© Colin Foo

18 February 2026

Journalism under attack: Predator spyware in Angola

A new investigation by Amnesty International's Security Lab has discovered evidence that the Predator spyware was used in 2024 to target Teixeira Cândido – an Angolan journalist, jurist, press freedom activist, and former Secretary-General of the Syndicate of Angolan Journalists (Sindicato dos Journalists Angolanos). This is the first forensically confirmed case of the Predator spyware being used to target civil society in Angola.

Teixeira Cândido is known for his vocal defense of press freedom and his criticism of government restrictions on journalism. He has repeatedly condemned attacks on journalists and the increasing intimidation against the media, describing these incidents as direct threats to freedom of expression. In December 2022, the Syndicate of Angolan Journalists, at the time led by Teixeira Cândido, organised a national protest condemning attacks on journalists and defending press freedom in Angola.

"I feel naked knowing that I was the target of this invasion of my privacy. I don't know what they have in their possession about my life. [...] Now I only do and say what is essential. I don't trust my devices. I exchange correspondence, but I don't deal with intimate matters on my devices. I feel very limited", said Teixeira Cândido.

Predator is a highly invasive mobile spyware developed and sold by Intellexa – a mercenary spyware company – for use by governments

in surveillance operations. Previous investigations by Amnesty International, Citizen Lab, Recorded Future, among others, have documented human rights abuses tired to the spyware in multiple countries over the past five years. Intellexa has rebranded their spyware products and shifted their corporate structure multiple times during that same period, apparently in response to public exposure of spyware misuses. This publication will refer to Intellexa's flagship spyware product exclusively for mobile as Predator.

This new case of Predator spyware targeting in Angola is the first documented case in the country and one of the most recent confirmed Predator cases, along with the 2025 attack to a human rights lawyer in Pakistan's Balochistan province. Despite repeated public exposure, criminal investigations, and sanctions directed at the company and its senior executives, the research adds further evidence that Intellexa's spyware system remained operational until 2025, in jurisdictions unknown until now. It is not currently possible to conclusively identify the customer responsible for these attack campaigns.

In December 2025, Amnesty International in collaboration with Inside Story, Haaretz and WAV Research Collective published the Intellexa Leaks, which exposed the inner operations of Intellexa and how the company retained the capacity, at least in some cases, to remotely access the systems of Predator customers. The investigation also revealed evidence of Predator abuses in Pakistan, where a human rights lawyer was targeted with spyware in 2025, although it was not possible to conclusively identify the responsible customer.

This new confirmed case emerged from a broader investigation into surveillance threats in Angola, during 2025, originally led by Friends of Angola and Front Line Defenders. Amnesty International is deeply grateful for their pivotal role in the initial research and for their ongoing work to protect civil society in Angola. Amnesty International is also grateful for the support and peer review of the Digital Security Lab (DSL) at Reporters Without Borders (RSF).

The attack

Since 2022, Teixeira Cândido has been subject to multiple attacks and assaults. "At the end of 2022, there was a series of break-ins at our offices with no signs of forced entry. [...] That was when the suspicion of surveillance began. There were also break-ins targeting other journalists, again with no signs of forced entry [...]. We knew we were being watched."

From April to June 2024, in the final months of his ten-year mandate at the Angolan Journalists Union, Teixeira Cândido received a series of WhatsApp messages on his iPhone from an unknown sender who was using an Angolan phone number. The attacker attempted to build trust by claiming to represent a group of young students interested in Angola's socioeconomic development and by setting a familiar Angolan name for their WhatsApp profile.

The conversation between Teixeira Cândido and the attacker began on 29 April 2024. The attacker first sent WhatsApp messages without any malicious links. This was likely another attempt to build trust, as potential targets may become suspicious if they unexpectedly receive links from an unknown contact.

On 3 May 2024, the attacker sent the first malicious link aimed at infecting Teixeira Cândido's phone. Over the coming days and weeks, the attacker proceeded to send more malicious links, each pretending to link to news articles or seemingly innocent websites, as well as numerous follow-up messages to encourage the journalist to open the links (Figures 1, 2 and 3).

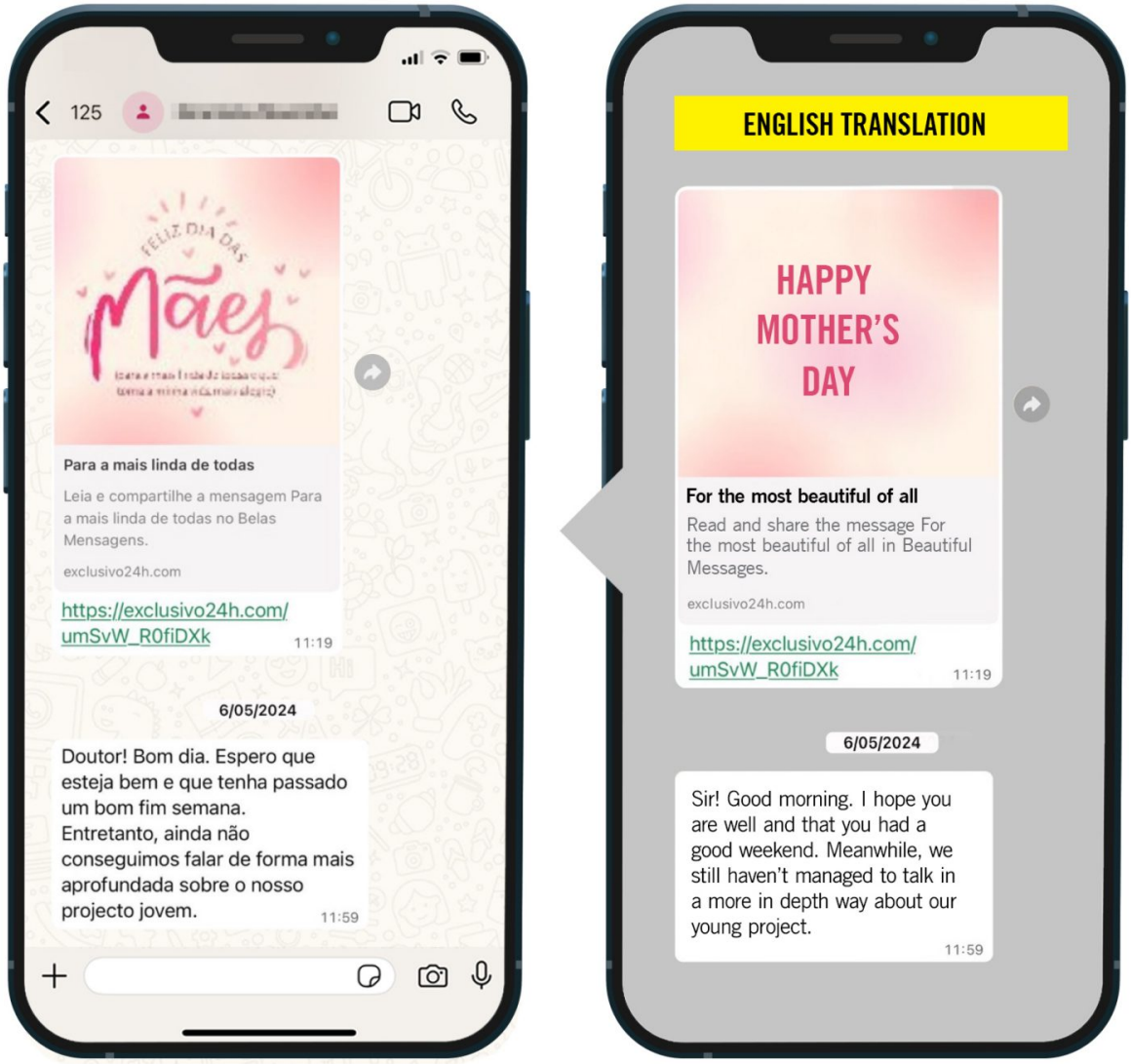

Figure 1: Screenshot of Whatsapp messages sent to Teixeira Cândido, containing malicious links, with the sender's name blurred. The original messages in Portuguese are in the left, and the translations to English in the right.

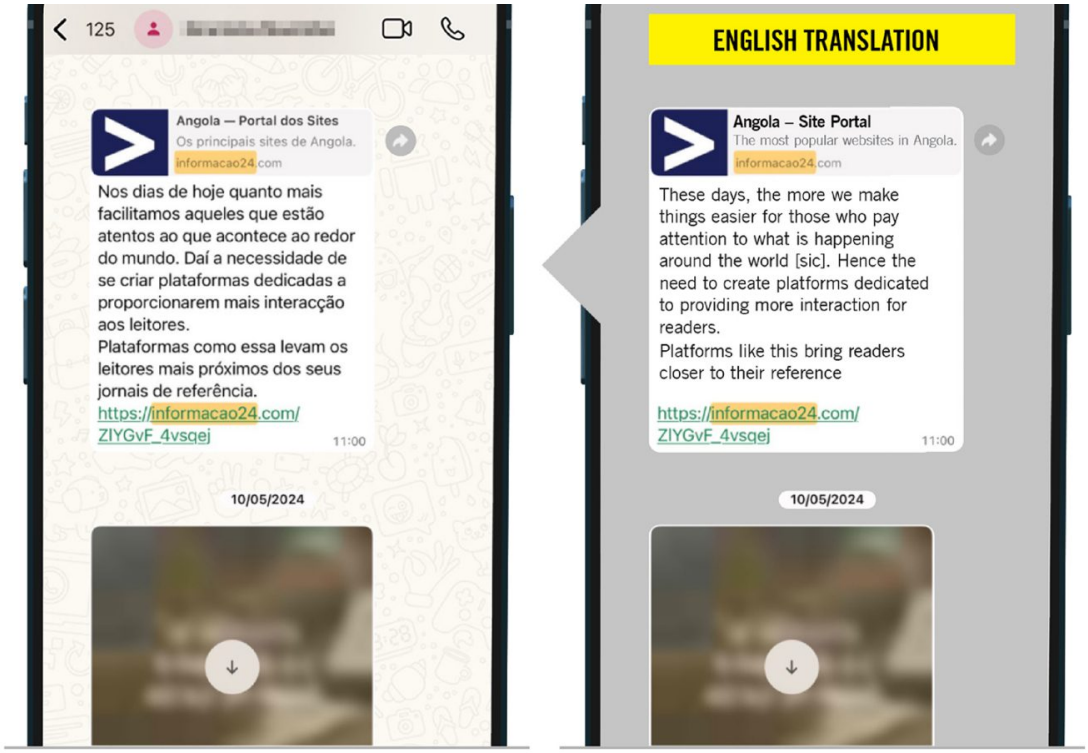

Figure 2: Screenshot of Whatsapp messages sent to Teixeira Cândido, containing malicious links, with the sender's name blurred. The original messages in Portuguese are in the left, and the translations to English in the right.

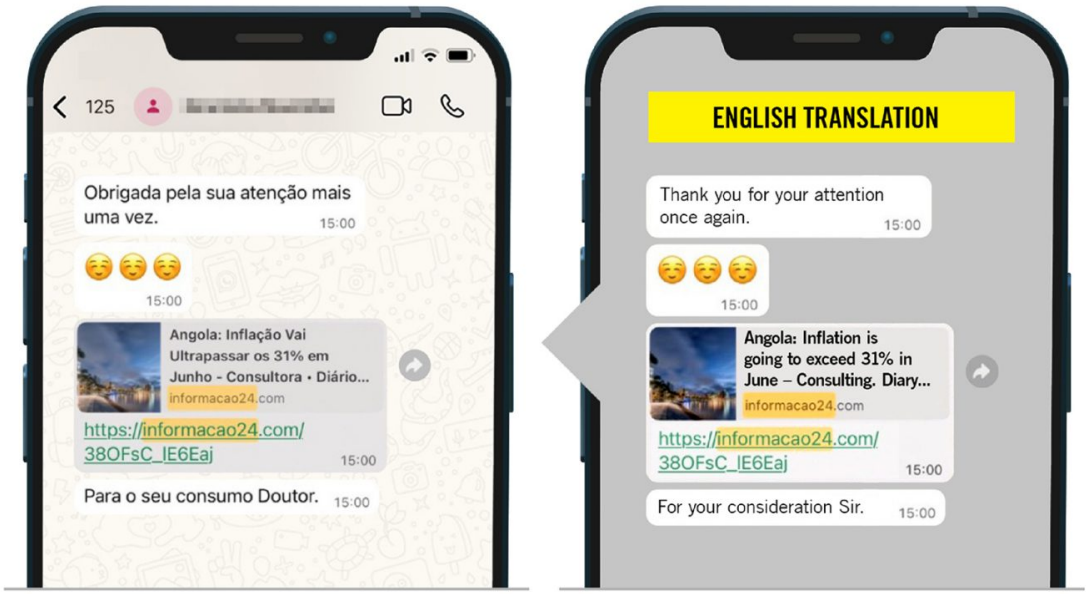

Figure 3: Screenshot of Whatsapp messages sent to Teixeira Cândido, containing malicious links, with the sender's name blurred. The original messages in Portuguese are in the left, and the translations

to English in the right.

Through forensic analysis of the links and associated domain names, Amnesty International's Security Lab determined with high confidence that all the links sent to Teixeira Cândido to this WhatsApp number were attempts to infect his phone with the Predator spyware. All infection domains matched a network fingerprint used to track Intellexa infection servers.

On 4 May 2024, one day after the first Predator infection link was received (Figure 4), Teixeira Cândido appears to have opened the infection link received, which would have resulted in the successful infection of the journalist's phone with the Predator spyware.

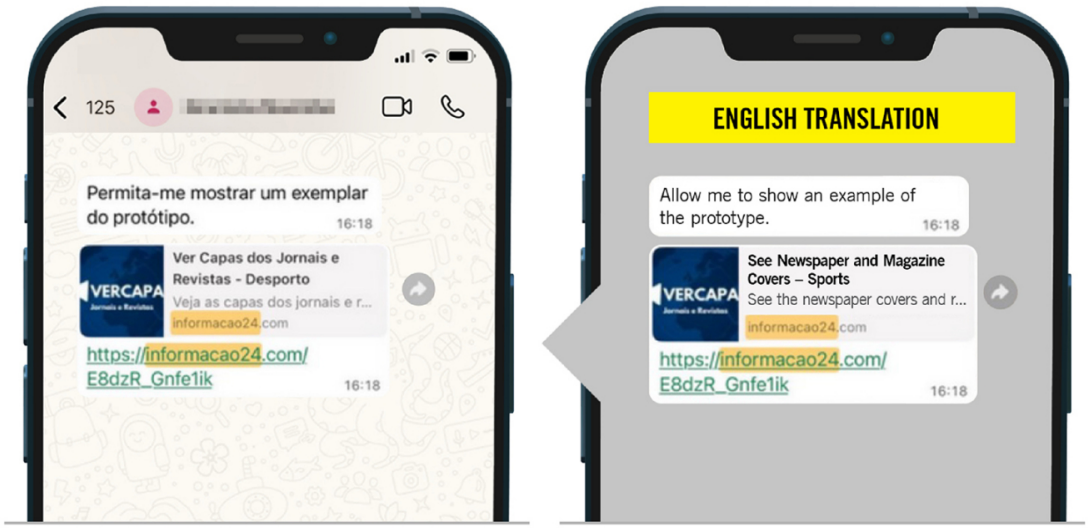

Figure 4: Screenshot of a WhatsApp message received by Teixeira Cândido on 3 May 2024 at 16:18 local time containing the malicious link that was clicked on and led to a successful Predator infection. The sender's name is blurred. The original messages in Portuguese are on the left, and the translations to English in the right.

Once the spyware was installed, the attacker could gain unrestricted access to Teixeira Cândido's iPhone. As outlined in a leaked Intellexa marketing brochure published as part of the Intellexa Leaks investigation (Figure 5), the spyware is capable of accessing an extensive range of data including encrypted messaging apps like Signal and WhatsApp, audio recordings, emails, device locations, screenshots and camera photos, stored passwords, contacts and call logs, and the ability to activate the phone's microphone.

Figure 5: Leaked marketing brochure presenting the capabilities of Intellexa's Predator spyware, published in the Intellexa Leaks investigation from 2025.

Forensic traces of active Predator infection

Amnesty International's Security Lab identified forensic traces of network communications made by the Predator spyware from Teixeira Cândido's phone throughout the day on 4 May 2024. This confirmed that the spyware was installed and running on the journalist's phone during that time frame.

The spyware process was found running from the directory /private/var/containers/Bundle/. Amnesty International has previously found cases of Predator using this directory for execution. A separate public analysis of a 2023-era Predator sample also confirms that the same execution path was used by Predator at the time. These forensic traces, in addition to known Predator infection domains used in the infection links, allow for the attribution of this attack to Predator.

Predator process execution on disk
/private/var/containers/Bundle/iconservicesagent

Unlike in earlier cases, Intellexa now appears to randomise the process name used when running the Predator implant and watcher binaries on target devices. In an effort to avoid detection, the spyware now impersonates one of a set of legitimate iOS system processes. In this case, the spyware was running as "iconservicesagent", although unlike the legitimate iOS system binary, the malicious process was running from the "/private/var/containers/Bundle/" directorv.

On 4 May 2024, the day of the successful spyware infection, Teixeira Cândido's iPhone was still running iOS 16.2, an outdated version with publicly known security issues, released in December 2022. Using older operating versions can open the phone to possible infections as malicious actors take advantage of older and already known exploits, although in this case it is unclear if this happened. At the time of Candido's attack, iOS 17.4.1 was already available and included security patches for critical vulnerabilities on iOS 16.7 and iOS 17.0.1. These vulnerabilities include CVE-2023-41993 (WebKit JIT remote code execution), CVE-2023-41992 (Kernel IPC Use-After-Free) and CVE-2023-41991 (Code signing bypass), all of which were attributed to Intellexa by Google. While it is difficult to determine the exact exploit used, it is plausible that the same exploit chain was used against Teixeira Cândido's phone due to an older operating system. Nevertheless, Intellexa is believed to have had access to zero-day exploits in 2024 and 2025, so it is also possible the phone could have been successfully infected even if fully patched. A zero-day exploit is a piece of software or code that takes advantage of a software vulnerability not known to the original software developer to gain access to a device. A zero-day exploit can successfully target even fully patched and updated devices.

The Predator spyware infection appears to have lasted less than one day, with the infection being removed when Teixeira Cândido's phone was restarted in the evening of 4 May 2024. From that time until 16 June 2024, the attackers made 11 new attempts to re-infect the device by sending him new malicious Predator infection links. All of these subsequent attack attempts appear to have failed, likely due to the links simply not being opened.

TIMESTAMP (UTC)	EVENT
2024-05-03 15:18:59	Malicious WhatsApp message with Predator exploit link: https://infor-macao24[.]com/E8dzR_Gnfe1ik
2024-05-04 05:33:40	Network activity from mali-cious Predator iconservicesagent (1.94 MB download of data, 50.17 MB up-load).
2024-05-04 08:36:07	Forensic traces of mali-cious Predator process running on the phone.
2024-05-04 16:32:12	Additional forensic traces of malicious process execution.

2024-05-05 10:19:04	Malicious WhatsApp message with Predator exploit link: https://exclusivo24h[.]com/umSvW_R0fiDXk
2024-05-06 11:00:27	Malicious WhatsApp message with Predator exploit link: https://informacao24[.]com/bO7cqa_ROcg4Rx
2024-05-07 10:00:25	Malicious WhatsApp message with Predator exploit link: https://informacao24[.]com/ZlYGvF_4vsqej
2024-05-10 14:21:47	Malicious WhatsApp message with Predator exploit link: https://exclusivo24h[.]com/aeN9mE_P0GnSq
2024-05-15 14:00:33	Malicious WhatsApp message with Predator exploit link: https://informacao24[.]com/38OFsC_IE6Eaj
2024-06-03 15:46:04	Malicious WhatsApp message with Predator exploit link: https://exclusivo24h[.]com/PwYd6_9jeeFCi
2024-06-04 15:19:59	Malicious WhatsApp message with Predator exploit link: https://informacao24[.]com/IAiVN_oH1hXp
2024-06-14 10:17:43	Malicious WhatsApp message with Predator exploit link: https://exclusivo24h[.]com/6ZzfY0_2IMMXxk
2024-06-20 10:42:51	Malicious WhatsApp message with Predator exploit link: https://informacao24[.]com/cAhQK_qBeTdNq
2024-07-16 14:10:23	Malicious WhatsApp message with Predator exploit link: https://blocoinformativo[.]com/VDBE8_PUwOucy

Figure 6: Device's events timeline.

The tip of the iceberg: evidence of wider Intellexa's Predator domains and attack activity linked to Angola

Infrastructure analysis and tracking indicates that the Predator spyware has been active with a focus on Angola since at least early 2023. Amnesty International believes the attack on Teixeira Cândido is only a fragment of the overall Predator spyware targeting connected to Angola. It is not currently possible to conclusively identify the customer of the Predator spyware in the country.

Spyware systems like Predator must communicate with servers on the internet to receive commands from the spyware operator and to collect surveillance data extracted from the phone. These spyware servers are usually also tied to specific domain names chosen by the customer or by the spyware company on behalf of the customer. By analysing domain names used by the spyware campaign, researchers can often infer that the spyware is focused on a particular region, country or group of individuals based on patterns in domain name registration and other linguistics.

In 2024, Recorded Future's Insikt Group published independent research documenting on a likely Predator customer within Angola for the first time, based on their tracking of Predator infrastructure and network intelligence data. In thise current research, Amnesty International's Security Lab also attributes the domains sent to Teixeira Cândido to Intellexa's Predator spyware, as they match a known network fingerprint for Predator infection servers. The first domain sent to Teixeira Cândido on 3 May 2024 – "exclusivo24h[.]com" – was registered in March 2024. All the domain names were written in Portuguese.

By mapping out other Predator domains potentially linked to Angola, it is possible to build a deeper understanding of the timeline of Predator's activity in the country. Through technical investigations, Amnesty International identified Predator domains linked to possible Angola targeting, based on the thematic focus, language and other technical measurements (Figure 7). The first domains linked to Angola were deployed as early as March 2023, indicating the start of Predator testing or deployment in the country. Some of the domains could be linked to other Portuguese-speaking contexts.

DOMAIN	FIRST SEEN ON
jornaldeangola[.]co	2023-03-28

angop[.]co	2023-03-28
jornaldeangola[.]net	2023-06-16
novojornal[.]info	2023-06-16
mujimbo[.]co	2023-06-16
factosdiarios[.]online	2023-06-16
folha8[.]net	2023-06-16
folha9[.]info	2023-06-16
mulherevips[.]com	2023-07-13
grupohel[.]social	2023-07-13
aoatlasescort[.]com	2023-08-10
clubs-k[.]com	2023-08-10
folha-9[.]com	2023-08-10
jornaldeangola[.]info	2023-08-10
mujimbos[.]co	2023-08-10
factosdiarios[.]co	2023-08-10
universedades[.]com	2023-08-10
lilpastanews[.]co	2023-08-10
adenuncia[.]com	2023-08-10
imparcialpress[.]com	2023-08-10

[illegible]	[illegible]
sicnoticia[.]com	2023-08-10
cnn-portugal[.]com	2023-08-10
platinalines[.]com	2023-08-10
ongs[.]life	2023-08-10
novojornal[.]co	2023-08-10
jornalf8[.]co	2023-08-10
vinhosadega[.]com	2023-08-10
taagangola[.]co	2023-08-10
tupuca[.]co	2023-08-10
mult[.]icaixa[.]info	2023-08-10
correiosdeangola[.]info	2023-08-10
candidaturasminfin[.]info	2023-08-10
candidaturassonangol[.]info	2023-08-10
mujmbosnoticias[.]com	2023-10-30
ongsworld[.]com	2023-11-15
vendaswebs[.]com	2023-11-15
mundodenoticias[.]online	2023-11-15
lusofonia-mundo[.]com	2023-12-14

vinho-online[.]com	2023-12-14
despachantonline[.]com	2024-01-11
exclusivo24h[.]com	2024-03-11
informacao24[.]com	2024-03-11
blocoinformativo[.]com	2024-07-08
despachosnegocios[.]com	2024-07-08
vslojasvendas[.]com	2024-07-16
gostosadeluxo[.]com	2023-08-10

Figure 7: Selection of Intellexa's Predator domains with potential links to Angola.

Human rights impacts

Intellexa's Predator spyware system is a form of highly invasive spyware that by default gains total access to data stored or transmitted from the target's device, for example encrypted messaging apps, audio recordings, emails, device locations, screenshots and camera photos, stored passwords, contacts and call logs, and the ability to activate the phone's microphone. The spyware is designed to leave no traces on the target's device, to render any independent audit of potential abuses difficult. As such, Amnesty International deems such forms of highly invasive spyware as fundamentally incompatible with human rights. The successful Predator attack against a journalist in Angola is a grave violation of the rights to privacy and freedom of expression, which in themselves impact a host of other rights such as freedom of association and peaceful assembly, as reported by Amnesty International. Such attacks create a chilling effect that affect journalists' ability to do their work.

The attack in Angola takes place in the context of deepening authoritarian practices. Under President João Lourenço's administration, Angola has experienced mounting legislative repression and shrinking civic space, including repression of peaceful protests and routine excessive or unnecessary use of force, arbitrary

arrests and detentions, as well as abuses in detention, and enforced disappearances.

"The use of commercial spyware against a journalist in Angola highlights a dangerous escalation in digital threats against civil society and the media. Governments and technology providers must be held accountable, and stronger protections are urgently needed for journalists, human rights defenders, and all citizens exercising their fundamental freedoms", said Friends of Angola.

States are the primary duty-bearers under international human rights law, but as laid out in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies also have a responsibility to respect human rights wherever they operate in the world and must carry out human rights due diligence. In a letter sent to Intellexa on 27 January 2026 outlining the findings of our investigation, Amnesty International asked about Intellexa's due diligence processes and practices.

Amnesty International revealed in Intellexa Leaks that, at the time of the leaked training videos used in the investigation, Intellexa retained the capability to remotely access Predator customer systems, even those physically located on the premises of its governmental customers, without evident technical limitations. In its letter to Intellexa sent on 27 January 2026, Amnesty International also asked whether the company had any knowledge of the attack in 2024, if it had access to the customer service system used in the Angola attack and to technical or other information about the target, and whether there were any technical limitations on their access. Amnesty International did not receive a response by the time of this publication.

While it remains unclear if Intellexa could access the specific Angolan deployment in 2024, the finding from Intellexa Leaks that the company had potential visibility into active surveillance operations of their customers, including seeing technical information about the targets, raises new legal questions about Intellexa's role in relation to the spyware and the company's potential legal or criminal responsibility for unlawful surveillance operations carried out using their products.

This new case of spyware use against a journalist in Angola makes clear – yet again – that the unchecked sale and use of surveillance technologies continue to facilitate human rights abuses at a global scale.