

PRESS FREEDOM FACT SHEET

SPYWARE AND SURVEILLANCE

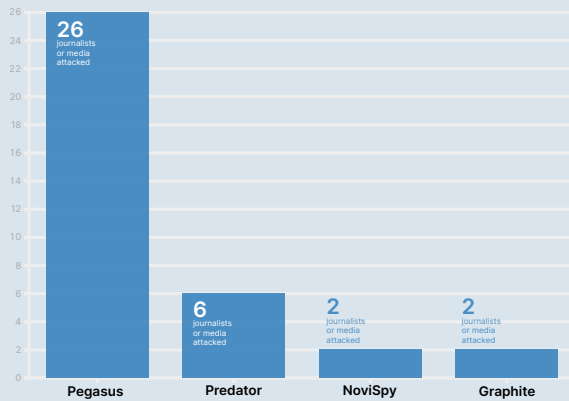


17
CASES OF SPYWARE
REPORTED BETWEEN
1 JANUARY 2020 AND
21 MARCH 2025



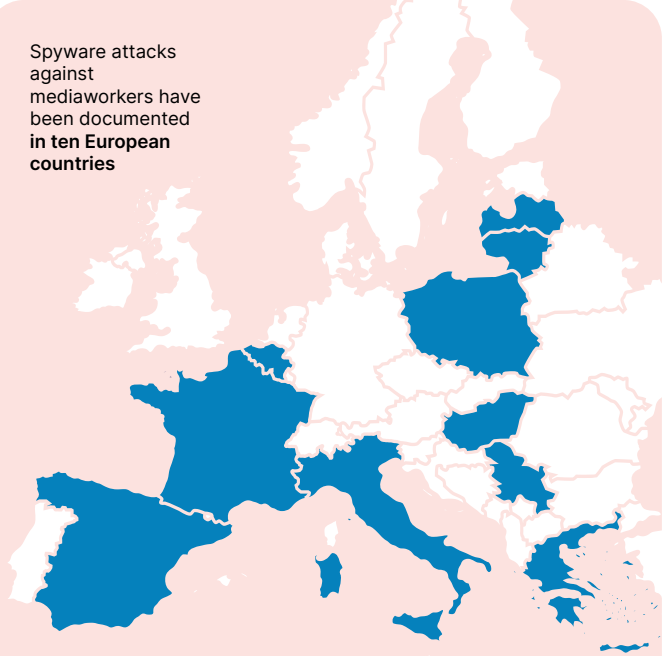
36
MEDIA-RELATED PERSONS
OR ENTITIES ATTACKED
ACROSS THE EU AND
CANDIDATE COUNTRIES

The type of Spyware registered to be used to attack journalists and media were **Pegasus, Predator, NoviSpy, and Graphite**.



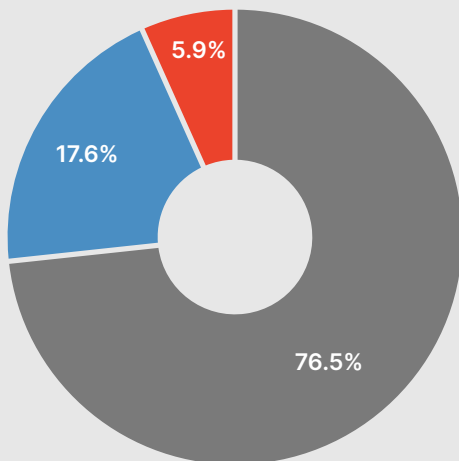
*These are conservative estimates for media-related persons or entities targeted by spyware. For example, at least 90 WhatsApp users have been targeted by the Graphite spyware but only two journalists has publicly come forward thus far.

Spyware attacks against mediaworkers have been documented in **ten European countries**



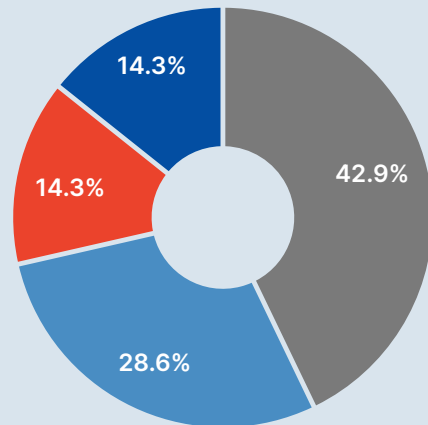
Greece, Hungary, Latvia, Serbia, Spain, Belgium, France, Italy, Lithuania, Poland

In 76.5% of registered cases, the perpetrators behind spyware-attacks remain **unknown**. In 17.6% of cases, mediaworkers were attacked and surveilled by the **government and public officials**. In 5.9% of cases, the perpetrators were **police or state security**.



*Spyware are military grade, dual use software that are primarily sold to and used by government agencies.

MapMF has recorded **7 cases**, where journalists investigating spyware have been targeted by **legal warnings, complaints, investigations or lawsuits**. In total, 19 media-related persons or entities were impacted.



In 42.9% of registered cases the **government or public officials** were the perpetrators, followed by **private individuals** (28.6%), **media regulatory authorities** (14.3%), and **other public authorities** (14.3%).

SPYWARES

Spyware definition: 'Spyware' means any product with digital elements **specially designed** to exploit vulnerabilities in other products that enables **the covert surveillance** of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, **without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent** in that regard.

PEGASUS

Maker: NSO Group

Country of origin: Israel

Journalists targeted in Europe: Peter Verlinden (Belgium), Szabolcs Panyi, András Szabó, Dávid Dercsényi, Dániel Németh (Hungary) Lénéig Bredoux, Edwy Plenel, Dominique Simonnot, Bruno Delpont, Rosa Moussaoui (France), Ignacio Cembrero, Meritxell Bonet, Marcel Mauri, Albano Dante Fachin, Marcela Topor (Spain), Galina Wiktorowna Timchenko, Evgeny Pavlov, Evgeny Erlikh, Maria Epifanova (Latvia), Nataliia Radzina (Poland), Jelena Veljković (Serbia), 5 journalists whose names have not been disclosed.

NSO Group is an Israeli technology company known for developing and selling surveillance software. Its Pegasus spyware is notorious for its capability to infiltrate mobile phones, allowing its clients to monitor communications, track locations, and access data stored on targeted devices. The company is also behind the malware Chrysaor, one of the most dangerous malware samples ever discovered on Android. NSO contracts with governments with a long history of imprisoning, murdering and silencing dissidents, and surveilling civil society organizations. In 2021, the US Commerce Department blacklisted NSO Group, accusing the company of providing spyware to foreign governments that used these tools to maliciously target journalists, embassy workers and activists. In 2023, the Luxembourg-based Dufresne Holdings emerged as NSO's new owner.

Case

On 16 September 2021, the Security Lab Amnesty confirmed that Flemish journalist Peter Verlinden and his wife Marie Bamudese's phones have been targeted by the Pegasus spy software. The 64-year-old freelance journalist, specialised in the topics of Central Africa, colonialism, media and politics, was contacted following an investigation opened by the Service Général du Renseignement et de la Sécurité SGRS (ADIV), the Belgian military secret services. The conclusion of the SGRS's preliminary investigation states that the Pegasus spyware was installed on Verlinden's phone "probably between 22 and 29 September 2020" and on Bamudese's phone between 20 October and 2 November 2020. Suspicion falls on Rwanda, says SGRS and the Rwandan authorities refuted the accusation.

PREDATOR

Maker: Intellexa Consortium

Country of origin: various

Journalists targeted in Europe: Thanasis Koukakis, Alexis Papahela, Yannis Kourtakis, Panos Kyriakopoulos, Antonis Dellatolas, Eva Antonopoulou (Greece)

The Intellexa Consortium is a network of vendors for spyware and surveillance services. The group, with companies in Greece, Ireland, North Macedonia, and Hungary, enables the proliferation of commercial spyware and surveillance technologies worldwide. Through one of its affiliated companies, Intellexa oversees the distribution and support of the Predator spyware service. Predator is designed to infiltrate,

monitor, and extract data from targeted devices. Once installed, Predator enables remote access to monitor the target device, control local microphones and cameras, and extract various forms of data, including files, messages, and location information.

Case

On 28 February 2022, journalist Thanasis Koukakis was informed that his mobile phone was surveilled for at least ten weeks using the spyware Predator, developed by the North Macedonian firm Cytrox. The news was published on 11 April 2022 by the Greek media outlet Inside Story. The surveillance was identified by the Citizen Lab of the University of Toronto, after Koukakis filed an official request to investigate the potential surveillance. Citizen Lab published a three-page report which concluded that Koukakis' phone was infected with the spyware between at least 12 July 2021 and 24 September 2021. The investigation identified the source of the hacking to be a Greek phone number, which sent Koukakis a text message containing an infected link to a fake website. Citizen Lab said it could not confirm whether the spyware was used by the Greek government or a private company.

GRAPHITE

Maker: Paragon Solutions

Country of origin: Israel

Journalists targeted in Europe: Francesco Cancellato, Ciro Pellegrino (Italy)

Paragon is an Israeli company that sells the spyware Graphite. It breaks into encrypted instant messaging communications, guaranteeing extended access to the compromised devices, even when rebooted. Many of the company's staff come from Israel Defense Forces intelligence units. US private equity giant AE Industrial Partners acquired Paragon in December 2024. In January 2025, WhatsApp accused the company of assisting in the deployment of Graphite against nearly 90 targets, which included journalists and civil society members. These individuals were targeted using a "zero-click" attack, which required no user interaction. The Citizen Lab released a technical report of their analysis of the infrastructure used for the targeted mass surveillance operation, including forensic analysis of some of the compromised devices. This report suggested that Paragon's claims of having found an abuse-proof business model by selling to democratic governments only may not hold up to scrutiny, with multiple democracies deploying spyware against journalists, human rights defenders, and other members of civil society.

Case

On 31 January 2025, it was reported that 90 users of social media platform Meta's WhatsApp, including journalists and members of civil society, were targeted with Paragon spyware, also known as Graphite. In the EU, it is understood that individuals were targeted in 13 Member States: Austria, Belgium, Cyprus, Czech Republic, Denmark, Germany, Greece, Latvia, Lithuania, Netherlands, Portugal, Spain, and Sweden. One of the targets was investigative journalist Francesco Cancellato, the editor-in-chief of Italian news outlet Fanpage, who was informed of the spyware attack by WhatsApp on 31 January. The company reportedly discovered that Paragon was targeting its users in December 2024, and had since disrupted the hacking effort. It was unknown how long Cancellato may have been compromised, but the journalist published a high-profile investigative story in May 2024 which exposed how members of Italian Prime Minister Giorgia Meloni's far-right party's youth wing had engaged in fascist chants, Nazi salutes and antisemitic rants. Cancellato reportedly said he did not have reason to suspect that his mobile device had been compromised and that he had never been told by any authorities that he was under investigation. The parliamentary committee that oversees the work of Italian intelligence services (Copasir) published an investigation report in June 2025, denying the involvement of Italian actors in the surveillance of the journalist, while indicating the possibility that foreign services were involved. The authorities have not taken further action, while two court proceedings are ongoing in Rome and Naples. In April 2025, another Fanpage journalist, Ciro Pellegrino, who has been similarly critical of the Meloni government, received a notification by Apple warning that a mercenary spyware was used against him – which was later confirmed to be Graphite.

NOVISPY

Maker: Serbian government

Country: Serbia

Journalists targeted in Europe: Ljubomir Stefanovic, Slaviša Milanov (Serbia)

NoviSpy is a novel domestically-produced Android spyware system, disclosed for the first time in the Amnesty report "A Digital Prison: Surveillance and the suppression of civil society in Serbia". While NoviSpy does not allow unlimited access to all data on the device as does software like Pegasus, according to forensic analysis conducted by the Amnesty Lab, it does gather extremely sensitive private information on its target, which includes the collecting of screenshots of all actions on the phone, tracking the target location, recording from the camera and microphone, and collecting sensitive files.

Case

On 21 February 2024, journalist Slaviša Milanov, who works for the news portal FAR, was arrested. He was questioned on suspicion of transporting wanted persons across the Bulgarian border, which Milanov denied, and also about his work. "When my phone was returned and I turned it on, I noticed that my mobile data and Wi-Fi, which I usually leave on, had been turned off. I installed an application that showed the activity on my phone during the period of my detention, and I contacted Amnesty," Milanov explained. An analysis conducted by Amnesty International's Security Lab revealed that Cellebrite's UFED product was used to secretly unlock Slaviša's phone during his interrogation. Additional forensic evidence also showed that NoviSpy was then used by the Serbian authorities to infect Slaviša's phone.

Additional resources:

[Amnesty International 1 / 2](#)

[Citizen Lab 1 / 2](#)

[Surveillance Watch](#)

[Carnegie Endowment](#)

Disclaimer

The information gathered represents a sample of cases made possible by the painstaking work of journalists, activists and scholars in a context of extreme opacity and lack of cooperation from European states.