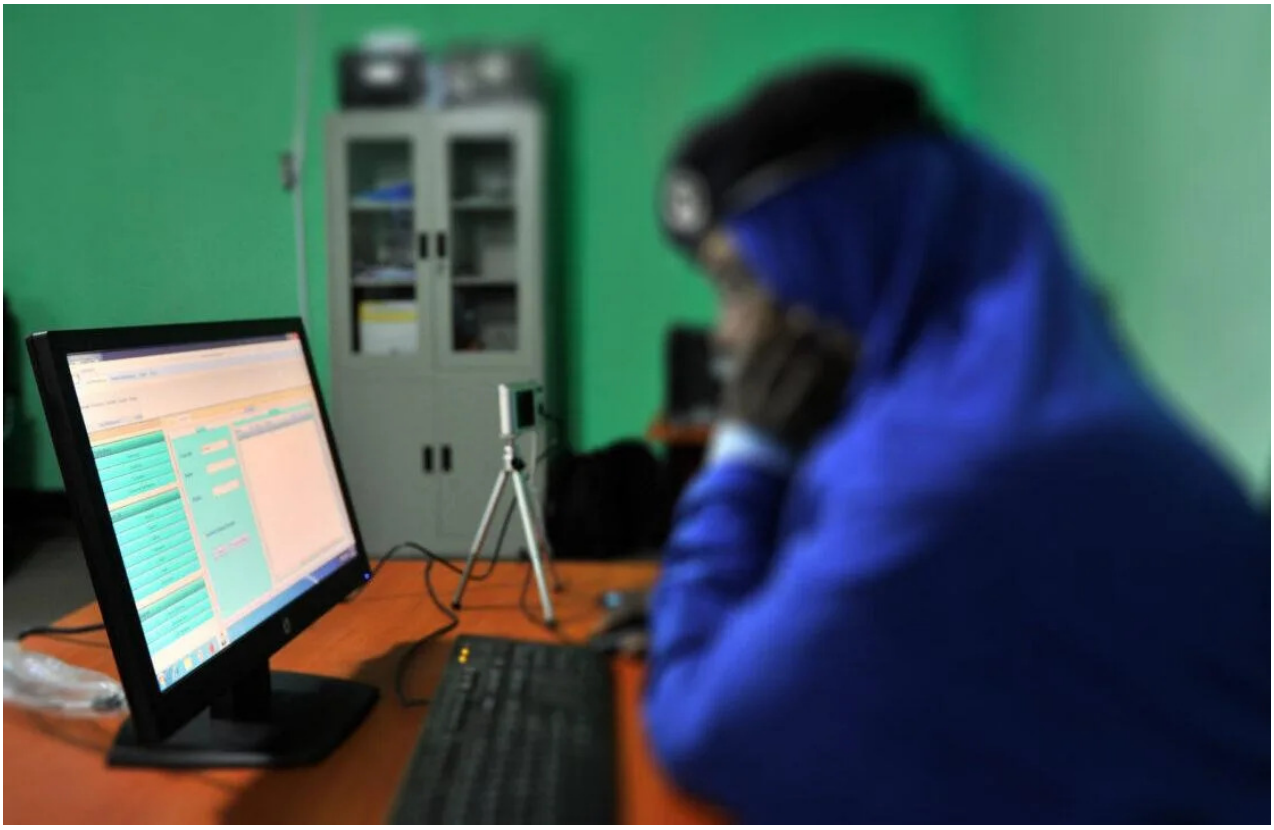
فريق التحرير | نشر في 26 March ,2026

Why Is “Israel” Supplying Africa With Advanced Surveillance Technologies?



In February 2026, an investigation by The Guardian revealed that Kenyan authorities used advanced Israeli technology from the company Cellebrite to hack the personal phone of activist and potential presidential candidate Boniface Mwangi while he was in detention.

The software enabled police to fully decrypt the device and extract private messages, files, passwords, and financial account information one of the latest episodes in which African governments have deployed Israeli technologies to suppress political dissent.

The incident once again cast a spotlight on the expanding footprint of Israeli cybersecurity firms and military hardware across the continent, as well as the reciprocal interests binding Tel Aviv to African capitals.

Three Advanced Israeli Spy Tools

Israeli spyware is widely deployed across Africa. Human rights activists in Angola, Morocco, and Rwanda have been documented as targets, along with journalists in Togo and media sources in Botswana.

Opposition figures in Ethiopia, Ghana, and Gabon as well as U.S. diplomats in

Uganda have also reportedly been targeted, according to research by the Institute for Security Studies in Africa.

Many African governments rely on such technologies to track political rivals and critics, deepening authoritarian tendencies and eroding democratic institutions, as a report by the Brookings Institution has warned.

The technologies exported by Israeli firms to Africa include sophisticated surveillance tools capable of transforming a smartphone into a comprehensive monitoring device. Among the most prominent:

1. Pegasus by NSO Group:
A zero-click spyware capable of infiltrating phones without any user interaction. It can steal photos, messages, and passwords, activate the camera and microphone, and track location data.

2. Predator by Intellexa:
Developed by the Intellexa consortium a network of companies led by former Israeli officer Tal Dilian it grants attackers full access to a compromised device’s microphone, camera, and stored data.

3. Cellebrite Device:
A digital forensics tool that enables the extraction of all data and files from Android and iPhone devices. It forms part of the global market for forensic analysis tools sold to governments worldwide.

Major Documented Surveillance Cases in Africa

1. Kenya: Targeting Opposition Figures With Cellebrite

In July 2025, Kenyan authorities arrested activist Boniface Mwangi and confiscated his phone. A technical analysis by Citizen Lab later revealed that police had used Cellebrite software to fully decrypt the device.

An application bearing Cellebrite’s digital signature was discovered on the phone. Through it, police extracted private messages, files, financial accounts, and passwords actions that constituted a clear violation of Kenya’s constitution and data protection law.

2. Angola: Journalism Under the Blade of Predator

In February 2026, an investigation by the Committee to Protect Journalists confirmed that the phone of Angolan journalist and lawyer Teixeira Cândido had been infected with Predator spyware ahead of the country’s 2027 elections, amid an increasingly restrictive media environment.

An unknown sender dispatched a WhatsApp message disguised as coming from a student group. The moment Cândido clicked the link, the spyware was installed,

granting attackers control over his microphone and camera and access to contacts, messages, and photos.

Cândido described the ordeal starkly: “I felt as though I were naked in the street, uncertain what information they had obtained about my private life.”

3. Togo: Journalists Targeted With Pegasus

In January 2024, cybersecurity platform Dark Reading reported that an investigation by Reporters Without Borders found that the phones of several Togolese journalists had been hacked using Pegasus.

The findings showed that between February and July 2021, Pegasus was used at least 23 times to infiltrate the phone of Loïc Lawson, publisher of the newspaper Flambeau des Démocrates. Freelance journalist Anani Sossou faced a similar attack in October 2021.

A leaked list of 50,000 numbers linked to the Pegasus Project included three additional Togolese journalists. The report detailed how the Israeli-made spyware enables operators to extract all data and intercept messages, emails, passwords, and location data without the user’s knowledge.

4. Morocco and Rwanda: Spying on Leaders and Officials

A 2021 study published by the Brookings Institution highlighted the expanding use of Pegasus across Africa, noting that both the Moroccan and Rwandan governments had deployed the software to spy on opposition figures and politicians beyond their borders.

Morocco is believed to have targeted up to 10,000 numbers, while Rwanda allegedly monitored around 3,500 activists, journalists, politicians, and diplomats—including the daughter of a Rwandan dissident living in exile.

These tools have also been used for cross-border surveillance. Rwanda reportedly included the number of South African President Cyril Ramaphosa on its target list.

Morocco, meanwhile, placed Algerian and French officials under surveillance. Such practices illustrate how Israeli technology is fueling a regional espionage race and reinforcing authoritarian tendencies.

Israel’s Objectives: A Diplomatic Lever

1. Breaching the African “Fortress”:
Israel’s foremost objective is to break what it calls the “automatic majority” supporting Palestine in international organizations.

Former Israeli officials and journalists—such as Amitai Ziv of Haaretz—have stated bluntly: “When Israel sells cyber technology to an African state, it secures

its vote at the United Nations.”

Arms and cyber sales have functioned as diplomatic currency, helping Israel obtain observer status at the African Union (later suspended).

2. Exporting the Occupation Model:
Israel seeks to normalize its repressive practices globally. When sovereign states deploy technologies developed to suppress Palestinians, they implicitly legitimize both the tools and the security model behind them. The occupation becomes a “laboratory” for innovation; Africa becomes the market.

3. Economic Returns:
The cyber sector represents a significant share of Israel’s high-tech exports. In 2023, defense exports reached $13 billion, a substantial portion of which came from cyber technologies funds crucial to sustaining Israel’s military-industrial complex.

African Gains: Regime Survival

1. Preemptive Superiority:
Israeli technology equips African governments with the capacity to “predict” protests before they erupt and to identify the intentions of opposition figures.

2. Bypassing Western Constraints:
Western countries nominally attach human rights conditions to arms sales. Israel, by contrast, sells “without questions,” making it an ideal partner for ostracized regimes.

3. Access to Washington:
Many African leaders believe that the road to the White House runs through Tel Aviv. Purchasing Israeli technology is seen as a gesture of goodwill one that can open doors to pro-Israel lobbying networks in Washington, shielding regimes from congressional scrutiny and polishing their image abroad.

The report concludes that Israeli technology in Africa is not a tool for development or human security in the humanitarian sense, but rather a “digital whip” lashing populations seeking freedom an attempt to replicate the “surveillance state” model employed in the West Bank and scale it across an entire continent.