposed to insider abuses, off-the-shelf spy tools, and social engineering attacks. These methods often precede or accompany higher-end attacks. For example, a phishing email might be used to steal passwords, which attackers then use to read a journalist's communications in the cloud, even without hacking the phone itself. This layer of the ecosystem is characterised by its accessibility – it does not necessarily require nation-state level resources and is widely employed by both government-aligned actors and private figures (as well as abusive spouses and criminals).

Common tactics in this category include:

- **Insider access at telecom/internet providers**

Rather than deploying malware, authorities (or malign actors) can simply buy or coerce their way to accessing a journalist's phone records or internet traffic. For instance, intelligence agencies might have insiders at an ISP or mobile carrier who can pull a target's call logs, locate which cell tower they last connected to, or even provide raw internet traffic data. In countries with weak rule of law, security services have the ability to bypass legal processes and directly request user data from tech and telecom companies, or maintain back-door portals to these systems. Such access can reveal a journalist's contacts, communication patterns and location without any device infection. It's essentially surveillance by flipping a switch on the existing telecom infrastructure. This form of insider surveillance is cheap, leaves no trace on the target's device, and is nearly impossible for the journalist to detect, making it an attractive tool for monitoring. For example, multiple reports indicate that in countries like Mexico and Nigeria, government agencies have obtained mobile phone metadata to track journalists' movements or identify their sources.[33]

- **Commercial stalkerware and DIY spy tools**

A vast market of stalkerware apps and commodity spyware exists, which is often marketed for 'family safety' or 'employee monitoring'. These are far less advanced than Pegasus-type tools but are readily available for a few hundred dollars (or even free) online.
Software like FlexiSpy, mSpy or Hoverwatch can be installed on a target's device – sometimes manually by someone with brief physical access, or through trickery such as convincing the target to install an innocuous-looking app. Once installed, these apps covertly send copies of the phone's SMS texts, call audio, GPS location and other data to the attacker's account. There have been cases of authorities or pro-government actors using such tools against journalists who lack high security on their devices.
In some countries where sophisticated spyware is too expensive or sanctioned, officials also resort to commercial keyloggers or remote access tools to spy on reporters. Even ubiquitous services like Google, iCloud, or WhatsApp web can be abused: if an attacker can obtain a journalist's login credentials via phishing, they might simply log into the journalist's email or messaging account from afar and quietly read private communications (an indirect form of surveillance that achieves the same goal). This 'low-tech' approach is alarmingly common – Amnesty International documented widespread phishing and account hijack attempts against human rights defenders in the Middle East, which often targeted journalists as well.[34] [22] The prevalence of these tools means virtually any journalist could be targeted by someone with

moderate skills, not just state actors.

- **Phishing and social engineering attacks**

Phishing remains one of the most effective entry points for surveillance operations. Journalists receive authentic-looking emails or messages that lure them into clicking a malicious link, downloading a tainted document, or entering their passwords on a fake login page. For example, a journalist might get an email that looks like a Google security alert asking them to re-login – in reality, it's a trap to steal their password. Or they might receive a WhatsApp message with a link claiming to be leaked information; one click could deploy malware (this is known as a one-click exploit). Attackers also create tailored honey traps – such as an attractive person reaching out on social media – to build trust and trick journalists into letting their guard down. These methods exploit human vulnerability more than software flaws. They are 'everyday' in that they do not rely on advanced exploits, yet they can be highly targeted and convincing. A notable example occurred in 2015–2017 when Mexican journalists received SMS messages with personal details (such as their children's names) enticing them to click links which, if clicked, would attempt to infect their phones with Pegasus spyware.[13] Many journalists have learned to be wary of such suspicious links, which is one reason high-end attackers shifted more to zero-click exploits. Nevertheless, even in recent years media organisations have been compromised by well-crafted phishing exercises. For instance, Iranian state hackers have impersonated editors and colleagues to send infected documents to journalists abroad, resulting in device or email accounts being compromised.[35] Social engineering requires little technical infrastructure, making it attractive to a wide range of actors from state security agents to hack-for-hire mercenaries.

Everyday surveillance tactics are generally cheap, scalable, and often serve as the first wave of an attack. They might be used to harvest credentials that are then used to invade accounts, or to perform initial monitoring until a decision is made to deploy more expensive spyware. Critically, these tactics highlight that journalists face a spectrum of threats: not every attacker will burn a million-dollar zero-day exploit on a target if they can simply trick them via email or get an insider to hand over data. For journalists, this means digital hygiene (including strong passwords, two-factor authentication (2FA), and skepticism towards unsolicited links) is as important as patching phones. From an advocacy perspective, the ubiquity of these methods underscores the need for tech companies and regulators to provide better safeguards (such as phishing-resistant authentication or restrictions on stalkerware apps) to protect the press.

3. Signals and infrastructure exploits

This layer of the ecosystem involves surveillance conducted through telecommunications and internet infrastructure, effectively turning the networks on which journalists rely into points of access. These practices fall into two distinct categories:

1. Provider-assisted mechanisms, such as lawful interception systems built into telecom networks

2. More intrusive techniques that rely on protocol weaknesses, manipulation, or deceptive infrastructure, such as SS7 exploitation and IMSI catchers

While lawful interception operates through telecom providers (typically under legal authority, though often with limited transparency or oversight), the latter techniques bypass or manipulate the network itself

without requiring direct cooperation from providers. These methods can intercept communications in transit, track device locations, and in some cases enable the injection of malicious content into network traffic.

One key vector here is the abuse of longstanding flaws in phone routing protocols like Signaling System 7 (SS7). SS7 is an ageing protocol that connects telephone networks worldwide and was never designed with strong security. Surveillance firms such as Circles (a company affiliated with NSO Group) have built systems that connect to SS7 and issue commands to locate phones or intercept communications. With SS7 exploitation an attacker can, for example, trick a network into thinking the target's phone is roaming in their network – allowing them to redirect calls or SMS messages to themselves. This can yield the content of 2FA SMS codes or let them tap voice calls. Citizen Lab found Circles systems in at least 25 countries, sold to government clients who use them to snoop on calls, texts, and phone locations globally without needing any malware on the phone. Because SS7 is still widely used to interconnect mobile networks globally, these attacks are invisible to the target and very difficult to stop; they exploit a trust model from the 1970s that assumed only friendly telecom operators had access. Modern protocols like Diameter (for 4G/5G) have improved security, but many networks still interconnect with SS7, and vulnerabilities persist.[36]

Another technique is to use IMSI catchers (also known as Stingrays or cell-site simulators). These are essentially fake cell towers that broadcast a strong signal to trick all phones in a vicinity into connecting to them. Once a phone connects, the catcher can capture its IMSI (international mobile subscriber identity) and IMEI (device ID), then force the phone's connection down to an insecure 2G channel. This allows eavesdropping on unencrypted calls and texts, and real-time tracking of the phone's location within a few metres. Police and intelligence agencies worldwide use IMSI catchers to locate suspects – and they have been used against journalists and protesters as well. For instance, during protests or around sensitive events, a van equipped with a Stingray may be parked near a press centre to gather the identities of all phones – including those of journalists and activists – in the area.

In one documented case in Belarus, during the mass protests following the 2020 presidential election the authorities deployed these cell-site simulators to sweep the identifiers of every mobile phone in the vicinity of protest zones. The state's security apparatus used these devices to:

- identify participants by gathering the unique IMSI numbers of journalists and protesters present in a specific area
- intercept communications by capturing metadata and, in some cases, the content of unencrypted calls
- escalate the pressure by intercepting journalists' phone calls and airing them on state television as a tactic to intimidate and publicly discredit them [37]

The devices can also intercept metadata and even content if the communication isn't end-to-end encrypted. Because phones will automatically connect to what they perceive as the nearest cell tower, IMSI catchers exploit a fundamental trust in the mobile protocol. There is typically no way for a phone user to tell this is happening – at best, some apps like SnoopSnitch can alert advanced users to anomalies, but even these are not foolproof. [38]

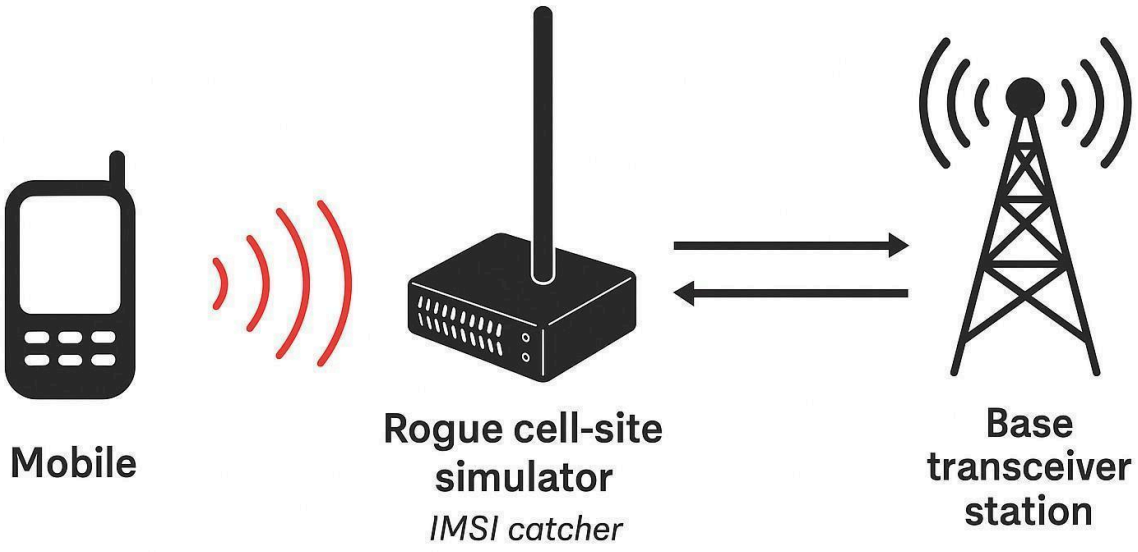


Illustration: Active IMSI catcher (cell-site simulator) — this rogue device impersonates a legitimate cell tower, tricking nearby phones into connecting. Once connected, it can collect identifiers (like IMSI/IMEI) and, in some cases, downgrade encryption from 4G/5G to 2G to intercept calls or messages. Its portability makes it deployable around protests and media offices, or during targeted surveillance campaigns.

In addition, many countries have invested in internet monitoring and injection equipment. Deep Packet Inspection (DPI) systems are deployed at ISP backbones to filter and surveil internet traffic. Authoritarian regimes (and some democracies) purchase DPI tech from companies in China, Europe and the US to integrate into their national networks, often under the guise of cybersecurity or counter-terrorism. These systems can read unencrypted traffic, allowing authorities to see which websites a journalist visits or to block content. More ominously, some DPI equipment can tamper with traffic on the fly. A recent example is the use of network injection attacks in Egypt – in 2023, Citizen Lab found that a device at the edge of a mobile network (Vodafone Egypt) was intercepting web browser requests from a target and redirecting them to a malicious site to silently install Predator spyware. This means that if the journalist tried to visit an http (non-HTTPS) website, the DPI device would hijack that connection and instead send them spyware without any click. It's effectively an invisible man-in-the-middle attack delivered by the ISP. This technique was part of the Predator spyware campaign and shows how the infrastructure layer can directly facilitate device infection.[18]

Another example of network-level surveillance is the use of lawful interception (LI) gateways built into telecom networks. Companies like Nokia, Ericsson, Huawei, and others, provide LI modules in their telecom gear which law enforcement can use (with legal authorisation) to intercept calls and data. However, in many places, this capability is abused with minimal oversight. In Greece, a whistleblower alleged that the national intelligence service abused lawful interception capabilities to monitor journalists. These allegations emerged alongside the separate Predator spyware scandal, in which journalists and other individuals were reportedly targeted. While both cases point to the use of surveillance against media actors, the precise operational links between lawful interception systems and Predator deployments have not been fully established in the public record.

The lack of transparency at the infrastructure level is severe, a journalist's phone could be perfectly

secure, yet their communications might still be intercepted by a secret order at the telecom company or by a rogue device on the network.

In summary, the signals and infrastructure layer shows that even the basic networks journalists use (such as phone networks and ISPs) can be turned into weapons of surveillance. This layer often complements spyware attacks – for example, using SS7 to track a journalist's location and then a Pegasus infection to read their messages, or using an IMSI catcher to identify which phones at a protest belong to journalists and then targeting those phones for hacking. It also enables mass surveillance: whereas spyware is one device at a time, network exploits can passively monitor large swaths of communications. This makes it a go-to instrument of governments looking to monitor not just individuals but entire media offices or populations. The pervasive use of these techniques (often shrouded in secrecy) underscores the need for international pressure on telecom companies and governments to tighten network security and respect privacy. As it stands, a journalist could have the most secure phone on the market and still have their calls listened to or location-tracked via these infrastructure weaknesses.[36]

4. Data fusion, forensics and AI

The final layer of the surveillance ecosystem moves beyond collection into the aggregation and analysis of data. Modern surveillance is not just about hacking a device or intercepting a call in isolation; it's about fusing data from multiple sources (spyware, network logs, open-source intelligence) to build a comprehensive picture of a journalist's life and networks. Authorities increasingly use advanced digital forensics tools and AI-driven analytics platforms to make sense of the deluge of information they collect.

A key component here is the use of forensic extraction devices like Cellebrite UFED and Oxygen Forensics kits. Cellebrite was established in Israel, in 1999, by founders Avi Yablonka, Yaron Baratz, and Yuval Aflalo.[39] Oxygen Forensics was set up in 2000 in Russia by founders Oleg Davydov and Oleg Fedorov, beginning as a consumer utility before evolving into a sophisticated forensic firm. While the company maintains its roots in early mobile data management, its global operations are now spearheaded from its current headquarters in Alexandria, Virginia, under the name Oxygen Forensics, Inc.[40]

These are essentially high-end hacking tools sold to law enforcement for use on seized devices. Cellebrite and Oxygen produce hardware/software that can unlock mobile phones and download all their data, even if the phone is secured with a password or PIN. Police units around the world have these devices in their arsenal, ostensibly to extract evidence from phones with a warrant. However, their use against journalists and dissidents has raised alarms. For example, an Amnesty International investigation in 2024 revealed that Serbian authorities used Cellebrite UFED devices to unlock confiscated phones of journalists and activists, and then implanted spyware on them while they were in custody.[41] Cellebrite's tools can exploit software vulnerabilities to get around phone security, even on up-to-date iPhones or Androids. In Serbia's case, police leveraged a Cellebrite exploit to bypass an Android phone's lock screen, then installed their own spyware (called NoviSpy) to monitor the journalist after he was released. This kind of one-two punch – forensic tool plus custom malware – is a novel tactic enabling physical access attacks.

More commonly, when authorities seize a journalist's device, tools like Cellebrite allow them to entirely clone it, with all messages, contacts, photos and app data extracted for analysis in a matter of minutes. The journalist may never know what was taken. These products are widely sold (Cellebrite boasts thousands of customers in over 150 countries) and, as Amnesty warned, pose enormous risk when used

without strict legal oversight.[42] Authoritarian regimes can essentially perform 'backdoor' hacks without needing NSO-style spyware, simply by misusing forensic kits on confiscated electronics.

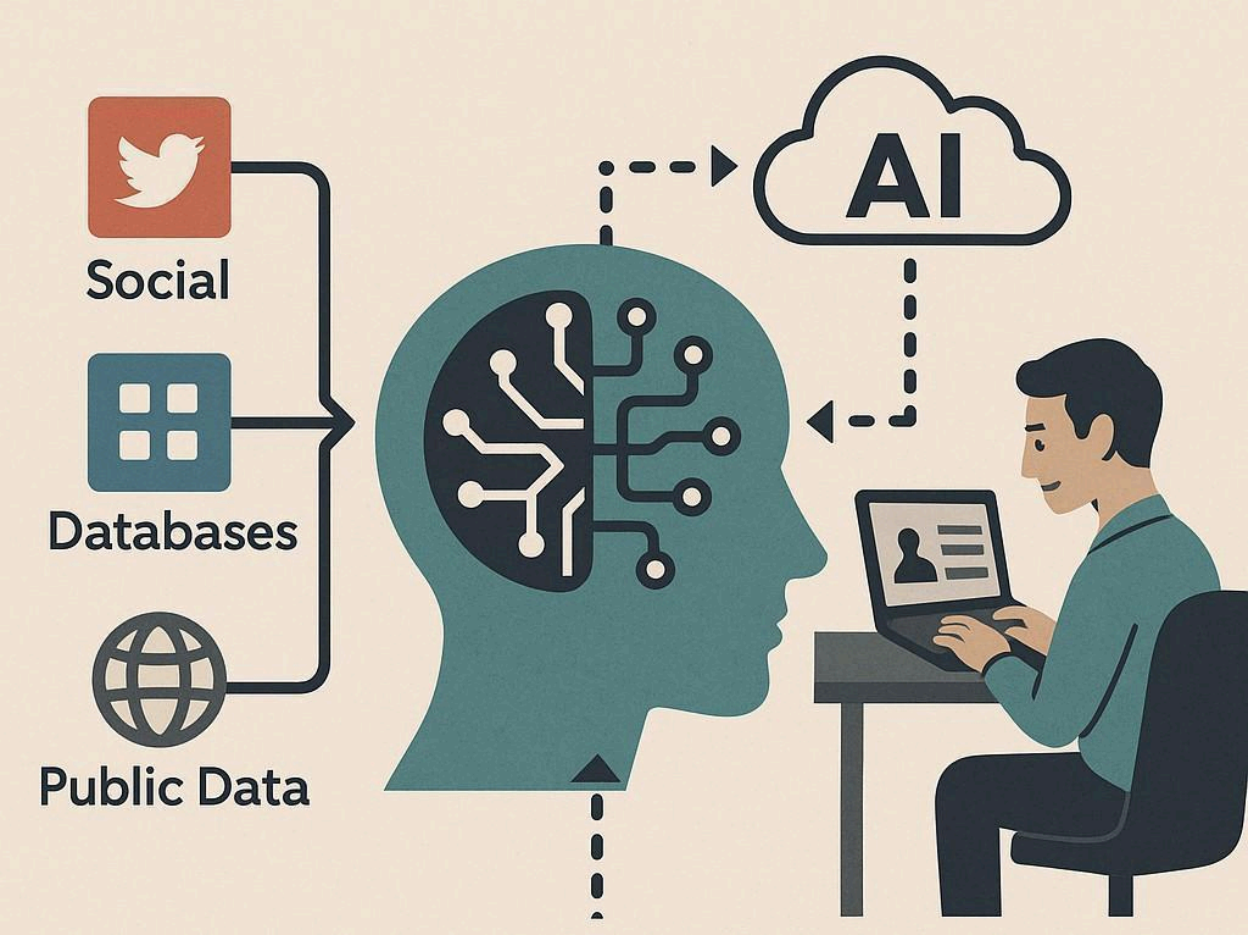
Another example of a surveillance tool that needs physical access is ResidentBat. This Android spyware was discovered in 2024 by Reporters Without Borders (RSF) and RESIDENT.NGO, who linked it to the Belarusian KGB. It was discovered on a journalist's phone after they were questioned by security forces.

The method for putting it on the phone is different from Pegasus, which can infect a device remotely. For ResidentBat to work, the police need to physically hold the phone. In this case, the journalist had to leave his phone in a locker and unlock it while officers watched. RSF believes the officers saw his PIN, took the phone while he was being questioned, and installed the spyware before giving it back.

ResidentBat gives the KGB access to almost everything, including phone calls, microphone recordings, screenshots, and messages from apps like Telegram or WhatsApp. Forensic experts found that this software has been used since at least 2021. After the discovery, Google began sending warnings to other people who were targeted by this government campaign.[43]

Beyond device data, there is the fusion of different data sources. Surveillance agencies now aggregate phone extraction data with telecom metadata, CCTV feeds with facial recognition, travel records, credit card transactions, and social media scraping. Using powerful analytic software – which may be custom-made or commercial platforms like US-based Palantir – they create profiles and social graphs of journalistic networks. In many countries, this has given rise to surveillance hubs or 'centralised analytics platforms' that let security officials query any journalist: this means they can see their calls and messages (from spyware or LI intercepts), view their location history (from SS7 or phone GPS data), and map their contacts (from address books and social media). For instance, in China's Xinjiang region, authorities famously combine phone monitoring with vast databases and AI to flag 'suspicious' behaviour – a model now being quietly adopted in other authoritarian contexts[44].

For journalists, the danger of data fusion is that surveillance is no longer just episodic (a tapped call here, a hacked phone there) but continuous and multilayered. A journalist might evade one form of surveillance only to be caught by another, and all the data ultimately ends up being pooled together. In conflict zones, this fusion becomes literally life-threatening. In Gaza, Israeli military intelligence reportedly uses integrated data – from drone surveillance, cell phone tracking and hacking – to identify and locate individuals in real time, turning surveillance into information that can be used for targeting for airstrikes.[45] In October 2023, Reuters journalist Issam Abdallah was killed by an Israeli tank strike while covering the Lebanon-Israel border. Independent investigations by Reuters, Amnesty International, Human Rights Watch and AFP confirmed that Israeli drones, an Apache helicopter, and five ground surveillance towers had the journalists' position in continuous view for over 75 minutes before the strike, illustrating how layered surveillance assets can establish persistent, real-time awareness of a journalist's location and identity in a conflict environment.[46][7][4] Such scenarios show the terrifying potential of these technologies, when fused. Even outside war zones, the psychological effect is powerful. When journalists know that every aspect of their digital footprint might be correlated, that even if their phone isn't hacked, their movements or contacts might give them away, it creates a climate of fear and self-censorship.



The illustration shows how artificial intelligence aggregates and analyses open-source data – such as social media, public record, and satellite imagery – to identify patterns, networks and risks. It highlights how analysts use these AI insights to monitor information environments, while also underscoring how such systems can be repurposed for surveillance.

From a technical standpoint, this layer relies on data fusion systems that aggregate and correlate multiple streams of information. Governments contract companies to provide lawful intercept monitoring centres and intelligence analytics platforms that ingest data from telecom networks (such as call detail records and location data), surveillance feeds, and device forensic extractions. These systems enable correlation analysis and pattern-of-life analysis which identifies relationships between individuals, maps communication networks, detects co-location events, and tracks behavioural regularities over time. For example, analysts can identify journalists who frequently communicate with specific sources, or determine whether a device was present at a protest based on location data. This shifts surveillance from isolated collection toward continuous analysis of relationships, movements and interactions, which is deeply worrying for press freedom. Reports show that police in places like Vietnam and Egypt use software to monitor the Facebook activities of journalists, while leaks have shown police in India compile network charts of journalists' contacts from seized phones. The technology to do this is often supplied by Western firms – for example, Cellebrite's parent company now markets analytics platforms alongside extraction tools, and companies like Sandvine have offered end-to-end solutions combining interception and analysis. [47] [48] [49] [50] [51]

Accountability at this stage is almost nonexistent. Unlike targeted spyware – about which public exposure sometimes sparks outrage – bulk data fusion happens quietly under broad 'national security' justifications. Few legal safeguards regulate how different streams of personal data can be combined within a country. As a result, even in democratic states investigations have revealed police units mining protesters' social media and phone data across the US and Europe, often with a lack of authorisation, clear oversight or consent.[52] [53] [54] [55] Surveillance-for-hire services also play a role, with some private companies offering spying and analysis as a service to clients. For instance, contractors might break into a journalist's email or cloud accounts and simply hand over the findings to a government, blurring accountability and making attribution more difficult.

This 'surveillance as a service' model means a government can outsource the entire data fusion and analysis process to third parties, who use whatever tools necessary (legal or not) to deliver results. It complicates accountability when abuses are exposed, since agencies can deny using banned tools by claiming a contractor did the work.

In essence, the data fusion and AI layer is about scaling surveillance. It takes the inputs from layers 1–3 and turns them into lasting power over targets. While a spyware infection or an intercepted call is a one-time event, a centralised database containing years of a journalist's communications and an AI system that flags their associations is an ongoing oppression apparatus. Combating this requires not only securing devices, but also advocating for stronger privacy laws, transparency on government surveillance programmes, and limits on how data (especially data on journalists and sources) can be collected and analysed. Without such safeguards, the fear is that any breach of a journalist's digital security doesn't end there; it feeds into a permanent file that can haunt their work and contacts for years. As one expert summarised it, "*surveillance is shifting from targeted hacks to mass profiling on dashboards"* – which poses a systemic threat to the free press.

Country case studies

To illustrate how these tools and tactics play out in practice, this section presents brief case studies from several countries and regions. Each case highlights specific surveillance incidents involving journalists, the methods or vendors implicated, and the local context that enables such abuse. The examples span democracies and authoritarian states alike, demonstrating that no region is immune.

Mexico

Mexico has become a global symbol of journalist surveillance, repeatedly identified in major investigations into Pegasus abuse and broader digital spying against the press.[10] Local digital rights practitioners describe an escalating, multi-layered playbook including: open-source profiling of reporters; telecom-layer access via insiders; physical intimidation and device seizures; and, for high-value targets, commercial spyware such as Pegasus.

The Pegasus operations first documented in Mexico in 2017 targeted journalists and civil society figures with infection attempts delivered by SMS links tied to NSO infrastructure. Citizen Lab documented at least 76 malicious messages sent to reporters, lawyers, and even a minor, often coinciding with investigations into government corruption.[57] Citizen Lab later showed that the *Río Doce* newsroom received Pegasus infection attempts days after the assassination of its cofounder Javier Valdez Cárdenas, with lures referencing the murder. This provides evidence of targeted surveillance against journalists covering organised crime.[58]

Subsequent research confirmed that Pegasus infections continued between 2019 and 2021, despite official denials. Mexican NGO R3D, with technical support from Citizen Lab, forensically identified new cases affecting journalists and a human rights defender during that period.[59] Investigative reporting and NGO documentation have further tied Mexico's armed forces to Pegasus procurement and use, prompting calls for accountability from ARTICLE 19 and partners.[60] In 2024, ARTICLE 19 noted a Mexico City court case related to surveillance of journalist Carmen Aristegui. The court confirmed illegal spyware surveillance occurred, although a defendant was acquitted for lack of direct participation evidence – underscoring both the reality of surveillance and the difficulty of attribution.[61]

The scale and persistence of these operations are also reflected in the international Pegasus Project disclosures (carried out by Forbidden Stories and Amnesty International), which identified Mexico among the countries where large numbers of potential targets – including journalists – appeared in leaked selection data.[62] The overlap between state actors and organised crime amplifies risk and complicates attribution; independent reporting has documented military acquisition and use of spyware as well as targeting activities linked to cartel-coverage contexts.[63]

These dynamics have a chilling effect. Accounts from newsrooms describe heightened caution, device rotation, and reduced electronic communication for sensitive beats – behaviours that are consistent with the threat environment documented by Citizen Lab, ARTICLE 19 and media partners.[58]

Brazil

Brazil's recent experience shows a complex interplay between imported surveillance tech and domestic practices. In 2023-24, Brazilian federal police investigations and court-authorised operations alleged that the intelligence agency ABIN misused a phone-tracking platform known as FirstMile in order to geolocate thousands of devices without judicial orders, reportedly including political opponents and journalists.[64] These probes included arrests of intelligence officials and searches across multiple states, with AP reporting claims (via TV Globo) that the tool may have been utilised tens of thousands of times.[65]

Beyond high-end platforms, Brazilian journalists also face lower-tech but pervasive threats such as targeted phishing, social media impersonation, and device searches or data extraction in criminal probes. These patterns align with broader documentation by press freedom groups about spyware and forensic tools being used against reporters worldwide. While allegations of Pegasus use in Brazil have circulated in the media, publicly-available evidence is thinner on the ground than in some neighboring countries and current, case-level forensic confirmations remain limited in the public domain. Ongoing judicial and parliamentary scrutiny focuses primarily on domestic procurement and misuse of tracking and interception capabilities.[64]

El Salvador

El Salvador endured one of the world's most intensive spyware campaigns against media workers in 2020-21. A joint forensic investigation by Citizen Lab, Access Now, Amnesty International Security Lab, and partners, confirmed 35 Pegasus-infected individuals (37 devices), which were mostly journalists and staff at independent outlets such as *El Faro* and *GatoEncerrado*.[66] The Inter-American Commission on Human Rights (IACHR) and OHCHR publicly expressed concern, underscoring the scale and pattern of abuse.[67]

Citizen Lab's timeline shows repeated compromises through mid-2020 to late-2021, a period that overlapped with escalating pressure on independent media. Technical and advocacy groups documented a significant chilling effect: reporters hardened their operational security and sought outside forensic support because domestic institutions offered no protection.[66]

Lebanon

Lebanon presents a dual-threat surveillance environment for journalists, involving both global spyware and local malware operations.[68] Investigations confirmed that Lama Fakih of Human Rights Watch was hacked multiple times with Pegasus in 2021, and reporting indicates that other Lebanese figures were targeted during the Pegasus Project period.[69] Local outlets have also reported that Radwan Mortada was among those targeted.[68] In parallel, the Dark Caracal campaign (2017-18), attributed to a Lebanon-based unit linked to the General Security agency, used Android malware hidden in spoofed secure-messaging apps to spy on journalists and dissidents.[70] Together these show a blend of imported and indigenous methods. On one hand, commercial spyware like Pegasus has been used against Lebanon-based targets; on the other, globally documented telecom-layer tracking techniques illustrate how phone metadata and location can be exploited.[69] Lebanon's state-controlled telecom

sector (OGERO backbone; government control of Alfa/Touch) further enables potential ISP-level monitoring. During the 2019 waves of protest, multiple journalists and digital right groups reported severe slowdowns and temporary blocking of live-streaming apps. Some experts suspected that these incidents aligned with attempts to manipulate traffic flows for monitoring or injection purposes, though no public forensic confirmation has been released to date.[71]

The killing of Reuters journalist Issam Abdallah on 13 October 2023, near Alma al-Chaab in southern Lebanon, offers one of the most forensically documented illustrations of how layered surveillance assets operate in the moments before lethal force is used. Abdallah and six colleagues from Reuters, AFP and Al Jazeera had been stationary on an open hilltop for at least 75 minutes, all wearing clearly marked 'PRESS' vests and helmets, with their cameras on tripods and their vehicle bearing the same markings on its hood and roof.[72] [74]

During that period, multiple surveillance platforms were continuously active on the group. AFP journalist Dylan Collins, who survived the attack, testified that an overhead Israeli drone circled their position 11 times before the first strike.[15] CyberScoop and Human Rights Watch verified that the journalists were within the direct line of sight of five Israeli ground surveillance towers, that a nearby UAV had its cameras trained on their position, and noted the likely use of infrared targeting or range-finding technology – pointing to active, multi-layered observation throughout. SC Media and Amnesty International independently confirmed that an Israeli Apache helicopter and likely an Israeli drone hovered above the group for more than 40 minutes before the first strike, and that the journalists were in full view of Israeli forces across the border.[72] [73]

A subsequent investigation by the United Nations Interim Force in Lebanon (UNIFIL) found that an Israeli tank killed Abdallah by firing two 120mm rounds at a group of clearly identifiable journalists, in violation of international law.[24] In October 2025, UN Special Rapporteur on extrajudicial executions Morris Tidball-Binz described the attack as "*a premeditated, targeted and double-tapped attack from the Israeli forces*" and a war crime.[25] Collins later reflected: "*The Israelis had drones in the air the entire time. With their state-of-the-art surveillance capabilities, they could see our faces – they probably knew which channels we were working for*."

Finally, Lebanon has served as an operational base for region-spanning cyber operations, as evidenced by Dark Caracal's global victim set.[70]

The three figures below, drawn from the Samir Kassir Foundation's monitoring of press freedom violations in Lebanon, provide broader quantitative context. The most frequently documented violation – interrogation under pressure (23.5%) – routinely involves the confiscation and search of journalists' phones, a direct vector for device-level surveillance and source exposure. Equipment confiscation (20.6%) creates similar risks, while hacking (13.2%) reflects the digital intrusion methods documented throughout this report. Taken together, these figures show that Lebanese journalists face surveillance threats operating across multiple levels simultaneously, from commercial spyware and telecom monitoring, down to physical device seizure during detention.

Figure 1 — Victims of attacks on journalists in Lebanon (Samir Kassir Foundation)

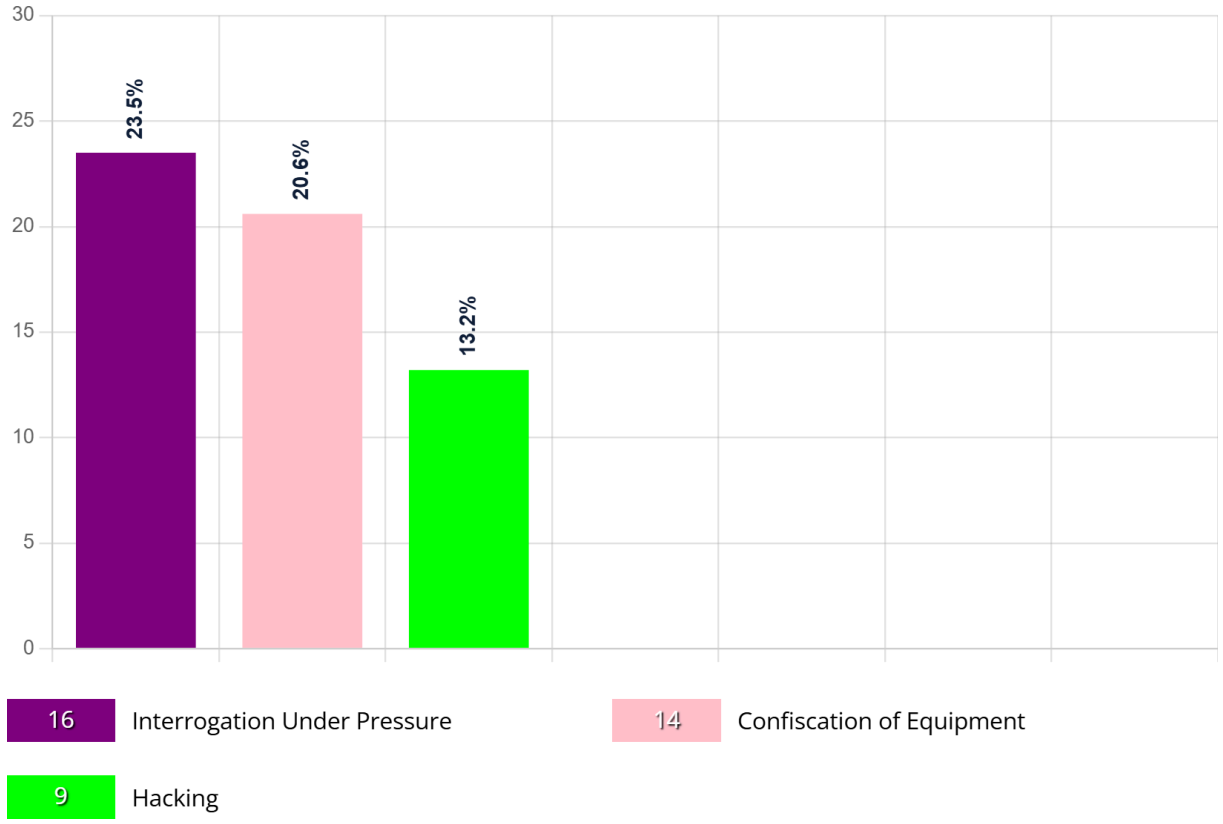


Figure 2 — Nature of violations against journalists in Lebanon (Samir Kassir Foundation)

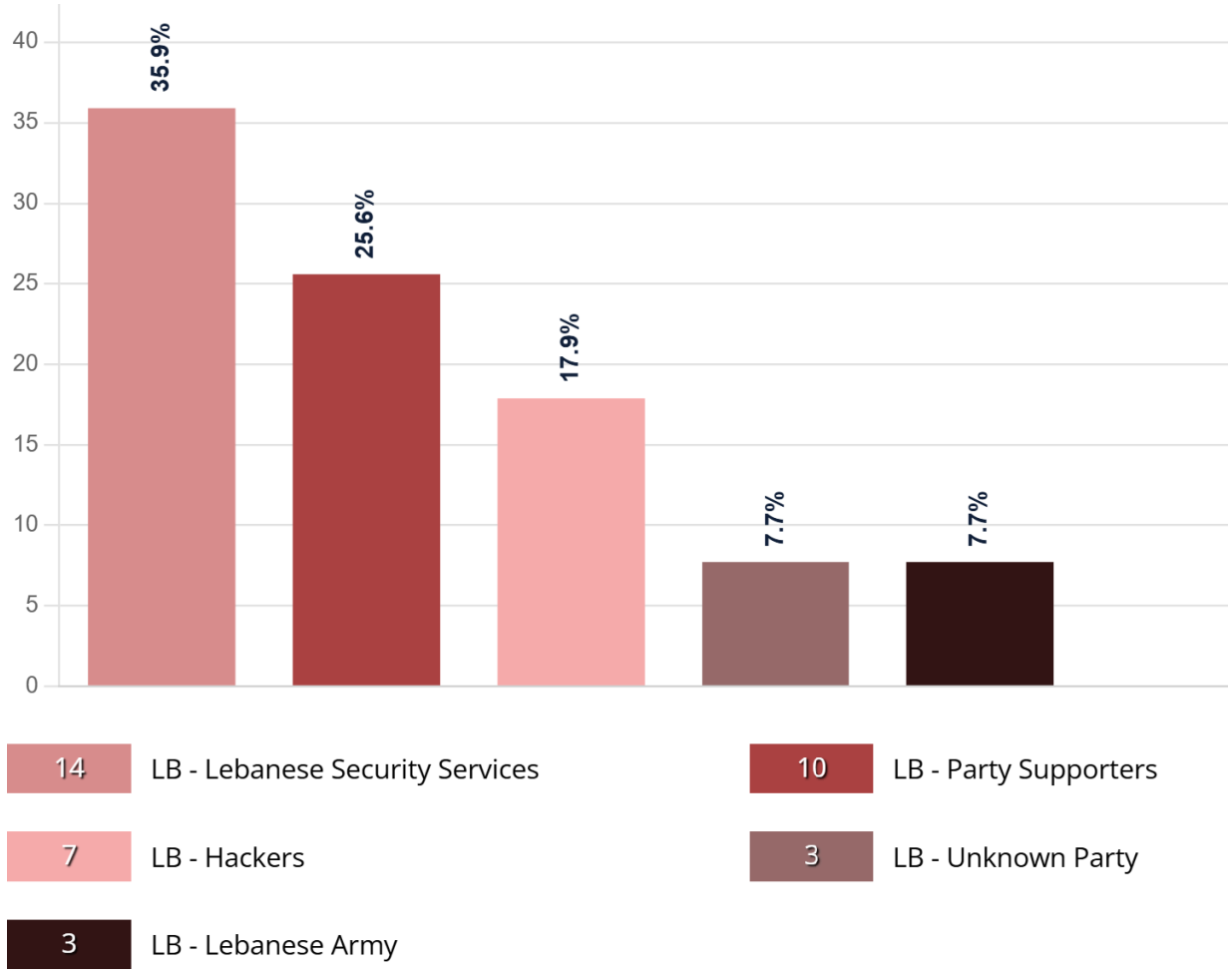


Figure 3 — Perpetrators of violations (Samir Kassir Foundation)

Source: SKeyes Media Website: www.skeyesmedia.org/en/Violations-in-Numbers

Israel / Palestine

Israel is home to several major surveillance vendors, including NSO Group (Pegasus) and other Israeli firms whose tools have been linked to the targeting of journalists and civil society actors worldwide.[74] In parallel, multiple investigations have documented the use of state surveillance systems in the Occupied Palestinian Territories, including facial recognition deployments in the West Bank and the use of integrated population databases to support large-scale monitoring.[76]

In addition to these systems, reporting during the Gaza war has described the use of data-driven target selection tools, often referred to as 'Lavender' and 'Gospel'. These systems are reported to rely on the aggregation and analysis of multiple data streams to identify individuals of interest. While the technical details and operational parameters of these systems are not fully public, they are relevant as examples of how data fusion and large-scale analytics may be applied in conflict settings.[77]

Separately, forensic investigations have confirmed the use of Pegasus spyware against Palestinian human rights defenders, demonstrating that device-level surveillance has been deployed alongside broader monitoring infrastructures prior to the current conflict.[78]

Taken together, these elements illustrate a convergence of surveillance capabilities: device-level intrusion (spyware), population-scale monitoring systems, and data fusion processes that aggregate and analyse multiple sources of information. This combination reflects the broader architecture described in this report, in which different layers of surveillance – device, network, and analytics – can operate in parallel.

Claims that surveillance data is directly used to guide specific military strikes against journalists remain difficult to substantiate through publicly-available technical evidence. While investigative reporting and journalist testimonies have described patterns consistent with targeted monitoring, these accounts are generally based on observed correlation rather than forensic attribution. As such, they should be understood as indicators of perceived risk rather than confirmed technical pathways.

Within this context, reporting by the IFJ highlights the extreme risks faced by media workers in Gaza, where a large number of journalists have been killed since October 2023.[79] Although direct causal links between surveillance systems and individual attacks are rarely established in the public record, the presence of extensive surveillance infrastructures combined with high-intensity military operations underscores how such technologies may shape the overall risk environment for journalists in conflict settings.

Jordan

A collaborative investigation by Front Line Defenders, Citizen Lab, and Amnesty Security Lab confirmed Pegasus infections against Jordanian human rights defenders and journalists – including prominent columnist Suhair Jaradat – with forensic artifacts (SMS/WhatsApp lures and device analysis) between 2019 and 2021.[80]

Freedom House also documents a broader environment of online harassment, surveillance and data requests affecting activists and journalists.[81] Interviews conducted for this study also indicated the use of commercial mobile device extraction tools, such as Cellebrite and Oxygen, when phones are confiscated by authorities.

Serbia

Recent Europe-focused investigations indicate that Serbian journalists and activists have been targeted with spyware and subjected to invasive device forensics. Amnesty International reported in late 2024 on the authorities' unlawful use of spyware and Cellebrite-type forensic extraction tools against civil society actors.[82] In March 2025, Amnesty Security Lab and partner reporting identified two journalists from the Balkan Investigative Reporting network (BIRN) as targets of NSO Group's Pegasus, with technical indicators published. Citizen Lab later issued the first forensic confirmation of the targeting of European journalists using Paragon's Graphite, which highlights the region-wide risk that also touched Serbia's media ecosystem.[83]

Separate Balkan reporting has documented Serbia's procurement/import of IMSI catchers, consistent with protest monitoring allegations raised by local media freedom groups.[84] Overall, Serbia illustrates how EU-adjacent states can combine commercial spyware, on-the-street interception tech, and smear campaigns to pressure investigative reporters.[85]

Italy

In 2025, multiple investigations revealed that Paragon Solutions' Graphite spyware targeted European journalists, including two from *Fanpage.it* – Francesco Cancellato and Ciro Pellegrino – with Citizen Lab providing the first published forensic confirmation of Graphite on iOS.[86] Italian officials acknowledged government acquisition/use of Paragon tooling in certain probes (for example, against NGO figures), while COPASIR scrutiny and media reporting intensified questions about scope and safeguards. Paragon subsequently severed ties with Italy, amid official denials of targeting Fanpage's editor.[87]

Amnesty and press reports frame the Italy episode as part of a wider European spyware crisis, echoing earlier history with the Milan-based Hacking Team (RCS/Galileo) whose 2015 leak exposed global sales to repressive clients.[88] Hacking Team did not disappear after that breach – it was acquired in 2019 and rebranded as Memento Labs, which has continued marketing surveillance tools to government clients. In 2025, Kaspersky researchers confirmed that Memento Labs' new commercial spyware, Dante, had been actively deployed in cyberespionage operations.[96]

India

The Pegasus Project (2021) indicated that numerous Indian journalists were selected as potential targets, and in December 2023 Amnesty Security Lab reported forensic evidence of repeated Pegasus targeting against high-profile journalists, with a companion forensic appendix describing zero-click iMessage exploit traces between August and October 2023.[89] Indian journalists previously received WhatsApp threat notifications in 2019 when a VOIP vulnerability used by NSO was patched, illustrating a pattern that spikes around elections and sensitive investigations (as summarised in regional coverage).[90]

India's government has neither confirmed nor denied Pegasus procurement, with matters raised before the Supreme Court and in parliamentary for a. Historically, researchers and litigants have also documented use/procurement controversies around tools like FinFisher. [89]

Pakistan

Pakistan illustrates a hybrid model that mixes telecom-layer access with commercial spyware. In 2015, civil society litigation in Lahore High Court challenged the government's alleged use of FinFisher/FinSpy, following technical findings that FinFisher infrastructure had operated in-country. Regional advocacy also flagged procurement and use controversies around commercial spyware in the mid-2010s.[91]

Citizen Lab's global mapping (2018) identified Pegasus operators that were active across 45 countries, with Pakistan among the locations of likely operational interest at the time, although public, case-level forensic confirmations remain limited compared with other regions.[92] Given the existence of a powerful security establishment, journalists describe routine assumptions of call/SMS monitoring and widespread phishing/social engineering, consistent with low-cost techniques used alongside any high-end tools.

These practices are extensively documented in regional press-freedom reporting, though Pakistan-specific device forensics are sparse in open sources.

Kenya

Kenya has not seen public, case-level confirmations of Pegasus infections against journalists to date, but investigations show significant communications surveillance capacity building. Privacy International's 2017 report documented the Communications Authority's pursuit of a National Intrusion Detection/Prevention System (NIDS/NIPDS) and broader interception capabilities with implications for elections and civil society.[93] Recent analyses (ICNL, ARTICLE 19) describe social media monitoring, expanding data access powers, and insufficient oversight, which produce a climate of low-grade, persistent risk for reporters and human rights defenders.[94]

Reports from human rights defenders emphasise that, in practice, insider access at telecom companies and lower-tech malware/phishing are often substituted for expensive spyware – an economic calculus that is echoed across the region.[93]

Challenges

The above overview and case studies make it clear that the use of surveillance to target journalists is widespread and highly sophisticated. Addressing this threat faces numerous challenges – technical, institutional and practical. Key challenges in detection, attribution and mitigation include:

1. **Invisible by design**

The most advanced spyware employs zero-click exploits and stealth features that are designed to leave minimal traces on devices and are often difficult to detect without specialised forensic analysis. Network-level attacks via SS7 or IMSI catchers are even harder to notice, as they generate no on-device indicators. This invisibility means a journalist could be surveilled for months, or years, without ever realising it. Standard antivirus or security software often fails to detect nation-state spyware, and indicators like battery drain or strange texts are often too subtle or absent. By the time a compromise is discovered, if ever, the damage – exposure of sources and monitoring of communications – is long done.

2. **Capacity gaps**

The expertise and tools to detect sophisticated intrusions are concentrated in a handful of organisations (including Amnesty International's Security Lab and Citizen Lab) and specialised cybersecurity firms. Most newsrooms, especially in the Global South, do not have the forensic capability to analyse devices for spyware. Journalists in Africa, Latin America and Asia often must physically send their devices abroad or wait for foreign experts to confirm infections. This delay not only prolongs exposure but can result in the loss of volatile evidence. Meanwhile, many journalists lack training in basic digital security hygiene, which could help catch simpler phishing attacks. The disparity between well-resourced attackers and under-resourced defenders is a major obstacle to timely detection and effective response.

3. **Lack of attribution and accountability**

Even when surveillance is detected, pinpointing who is behind it is challenging. Commercial spyware vendors sell identical tools to multiple governments, and those governments rarely admit responsibility. Infrastructure used in attacks (such as servers, domain names and SIM cards) can be rented or spoofed across borders. Additionally, state actors may collaborate with, or outsource to, private hackers and criminal groups. This blurred line makes it difficult to definitively attribute an attack to a particular agency or official. In turn, the lack of clear attribution hinders legal or diplomatic accountability – governments under scrutiny can simply deny involvement or blame 'unknown' actors. The overlapping of state and non-state surveillance in places like Mexico or the Gulf states further complicates this, as journalists cannot easily tell if they are being watched by a government, a cartel, or both.

4. **From targeting to mass profiling**

A fundamental shift is underway from targeting individual journalists to profiling entire media ecosystems. As described, open-source intelligence (OSINT) and data-fusion tools allow authorities to surveil potentially hundreds of people in a journalistic network without necessarily infecting each one. They might only hack a few key phones with spyware (to collect high-value content) but use AI to analyse metadata on all staff, map relationships, and analyse patterns of activity. This mass surveillance approach is harder to detect (there's no obvious incident like a malware alert) and even harder to mitigate, because it doesn't rely on a single point of attack. It erodes journalists' privacy on a broad scale, and traditional defences like secure messaging or device hardening may not protect against being caught in a dragnet of data analysis. In essence, the threat is no longer only 'will I be targeted with malware?' but also "are we all being quietly monitored through our digital exhaust?'
This poses a daunting challenge that current safety protocols barely address.

5. **SIM-tracking and geolocation threats**

The ability to derive a journalist's location from telecom data introduces a distinct challenge that is difficult to mitigate in practice. Even without device compromise, location data can be obtained through network-level access, allowing actors to track movements and infer sensitive activities such as meetings, reporting locations, or source interactions. Unlike content surveillance, which primarily affects confidentiality, geolocation exposure creates risks that extend beyond information access. The challenge lies in the fact that this form of surveillance often leaves no visible trace and does not require interaction with the target, making detection and verification particularly difficult. While the extent to which such data is operationally used in specific incidents is rarely established through publicly-available evidence, the combination of widespread access to telecom data and reports of monitoring in high-risk environments has led journalists to treat location tracking as a credible safety concern.
Mitigation options remain limited. Reducing exposure often conflicts with the operational realities of journalism, which require continuous connectivity. As a result, geolocation tracking represents a persistent vulnerability that cannot be fully addressed through individual security practices.

6. **Too little support, too much surveillance**

The number of journalists potentially targeted or affected by these surveillance tactics far exceeds the capacity of support organisations. A few digital rights NGOs and emergency helplines (such as Access Now's helpline) handle cases globally, but many journalists either don't know where to turn or come forward only after a serious compromise. Resources for digital security training and incident response are concentrated in certain regions and are often grant-dependent. This leads to uneven protection: a journalist in Western Europe who suspects spyware might quickly get assistance from a lab, whereas one in Central Africa or South Asia may have nowhere to obtain a forensic analysis. Moreover, many journalists under surveillance do not report it due to fear, or the normalisation of being watched. The scale of the problem – countless phishing attempts, dozens of spyware operations, mass metadata collection – is outpacing the scale of the response. Bridging this gap requires significantly more investment in journalist cybersecurity, more systematic threat information-sharing, and building local capacity to respond in countries that currently lack it.

7. **Chilling effects and self-censorship**

Finally, pervasive surveillance is undermining journalism itself by instilling fear, uncertainty and mistrust. When reporters suspect their devices are bugged or their calls are being listened to, they may avoid sensitive investigations, drop sources, or choose self-censorship to stay safe. Sources, in turn, become reluctant to talk to journalists if they believe the communication isn't secure – why risk it if the government might know immediately? This erodes the media's ability to serve as a watchdog. In some countries, public awareness of surveillance scandals has also damaged trust in media: audiences might wonder if a journalist has been compromised or fed disinformation via spyware – for example, a hacked phone could send messages a journalist didn't write.

As investigative journalist Szabolcs Panyi, who was targeted by Pegasus in Hungary, put it: "*Who the hell wants to talk to me after this? ... I feel ashamed to not be able to possibly protect some of them.*"[95]

In extreme cases, surveillance enables direct propaganda: eavesdropped private conversations have been edited and aired on state TV in places like Belarus to discredit reporters.

The overall result is a breakdown of the media's role in democracy, with surveillance becoming not just a tool to gather information, but to sow doubt and division. Combating this effect requires not only technical fixes but advocacy and public awareness. Journalists and their allies must continually highlight that surveillance of the press is a threat to the public's right to know, and push for norms and laws that treat it as the grave press freedom violation that it is.

Ultimately, the fight against the surveillance of journalists is an unending race – one in which those defending free expression must keep adapting faster than those trying to silence it. While technical defences (such as encryption, secure devices and threat intelligence-sharing) are crucial, they must be paired with strong legal protections, accountability for spyware vendors and abusers, and support networks for journalists at risk.

The following section provides recommendations that can inform collective efforts to mitigate the threat of technical surveillance and uphold the safety of journalists worldwide.

Recommendations

Introduction

Building on the findings of this study, it is clear that the surveillance of journalists is not an isolated phenomenon but part of a growing and increasingly global infrastructure of digital repression. The following recommendations propose concrete steps for journalists, media organisations, digital security support groups and policymakers. They are divided into two pillars: technical measures, aimed at strengthening immediate defences and resilience; and policy measures, aimed at achieving accountability, regulation, and long-term protection of press freedom. Together, they seek to close the gap between awareness and action, ensuring journalists can continue to report freely, securely, and without fear of digital intrusion.

1. Technical recommendations

For journalists

Journalists are often the first and most frequent targets of digital surveillance. As several experts interviewed for this study emphasised, technical self-defence cannot eliminate all risks, but it can significantly reduce exposure. The recommendations below combine globally recognised best practices with field-tested insights gathered during interviews with digital security specialists in Latin America, the Middle East and Europe.

Device hardening and encryption
Experts consistently recommended using hardware and operating systems designed with security in mind. The preferred devices include Apple iPhones with 'lockdown mode' enabled, or Google Pixel phones running GrapheneOS, both of which offer advanced sandboxing and exploit isolation. For laptops, enabling full-disk encryption is essential (FileVault for macOS, LUKS for Linux, BitLocker for Windows). Sensitive files should be stored in encrypted containers using tools such as VeraCrypt, and encrypted sparse disk images or sparsebundles (created via Disk Utility) on macOS, ensuring that even if a device is compromised the most critical data remains inaccessible.

When travelling or covering high-risk assignments, journalists should use loaner devices – in other words, phones or laptops configured only for that trip – and avoid logging into personal accounts. A strong alphanumeric passcode of at least six characters, rather than a numeric PIN, provides significantly better protection against forced entry at checkpoints, while RFID blockers or 'airplane mode' can block remote access during detentions or border crossings.

Secure communications
End-to-end encrypted platforms remain the backbone of safe communication. Interviewees repeatedly stressed the need to prioritise Signal for instant messaging and calls. WhatsApp can be acceptable for lower-risk exchanges but should not be trusted for highly sensitive communications due to its metadata collection. For email and file exchange, ProtonMail was identified as a reliable option offering zero-knowledge encryption. For communications of the highest sensitivity, secure instant messengers or in-person exchange are more appropriate than email. Email should be limited to medium-security needs.

A VPN can protect communications from local interception on untrusted networks but should not be relied upon to conceal identity or location; most VPNs still log metadata and can be compelled to cooperate with authorities. Self-hosted options such as Algo are an option. Experts emphasised that VPNs are a protective layer, not an anonymity tool.

Operational security (OpSec)

Surveillance frequently exploits human behaviour rather than technology. Experts recommended building disciplined habits such as the following:

- Rotate all passwords and keys after any detention or border inspection
- Minimise the storage of sensitive data on devices; use external encrypted drives for long-term archiving
- Assume every network, airport Wi-Fi, or shared computer is compromised
- Use clean phones with limited apps, disable cloud backups, and avoid automatic synchronisation with personal accounts, when reporting from hostile environments
- Avoid leaving devices unattended in untrusted environments
- Ensure hardware is not left powered on and unattended for extended periods in such settings

Regular risk assessments should become part of the workflow. Journalists should identify potential adversaries, likely vectors of attack (such as phishing, physical access or network interception), and the sensitivity of the materials they handle. This assessment determines the level of security measures required – not all threats are equal, and over-securing can hinder reporting if not balanced with usability.

Trusted points of contact and support

Every journalist should have at least one trusted technical point of contact (PoC) for emergencies. Experts interviewed cited organisations like SocialTIC, Article 19, Access Now, Amnesty International's Security Lab, and Citizen Lab as critical allies for incident triage and escalation. Establishing relationships with these groups *before* an incident occurs ensures faster response and more effective containment when surveillance is suspected.

Capacity building and education

The single most consistent message across all interviews is that education is the cornerstone of resilience. Building regional capacity enables journalists, editors and local technologists to 'speak the same language' as adversaries who wield advanced surveillance tools. Without technical education, journalists remain perpetually reactive. Training must therefore be institutionalised: every newsroom and journalist association should embed digital security modules into professional development programmes, focusing on real-world threats and hands-on defences.

Digital security is not a one-time workshop – it is an evolving skillset. Experts underscored that

continuous learning and mentorship are the only sustainable defences in an environment where the threat landscape changes weekly.

Monitoring and forensic awareness
Learn to identify potential signs of compromise – such as unusual battery drain, high data use, or unexpected app behavior – and document them securely. If you suspect spyware infection, do not reset your phone or update immediately (it could erase forensic traces). Instead, isolate it from networks and contact specialised organisations such as Citizen Lab, Access Now's Digital Security Helpline, or Amnesty's Security Lab.

Psychological and peer support
Surveillance creates trauma and isolation. Journalists should build peer-to-peer support networks, such as those facilitated by the IFJ or NGOs to share threat information and prevent silence or burnout.

For newsrooms and media organisations

Newsrooms play a crucial role in institutionalising safety, creating systems that protect journalists and preserve evidence when surveillance occurs.

Institutional security policy
Establish mandatory digital security protocols, including 2FA for all staff accounts, encrypted email systems, and enforced software updates. Adopt a clear device policy – for instance, journalists working on high-risk stories should use organisation-issued encrypted devices rather than personal ones.

Secure infrastructure and investment
Ensure there is a budget for cybersecurity. Hire or consult IT-security specialists to perform regular security audits, penetration tests and monitoring of newsroom networks. Provide journalists with secure, paid VPN services, encrypted file-sharing platforms, and protected backups.

Training and culture
Conduct annual digital security workshops, tailored to your context. Simulate phishing attempts internally to build awareness and test response. Encourage a non-punitive culture: journalists must feel safe when reporting suspected compromises without fear of being blamed.

Incident response and forensic readiness
Prepare an incident response protocol so that every staff member knows what to do if surveillance is suspected – who to contact, how to preserve data, and how to continue to work safely. Partner with digital security NGOs or forensic labs in advance. Maintain 'loaner' devices for emergencies so journalists can immediately switch to safe hardware.

Advocacy and solidarity
When attacks occur, publicise them responsibly and demand accountability. Silence benefits perpetrators. Join regional or international coalitions (such as the IFJ's Global Platform for the Safety of Journalists) to coordinate responses and pressure governments to disclose surveillance practices.

For digital security NGOs and support networks

Capacity building
Expand regional forensic capabilities in the Global South. Few organisations currently have the equipment or expertise to detect spyware, leaving many journalists without recourse. Support initiatives like the Amnesty Mobile Verification Toolkit (MVT) – which, while not sufficient on its own, can often be a useful forensic support tool –and train local technologists to use it.

Rapid response coordination
Create shared databases of known indicators of compromise (IOCs), infection vectors, and emerging spyware variants. Develop a global incident-reporting clearing house under neutral stewardship so that infections can be correlated and publicly attributed more rapidly.

Awareness and outreach
Translate technical information into accessible resources for non-technical journalists – including infographics, short videos and checklists. Encourage universities and media associations to integrate digital safety training into journalism curricula.

2. Policy and governance recommendations

While technical practices protect individuals, systemic change requires legal, diplomatic, and industry reform. Governments and international institutions must recognise surveillance of journalists as a direct attack on press freedom. While some regulatory and norm-setting initiatives already exist – for example the Pall Mall initiative – existing measures remain partial, uneven, or insufficiently enforced. These recommendations go further in calling for stricter restraint on the export, sale, and use of invasive spyware.

- **Regulate or ban spyware:** Call for an immediate moratorium on the export, sale, and use of invasive spyware technologies until clear human rights safeguards are implemented. Support efforts that govern surveillance technology exports, and advocate for its strict enforcement.

- **Strengthen legal protections for journalists:** Adopt and enforce shield laws protecting journalistic sources and communications in the digital domain. Establish independent oversight bodies empowered to audit and investigate government surveillance activities. Any use of spyware should require judicial authorisation and transparent reporting to parliament or the public.

- **Defend encryption and secure communications:** Governments should reject legislation mandating encryption ‘back doors’, which weaken protection for everyone, and instead fund research on open-source secure communication. The UN Human Rights Council and the Freedom Online Coalition already recognise encryption as essential to free expression – member states should align their policies accordingly.

- **Promote international accountability:** Support the creation of a UN Special Rapporteur mechanism that is dedicated to surveillance technology and human rights, and empowered to investigate global spyware abuse. Endorse initiatives under the Global Digital Compact to

establish global norms on lawful surveillance and privacy. Encourage coordination through the OECD and Council of Europe to sanction companies and governments involved in unlawful journalist surveillance.

- **Ensure transparency and redress:** Require governments to publish annual transparency reports detailing the number and scope of surveillance authorisations. Victims of illegal surveillance, including journalists, must have access to legal remedies and compensation. Support ongoing lawsuits and investigations into companies like NSO Group and Intellexa through the European Data Protection Board and UN Human Rights mechanisms.

Conclusion – a call to action

Protecting journalists from digital surveillance is no longer a technical or regional issue – it is a global democratic imperative. This study demonstrates that without decisive action, the same tools designed for national security will continue to be turned against those who hold power to account.

The IFJ and its partners urge media organisations, governments, funders and technologists to move from awareness to implementation: to invest in protective infrastructure, to legislate on transparency and oversight, and to build a culture where surveillance is not normalised but condemned.

Freedom of the press depends on the freedom to communicate securely.

Each unprotected journalist weakens collective truth.

Each secured newsroom strengthens democracy.

Annex: references and resources

Interview questionnaire

For journalists

- From your experience, what are the most common types of surveillance journalists are facing right now?
- Are you seeing state-sponsored tools, criminal actors, or both?
- Has surveillance increased since recent political/military events (eg wars, elections)?
- Have you or your colleagues experienced phone or laptop compromise?
- Did you notice suspicious signs (fast battery drain, unusual processes, notifications)?
- Has any forensic analysis been done? If yes, where and what tools were identified (Pegasus, Predator, FinFisher)?
- How were these infections delivered? (phishing links, fake apps, zero-click exploits)
- Have you been subject to phishing through email, WhatsApp, or social media?
- Are journalists facing account takeovers or suspicious 2FA resets?
- Have devices been seized at checkpoints, borders, or during protests?
- Did you receive direct threats to install apps or share passwords?
- Has surveillance been combined with physical attacks or arrests?
- What tools or strategies do journalists currently use for digital security?
- Do they use Signal, VPNs, password managers, any other security tool? If yes, do they feel confident using them?
- What's missing? Training? Easier tools? Awareness?
- Are organizations supporting journalists who are facing surveillance? If yes, how? and what is missing?
- If you could request one anti-surveillance resource, what would it be?

For security experts

- From your experience, what are the most common types of surveillance journalists are facing right now in your region?
- Are you seeing state-sponsored tools, criminal actors, or both?
- Has surveillance increased since recent political/military events (eg wars, elections)?
- Have you or your colleagues analysed compromised phones or laptops?
- Which spyware families did you identify (Pegasus, Predator, FinFisher, Candiru, etc.)?
- What specific indicators of compromise (IoCs) did you see (domains, processes, file paths) Did you observe zero-click exploits or social-engineering delivery?
- How long did infections persist before detection?
- Have you seen evidence of ISP-level interception or deep packet inspection?
- Were telecom providers compromised or collaborating with state actors?
- Have there been internet shutdowns or suspicious network anomalies linked to surveillance?
- Did you trace any C2 (command & control) servers or infrastructure linked to known vendors?
- Do you see overlaps in infrastructure across countries (eg same Pegasus clusters in multiple regions)?

- Do you see patterns in phishing or account takeovers targeting journalists?
- How do you typically detect these infections (e.g. MVT from Amnesty, sandboxing, manual log review)?
- Which tools/approaches work best for journalists with low technical capacity?
- Have you seen any new or emerging surveillance toolkits beyond the well-known ones?
- Which anti-surveillance tools (Signal, VPNs, sandboxing) are effective in your view?
- What gaps remain in journalist protection from a technical standpoint?
- If you could recommend ONE resource for journalists, what would it be?

Key international organisations' work concerning surveillance of journalists

- **Amnesty International Security Lab – spyware investigations (2021–2025):** Forensic reports and case studies confirming spyware attacks on civil society (such as the Pegasus Project and Predator Files). Amnesty's analyses have been pivotal in uncovering Pegasus infections and Intellexa/Predator operations. securitylab.amnesty.org

- **Citizen Lab – investigations of Pegasus, Circles, Graphite:** Groundbreaking research by the Citizen Lab (University of Toronto) on commercial spyware, surveillance-for-hire and telecom exploits. Notable reports include the 2021 Pegasus Project collaboration, *Running in Circles*, on SS7/telecom spying, and the 2025 confirmation of Paragon's Graphite spyware use against journalists. africanarguments.org and ap.orgap.org

- **Access Now Digital Security Helpline:** Frontline support service providing 24/7 technical assistance to journalists and human rights defenders facing digital threats. Access Now has helped investigate cases like El Salvador's Pegasus hacks and offers guidance on emergency responses for at-risk journalists. citizenlab.ca

- **Masaar's *Impact of Online Surveillance on Press Freedom* (2024):** Research paper by the Egyptian digital rights group Masaar, detailing how surveillance undermines investigative journalism and source confidentiality, with regional examples such as the targeting of Jordan's Suhair Jaradat with Pegasus. masaar.net

- **Freedom Online Coalition – *Guiding Principles on Government Use of Surveillance Technologies* (2023):** A set of voluntary principles endorsed by 36 countries to prevent the misuse of digital surveillance tools and uphold human rights. These principles urge transparency, rule of law, and proportionality in state surveillance – a framework that civil society can use to hold governments accountable. freedomonlinecoalition.com

- **Privacy International & partners – Africa surveillance reports:** Investigations by Privacy International, CIPESA, Paradigm Initiative and others into surveillance practices in African countries. Paradigm Initiative's *State of Surveillance in Africa* (2024) outlines how spyware and interception tech from global vendors are proliferating in West Africa, and CIPESA's 2023 brief, *How Enhanced State Surveillance is Hurting Digital Rights in Africa*, documents the impact on journalists and activists. paradigmhq.org and cipesa.org

- **TechCrunch – SS7 tracking exploit exposé (2025):** News report on a Middle Eastern surveillance vendor caught exploiting a new SS7 vulnerability to geolocate phones to within a few hundred metres. techcrunch.com

- **SMEX (Social Media Exchange) – MENA surveillance reporting:** Lebanon-based digital rights organisation SMEX has published reports mapping the surveillance landscape in the Middle East. A 2016 report detailed Lebanon's extensive digital monitoring capabilities and ongoing articles cover regional spyware use, legal gaps, and digital safety tips for journalists in Arabic-speaking countries. smex.org

- **Selected case documentation:**
  - **Project Torogoz** report on Pegasus in El Salvador citizenlab.ca
  - **Reuters investigations** on Brazil's FirstMile surveillance scandal reuters.com
  - **Associated Press** coverage of Paragon Graphite targeting European journalists ap.org

Glossary

2FA (two-factor authentication)
A login protection that requires two proofs of identity (a password plus a code or security key). It blocks most simple account takeovers.

AI (artificial intelligence)
Software that learns patterns from data. In surveillance, it can correlate phone logs, locations and social media to map networks or flag targets.

Air-gapped
A device or network that is physically isolated from the internet to prevent remote compromise.

Amnesty International Security Lab
A research team that performs forensic analysis of devices to detect advanced spyware and develops tools like the Mobile Verification Toolkit (MVT) and publishes security guides.

ARTICLE 19
An NGO focused on freedom of expression and information. Documents violations affecting journalists and media and advocates for improved regulation/legislation.

Big-data analytics
Software that ingests large volumes of data (such as telecom metadata, device dumps, open source intelligence) to find patterns and relationships.

C2 / command-and-control server
A remote server that sends instructions to spyware on an infected device and receives exfiltrated data.

Candiru (now called Saito Tech)
An Israeli commercial-spyware vendor implicated in targeting journalists and activists. Known for stealthy Windows and mobile exploits.

Cell-site simulator (see IMSI catcher)
A fake cell tower used to trick nearby phones into connecting so operators can identify, track, or intercept them.

Cellebrite (UFED)
A widely used forensic toolset that can unlock and clone phones when seized, enabling access to data for analysis (and abuse if oversight is weak).

Citizen Lab
A University of Toronto research group that investigates targeted digital threats against civil society, including Pegasus, Predator and Graphite.

Circles
A surveillance vendor (affiliated historically with NSO) that sells systems exploiting SS7 signaling to locate devices and intercept SMS/calls at the network core.

VeraCrypt
Tools that create encrypted containers/folders so sensitive files remain unreadable even if a device or cloud account is accessed.

Dark Caracal
A Lebanon-linked Android spyware campaign that used trojanized apps to monitor journalists and activists worldwide.

Diameter
A newer mobile core signaling protocol used in 4G/5G. More secure than SS7 but can still be misconfigured or bridged to SS7.

DPI (deep packet inspection)
Network equipment that inspects internet traffic content/headers to monitor, filter, throttle, or inject code (for example, for spyware delivery).

Exploit/exploit chain
Code that abuses a software flaw to gain control of a device. A chain links multiple flaws to bypass defences and escalate privileges.

Faraday bag/pouch
A shielded sleeve that blocks radio signals so a phone can't send/receive (useful during detention or device seizure).

FinFisher/FinSpy
A government-grade spyware suite (now defunct) once used globally to infect computers and phones of journalists and activists.

GrapheneOS
A hardened Android for Google Pixel phones that improves security against exploits and data exfiltration.

Graphite (Paragon Solutions)
A zero-click spyware platform reported to target journalists on iOS/Android – marketed as 'lawful access' but repeatedly found in civil society abuse.

Honey trap
A social engineering lure that uses a fake persona/relationship to gain trust and compromise a target.

Hacking Team/RCS (Galileo)
An Italian vendor (defunct) whose Remote Control System malware was sold widely and used against journalists before a 2015 leak.

IA/LI (lawful intercept/intercept access)
Built-in telecom capabilities for legal interception of calls/data. Abused where oversight is weak.

IACHR/OHCHR
Inter-American Commission on Human Rights/Office of the United Nations High Commissioner for Human Rights – document and respond to human rights abuses, including surveillance of journalists.

IFJ (International Federation of Journalists)
The world's largest journalists' organisation. Commissioned this study to inform training, advocacy and protection.

IMEI/IMSI
Unique identifiers: IMEI for the handset; IMSI for the SIM/subscriber. IMSI-catchers harvest these to identify/track phones.

IMSI-catcher
Often called 'Stingrays', these devices act as fake base stations (towers) that force phones to connect, exposing IMSI numbers, location, and sometimes calls or messages so operators can identify, locate, and sometimes intercept or inject. Can be a portable device (often van-mounted).

Indicators of Compromise (IoCs)
Forensic breadcrumbs – domains, files, logs – that suggest infection or attempted intrusion.

Intellexa/Cytrox (Predator)
A surveillance alliance and vendor behind Predator spyware, linked to one-click and network-injection infections of civil society activists' and journalists' devices.

Lockdown mode (iOS)
An Apple feature that disables risky services and tightens parsing to reduce the iPhone's attack surface against zero-click exploits.

Man-in-the-Middle (MitM)
Intercepting traffic between a device and a server (for example, via rogue Wi-Fi, DPI gear) to read/alter it or inject malware.

Malware-laden site
A malicious website that specifically delivers or installs harmful software on a user's device.

Memento Labs
The rebranded successor to Italy's Hacking Team, acquired in 2019 following the latter's reputational collapse after a massive 2015 data breach that exposed its global sales of surveillance tools to repressive governments.

Metadata
Data about data (such as who contacted whom, when, where). Even without message content, metadata can reveal networks and patterns.

MVT (Mobile Verification Toolkit)

Open-source toolkit (developed by Amnesty Tech) to scan phones for signs of advanced spyware infection.

Network injection
Tampering with a victim's web traffic (often at ISP level) to silently redirect them to malware – no click needed if traffic is unencrypted.

NSO Group/Pegasus
A leading commercial spyware vendor and its flagship tool, capable of zero-click iOS/Android infections delivering full device access.

Oxygen Forensics
Sells forensic software used by police/authorities to extract and analyse data from seized devices.

OSINT (open-source intelligence)
Collecting and analysing publicly-available information (social media, leaks, public records) to map targets and craft attacks.

Persistence (malware)
Techniques that help spyware survive reboots or updates – for example, by re-installing itself or hiding within system processes.

Phishing/spear-phishing
Deceptive messages or sites used to steal credentials or deliver malware. 'Spear-phishing' is highly targeted and personalised.

Predator
A commercial spyware platform (Cytrox/Intellexa) often delivered by one-click links or through network injection. Enables full device access once installed.

Proton (mail/drive/pass/VPN)
A suite of privacy tools (end-to-end encrypted email, file storage, password manager, VPN) used by high-risk users.

RSF (Reporters Without Borders)
An NGO tracking press freedom conditions globally.

Safe city (camera/analytics systems)
Urban surveillance platforms combining CCTV, facial recognition, and analytics for population monitoring.

Sandvine/DPI Vendors
Companies that sell DPI gear enabling filtering, throttling, or injection on ISP networks.

SIM swapping vs. SIM tracking
'Swapping' hijacks the user's number at the carrier to intercept calls/SMS; 'tracking' queries the network for a SIM's location/metadata.

SIGINT (signals intelligence)
Intercepting and analysing electronic signals (cellular, Wi-Fi, satellite). In conflicts, often combined with drones and AI.

SIGTRAN/SS7
Legacy mobile network signalling used to set up calls/SMS/roaming. Weak design lets attackers locate phones or intercept SMS/calls if they gain access.

Source protection
Practices that keep informants safe (secure communications, minimising digital traces, compartmentalising devices).

Stalkerware
Commercial 'monitoring' apps (often abusive partner tools) that can be repurposed to spy on journalists if installed on their phones.

Threat actor
The person or organisation behind an attack (such as a state agency, contractor, criminal group).

Triangulation (cellular)
Estimating a phone's location by measuring its signal to multiple towers.

VPN (virtual private network)
Encrypts internet traffic between a device and a VPN server – useful on untrusted networks, but not an anonymity or location-hiding tool.

Zero-click exploit
A compromise that requires no action by the victim (for example, an invisible message triggers a flaw in iMessage or WhatsApp).

Zero-day (0-day)
A previously unknown software flaw. Attackers exploit it before the vendor can release a patch.

References

"1." *Huawei Staff Help Governments to Spy on People: WSJ Investigation,* YouTube, 14 August 2019

https://www.youtube.com/watch?v=_Fk7LV_IcXc

"2." *How to Catch an IMSI Catcher,* Open Technology Fund, 23 February 2024

https://www.opentech.fund/news/how-to-catch-an-imsi-catcher/

"3." *'Lavender': The AI machine directing Israel's bombing spree in Gaza***,** +972 Magazine, 3 April 2024

https://www.972mag.com/lavender-ai-israeli-army-gaza/

"4." *Questions and Answers. Israeli Military's Use of Digital Tools in Gaza,* Human Rights Watch, 10 September 2024

https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza

"5." *Spyware Pegasus helped target over 180 journalists, global report reveals*, IFJ

https://www.ifj.org/media-centre/news/detail/article/spyware-pegasus-helped-target-over-180-journalists-global-report-reveals

"6." *The most notorious instances of commercial spyware,* Kaspersky Daily, March 2024

https://www.kaspersky.co.in/blog/commercial-spyware/27208/

"7." *Case study: The Pegasus Project*, Security Lab

https://securitylab.amnesty.org/case-study-the-pegasus-project/#:~:text=The%20Pegasus%20Project%20was%20a,cases%20of%20Pegasus%20spyware%20attacks

"8." *Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*, Citizen Lab

https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/#:~:text=,Diario%20de%20Hoy%2C%20and%20two

"9." *The seven African governments using Israeli cyberespionage tools*, African Arguments, 23 February 2021

https://africanarguments.org/2021/02/the-seven-african-governments-using-israeli-cyberespionage-tools/"

10." *Revealed: leak uncovers global abuse of cyber-surveillance weapon*

https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber surveillance-weapon-nso-group-pegasus

"11." *The Battle for the World's Most Powerful Cyberweapon (Published 2022)*, 28 January 2022 https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

"12." *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 September 2018 https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

"13." *Private spy software sold by NSO Group found on cellphones worldwide*, The Washington Post, 18 July 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

"14." *What is Pegasus spyware, and how to detect and remove it*, Norton, 13 June 2025 https://us.norton.com/blog/emerging-threats/pegasus-spyware

"15." *Reporters decry lack of accountability on tank shelling in Lebanon that killed Reuters cameraman Issam Abdallah*, National Press Club, https://www.press.org/newsroom/reporters-decry-lack-accountability-tank-shelling-lebanon-killed-reuters-cameraman-issa

"16." *Predator Files: Technical deep-dive into Intellexa Alliance's surveillance products*, Amnesty International Security Lab, 6 October 2023 https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

"17." *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, The Citizen Lab, 16 December 2021 https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware

"18." *PREDATOR IN THE WIRES Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions*, The Citizen Lab

https://citizenlab.ca/research/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

"19." *Multiple zero-day vulnerabilities exploited to deploy Predator Spyware*, Secure Blink

https://www.secureblink.com/cyber-security-news/multiple-zero-day-vulnerabilities-exploited-to-deploy-predator-spyware

"20." *Predator Still Active, with new client and corporate links identified*

https://www.recordedfuture.com/research/predator-still-active-new-links-identified#:~:text=Over%20the%20past%20two%20years,mercenary%20spyware%2C%20such%20as%20Pegasus

"21." *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*, The Citizen Lab, 19 March 2025

https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

"22." *US-backed Israeli company's spyware used to target European journalists, Citizen Lab finds*, The Associated Press, 12 June 2025

https://www.ap.org/news-highlights/spotlights/2025/us-backed-israeli-companys-spyware-used-to-target-european-journalists-citizen-lab-finds/

"24." *RSF and ten organisations call on UN to investigate Israeli attack that killed Issam Abdallah*, Reporters Without Borders,

https://rsf.org/en/lebanon-rsf-and-ten-organizations-call-un-investigate-israeli-attack-killed-issam-abdallah

"25." *UN: Deadly 2023 Israel attack on Reuters, AFP journalists in Lebanon was war crime*, L'Orient Today,

https://today.lorientlejour.com/article/1480650/un-rapporteur-says-deadly-2023-israel-attack-that-wounded-afp-journalists-in-lebanon-was-war-crime.html

"26." *Triple Threat NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*, The Citizen Lab https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/#:~:text=variety%20of%20apps%20and%20features,3%20%28PWNYOURHOME

"27." *Report: Israel nixed QuaDream's spyware deal with Morocco, leading to firm's closure*, Times of Israel https://www.timesofisrael.com/report-israel-nixed-quadreams-spyware-deal-with-morocco-leading-to-firms-closure/

"28." *Journalists, politicians targeted by 'new Israeli spyware'*, TRT World https://www.trtworld.com/article/12797476

"29." *Experts warn of new spyware threat targeting journalists and political figures*, The Guardian https://www.theguardian.com/technology/2023/apr/11/canadian-security-experts-warn-over-spyware-threat-to-rival-pegasus-citizen-lab

"30." *Saito Tech (formerly Candiru)*, Business and Human Rights Centre https://www.business-humanrights.org/en/companies/candiru/

"31." *Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus*, the Citizen Lab https://citizenlab.ca/research/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus

"32." *Austrian Investigation Reveals Spyware Targeting Law Firms, Finance Institutions*, Info Security Magazine https://www.infosecurity-magazine.com/news/austria-spyware-law-firms-finance/

"33." *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*, The Citizen Lab, 1 December 2020 https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

"34." *Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the*

Middle-East and North Africa, Amnesty International https://www.amnesty.org/en/latest/research/2019/08/evolving-phishing-attacks-targeting-journalists-and-human-rights-defenders-from-the-middle-east-and-north-africa/

"35." *Under Attack: How Journalists Can Defend Themselves Against Digital Threats*, KSJ https://ksj.mit.edu/news/2025/06/12/cyber-security-wolfangel

"36." *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*, The Citizen Lab, 1 December 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles.

"37." *Belarus authorities strip accreditation from foreign journalists*, The Guardian, https://www.theguardian.com/world/2020/aug/29/belarus-authorities-strip-accreditation-from-foreign-journalists

"38." *Cell-Site Simulators/ IMSI Catchers*, Street Level Surveillance https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers

"39." *From bootstrapped startup to a $5B powerhouse: Cellebrite's outgoing CEO reflects on 19 years of highs and controversies*, C Tech https://www.calcalistech.com/ctechnews/article/lhck15vtj

"40." *ICE Is Using Phone Extraction Software Linked to Russia's FSB-Connected Network*, Malign Influence Operations, 18 February 2026 https://maligninfluenceoperations.substack.com/p/ice-is-using-phone-extraction-software

"41." *Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists*, Amnesty International, 16 December 2024 https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/

"42." *Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists*, Amnesty International, 16 December 2024 https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic

"43." *Exclusif : RSF met au jour un nouveau logiciel espion utilisé par le KGB biélorusse*, Reporters Sans Frontieres
https://rsf.org/fr/exclusif-rsf-met-au-jour-un-nouveau-logiciel-espion-utilis%C3%A9-par-le-kgb-bi%C3%A9lorusse

"44." China's Surveillance Ecosystem and the Global Spread of Its Tools, Atlantic Council
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/

"45." *'Lavender': The AI machine directing Israel's bombing spree in Gaza*, +972 Magazine, 3 April 2024
https://www.972mag.com/lavender-ai-israeli-army-gaza/

"46." Lebanon: Deadly attack on journalists must be investigated as a war crime, Amnesty International USA
https://www.amnestyusa.org/press-releases/lebanon-deadly-attack-by-israeli-authorities-on-journalists-must-be-investigated-as-a-war-crime/

"47." *Viet Nam: Tech giants complicit in industrial-scale repression*, Amnesty International
https://www.amnesty.org/en/latest/press-release/2020/12/viet-nam-tech-giants-complicit/

"48." *Freedom of the Net 2021 - Egypt*, Freedom House
https://freedomhouse.org/country/egypt/freedom-net/2021

"49." *'Taking away our livelihood': Journalists on phone seizures and harassment by police*, The News Minute
https://www.thenewsminute.com/news/taking-away-our-livelihood-journalists-on-phone-seizures-and-harassment-by-police

"50." Cellebrite Pathfinder | AI-Driven Investigative Link Analysis Software, Cellebrite
https://cellebrite.com/en/pathfinder/

"51." From Sandvine to AppLogic Networks: a rebrand doesn't mean reform, Access Now, 12 February 2026

https://www.accessnow.org/press-release/from-sandvine-to-applogic-networks-a-rebrand-doesnt-mean-reform/

"52." Documents Reveal How DC Police Surveil Social Media Profiles and Protest Activity, Brennan Center for Justice https://www.brennancenter.org/our-work/analysis-opinion/documents-reveal-how-dc-police-surveil-social-media-profiles-and-protest

"53." Amnesty and S.T.O.P. reveal NYPD surveillance-abuses, Amnesty International, 13 November 2025, https://www.amnesty.org/en/latest/news/2025/11/amnesty-and-s-t-o-p-reveal-nypd-surveillance-abuses/

"54." PROTEST SURVEILLANCE INTO COURTS, privacyinternational.org, December 2024 https://privacyinternational.org/sites/default/files/2025-01/Protest-surveillance-into-courts.pdf

"55." Preventing unlawful profiling today and in the future: a guide, Statewatch 2018 https://www.statewatch.org/media/documents/news/2018/dec/eu-fra-preventing-unlawful-profiling-12-18.pdf

"56." *Revealed: leak uncovers global abuse of cyber-surveillance weapon*, The Guardian, 18 July 2021 https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

"57." *Reckless Exploit Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, The Citizen Lab, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso

"58." *Reckless VI Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*, The Citizen Lab https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague

"59." *New Pegasus Spyware Abuses Identified in Mexico*, The Citizen Lab https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico

"60." *Mexico: Army used Pegasus spyware against journalists and activists,* Article 19, 4 October 2022 https://www.article19.org/resources/mexico-army-spyware-journalists-activists/

"61." *Mexico: Investigations into the use of Pegasus spyware must continue*, Article 19 https://www.article19.org/resources/mexico-investigations-into-the-use-of-pegasus-spyware-must-continue/

"62." *Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders*, Amnesty International, 19 July 2021 https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

"63." *Military forces behind new cases of spying on Mexican journalists, reveals 'Ejército Espía' investigation*, LatAm Journalism Review https://latamjournalismreview.org/articles/military-forces-behind-new-cases-of-spying-on-mexican-journalists-reveals-ejercito-espia-investigation/

"64." *Brazil to probe claims of spy agency eavesdropping on cell phones - minister*, Reuters https://www.reuters.com/world/americas/brazil-probe-claims-spy-agency-eavesdropping-cell-phones-minister-2023-03-15/

"65." *Brazil police conduct searches targeting intelligence agency's use of tracking software*, AP News https://apnews.com/article/ef22ef84fb76fa40d44e8bebc6f25f2d

"66." *Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*, Citizen Lab, https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/#:~:text=,Diario%20de%20Hoy%2C%20and%20two

"67." *Identified members of the digital newspaper "El Faro"* INTER-AMERICAN COMMISSION ON HUMAN RIGHTS https://www.oas.org/en/iachr/decisions/mc/2022/res_32-22_mc_1051-20_sv_en.pdf

"68." *The state of Digital Security among Independent Media Organizations In Lebanon*, The Samir Kassir Foundation https://www.skeyesmedia.org/documents/bo_filemanager/The-State-of-Digital-Security-among-Independ

ent-Media-Organizations-in-Lebanon.pdf

-extraction-tools-to-hack-journalists-and-activists/

"69." *Human Rights Watch Among Pegasus Spyware Targets*, Human Rights Watch https://www.hrw.org/news/2022/01/26/human-rights-watch-among-pegasus-spyware-targets

"70." *Dark Caracal Cyber-espionage at a Global Scale*, Lookout chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

"71." *Freedom of the Net 2021 - Lebanon*, Freedom House https://freedomhouse.org/country/lebanon/freedom-net/2021

"72." *Israeli tank fire killed Reuters journalist Issam Abdallah in Lebanon*, Reuters https://www.reuters.com/graphics/ISRAEL-LEBANON/JOURNALIST/akveabxrzvr/

"73." *Lebanon: Deadly Israeli attack on journalists must be investigated as a war crime*, Amnesty International https://www.amnesty.org/en/latest/news/2023/12/lebanon-deadly-israeli-attack-on-journalists-must-be-investigated-as-a-war-crime/

"74." *Israel: Strikes on Journalists in Lebanon Apparently Deliberate*, Human Rights Watch, https://www.hrw.org/news/2023/12/07/israel-strikes-on-journalists-in-lebanon-apparently-deliberate

"75." *Revealed: leak uncovers global abuse of cyber-surveillance weapon*, The Guardian, 18 July 2021 https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

"76." *Israel escalates surveillance of Palestinians with facial recognition program in West Bank*, Washington Post https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

"77." *'The machine did it coldly': Israel used AI to identify 37000 Hamas targets*, The Guardian, 3 April 2024

https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

"78." *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware*, The Citizen Lab

https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

"79." *War in Gaza,* International Federation of Journalists – IFJ

https://www.ifj.org/war-in-gaza

"80." *PEACE THROUGH PEGASUS: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware*, Joint investigation between Front Line Defenders and Citizen Lab

https://www.frontlinedefenders.org/sites/default/files/jordanpegasusreport.pdf

"81." *Jordan: Freedom on the Net 2024*, Freedom House

https://freedomhouse.org/country/jordan/freedom-net/2024

"82." *Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists*, Amnesty, 16 December 2024

https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/

"83." *Serbia: Journalists targeted with Pegasus spyware*, Amnesty International

https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware

"84." *Serbia Imports Wireless Equipment Capable of Indiscriminate Mass Surveillance*, Balkan Insight

https://balkaninsight.com/2024/12/12/serbia-imports-wireless-equipment-capable-of-indiscriminate-mass-surveillance/bi/

"85." *Serbia: A Digital Prison": Surveillance and the suppression of civil society in Serbia: Executive Summary*, Amnesty International

https://www.amnesty.org/en/documents/eur70/8814/2024/en/

"86." *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*, The Citizen Lab, 12 June 2025,

https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journa

lists-targeted/

"87." *Italian government approved use of spyware on members of refugee NGO, MPs told*, The Guardian, 27 March 2025 https://www.theguardian.com/world/2025/mar/27/italian-government-approved-use-of-spyware-on-members-of-refugee-ngo-mps-told

"88." *Italy: New case of journalist targeted with Graphite spyware confirms widespread use of unlawful surveillance*, Amnesty https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/

"89." *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists*, Amnesty, 28 December 2023 https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/

"90." *India targeted high-profile journalists with Pegasus spyware* Al Jazeera, 28 December 2023, https://www.aljazeera.com/news/2023/12/28/india-targeted-high-profile-journalists-with-pegasus-spyware-amnesty

"91." *Pakistan: Civil society demands transparency over revealed spyware purchases*, Business and Human Rights Centre https://www.business-humanrights.org/en/latest-news/pakistan-civil-society-demands-transparency-over-revealed-spyware-purchases/

"92." *HIDE AND SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, The Citizen Lab https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

"93." *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya*, Privacy International

https://www.privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

"94." *Regulation of Digital Surveillance and the Impact on Civil Society in Africa: Experiences from Kenya*, International Center for Not Profit Law

https://www.icnl.org/wp-content/uploads/Kenya-Digital-Surveillance-report-new-cover.pdf

"95." *Szabolcs Panyi: I was hacked with Pegasus software*, Vsquare

https://vsquare.org/szabolcs-panyi-i-was-hacked-with-pegasus-software/

"96." Kaspersky GReAT spot new HackingTeam spyware in the wild after years of silence, Kaspersky

https://www.kaspersky.com/about/press-releases/kaspersky-great-spot-new-hackingteam-spyware-in-the-wild-after-years-of-silence