

Forum:[Hack Forums](#)

Thread: [The US is now the largest investor in commercial spyware](#)

MadScientist - September 14, 2025, 8:28 am

The United States has emerged as the largest investor in commercial spyware—a global industry that has enabled the covert surveillance of journalists, human rights defenders, politicians, diplomats, and others, posing grave threats to human rights and national security.

In 2024, 20 new US-based spyware investors were identified, bringing the total number of American backers of this technology to 31. This growth has largely outpaced other major investing countries such as Israel, Italy, and the United Kingdom, according to a new report published today by the Atlantic Council.

The study surveyed 561 entities across 46 countries between 1992 and 2024, identifying 34 new investors. This brings the total to 128, up from 94 in the dataset published last year.

The number of identified investors in the EU Single Market, plus Switzerland, stands at 31, with Italy—a key spyware hub—accounting for the largest share at 12. Investors based in Israel number 26.

US-based investors include major hedge funds D.E. Shaw & Co. and Millennium Management, prominent trading firm Jane Street, and mainstream financial-services company Ameriprise Financial—all of which, according to the Atlantic Council, have channeled funds to Israeli lawful-interception software provider Cognyte, a company allegedly linked to human rights abuses in Azerbaijan and Indonesia, among others.

Another notable example of a new US-based investment in spyware is the late-2024 acquisition of Israeli spyware vendor Paragon Solutions by AE Industrial Partners, a Florida-based, national-security-focused private equity firm. Paragon made headlines last week when its one-year contract with Immigration and Customs Enforcement (ICE)—first reported by WIRED in October 2024—was suddenly reactivated after a lengthy pause.

Civil society groups described the move by the Trump administration as “extremely troubling” and said it “compounds the civil liberties concerns surrounding the rapid and dramatic expansion of ICE’s budget and authority.”

Paragon was linked to alleged misconduct in Europe after WhatsApp reported that Italian journalists and civil society members had been targeted with its technology. An Italian parliamentary committee found that the government had used its Graphite spyware to only surveil human rights defenders. However, University of Toronto’s Citizen Lab confirmed the targeting of an Italian journalist and identified potential Paragon customers in Australia, Canada, Denmark, Cyprus, Singapore, and Israel.

Paragon, responding to the committee’s findings, accused Italian authorities of refusing to conduct a thorough technical verification—an assessment it argued could have resolved the issue.

Apart from focusing on investment, the Atlantic Council notes that the global spyware market is “growing and evolving,” with its dataset expanded to include four new vendors, seven new resellers or brokers, 10 new suppliers, and 55 new individuals linked to the industry.

Newly identified vendors include Israel's Bindecy and Italy's SIO. Among the resellers are front companies connected to NSO products, such as Panama's KBH and Mexico's Comercializadora de Soluciones Integrales Mecale, as highlighted by the Mexican government. New suppliers named include the UK's Coretech Security and UAE's ZeroZenX.

The report highlights the central role that these resellers and brokers play, stating that it is "a notably under-researched set of actors." According to the report, "These entities act as intermediaries, obscuring the connections between vendors, suppliers, and buyers. Oftentimes, intermediaries connect vendors to new regional markets."

"This creates an expanded and opaque spyware supply chain, which makes corporate structures, jurisdictional arbitrage, and ultimately accountability measures a challenge to disentangle," Sarah Graham, who coauthored the report, tells WIRED.

"Despite this, resellers and brokers are not a current feature of policy responses," she says.

The study reveals the addition of three new countries linked to spyware activity—Japan, Malaysia, and Panama. Japan in particular is a signatory to international efforts to curb spyware abuse, including the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware and the Pall Mall Process Code of Practice for States.

"The discovery of entities operating in new jurisdictions, like Japan, highlights potential conflicts of interest between international commitments and market dynamics," Graham says.

Despite efforts by the Biden administration to constrain the spyware market through its executive order, trade and visa restrictions, and sanctions, the industry has continued to operate largely without restraint.

"US policymakers have systematically targeted the proliferation and misuse of spyware through robust policy action, but there is a critical gap between them and US investors—where US dollars continue to fund the very entities US policymakers are trying to combat," says Atlantic Council's Jen Roberts, who also worked on the report.

For example, spyware vendor Saito Tech (formerly Candiru), which has been on the US Commerce Department's Entity List since 2021, saw new investment by US firm Integrity Partners in 2024. "[This] shows that signaling from the US government has not gone far enough to deter investment in this technology," Roberts says.

In addition, there is limited public awareness that some of the money spent on this controversial technology may ultimately come from ordinary citizens' own pockets.

In the case of AE Industrial Partners, investment performance reports show that the firm was backed by several US pension funds—among them the Contra Costa County Employees' Retirement Association, Baltimore Fire & Police Retirement System, Houston Firefighters' Relief and Retirement Fund, and the New Mexico Educational Retirement Board—providing cash that could help support the deal with Paragon, which could reach \$900 million.

"This highlights the need for better understanding from both US government and the public—that the average American might not understand how their dollars are funding the proliferation and misuse of spyware," says Roberts.

Crucially, the Trump administration's policy in this space is not yet fully defined.

The Atlantic Council's Roberts calls for further action to target US outbound investment and suggests broadening the scope of Executive Order 14105—which already requires notification of overseas investments in quantum technology, AI, semiconductors, and microelectronics—to also cover investment in spyware.

Some reports suggest that the administration may also be considering amendments to the Biden-era Executive Order 14093 that restricts government use of spyware.

In particular, it is crucial to maintain this executive order, which leverages US purchasing power to protect Americans against this technology, Roberts explains.

“US purchasing power is a significant tool in shaping and constraining the global market for spyware.”

Source -

<https://arstechnica.com/security/2025/09/the-us-is-now-the-largest-investor-in-commercial-spyware/>