Click, Load, Kill:

A Look into the Cyberweapon Industry in the WANA Region

SMEX

Acknowledgments

This research was conducted by SMEX, with support from FIND (find[.]ngo) and Access Now. This report's authors also want to acknowledge the assistance of Steven Feldstein, James Shires, and "V" for their feedback and guidance on this work.

SMEX is a nonprofit dedicated to safeguarding human rights in digital1 spaces across West Asia and North Africa. We advocate for safe and uncensored access to the internet, mobile services, and networked spaces for people in the region and the diaspora.

Published in 2025 by SMEX.

Visit www.smex.org to learn more.

Executive Summary

As we spend more of our time online, privacy, one of the fundamental human rights enshrined in international law, becomes more important than ever.[1] Yet the right to privacy is constantly under attack.

While the meaning of the right to privacy has changed over time, Samuel D. Warren and Louis D. Brandeis in 1890 famously offered a timeless definition of privacy as "the right to be let alone."[2] But modern internet users would be hard-pressed to feel truly let alone today. Yes, some privacy-focused technology like end-to-end encrypted chat services promise higher levels of data confidentiality. But many large technology companies mine users' personal data and sell it to the highest bidder,[3] governments across the world employ widespread surveillance,[4] and multiple countries actively censor and manipulate internet content.[5] One of the biggest offenders in this trend is commercial spyware vendors (CSVs)—companies that design, market, and/or sell spyware to entities across the world for profit. In this report, SMEX investigates some of the major purveyors of spyware in the West Asia and North Africa (WANA) region.

Spyware is a form of malware that enables threat actors to clandestinely spy on victims. Upon successful infection, a spyware operator can monitor and steal almost every type of data imaginable on a person—their messages, calls, and search history, and even camera and mic use—without their knowledge.[6] Due to how it spies on users without their permission, spyware fundamentally violates victims' human right to privacy.

Many states across the world repress their populations to maintain control.[7] Researchers like Steven Feldstein argue that autocracies rely on what Levitsky and Way (2010) have coined low-intensity coercion tactics: imposing widespread surveillance, obstructing the activities of political opponents, and harassing the opposition.[8] While we often conceive of repression as physical violence, repression can also be digital.[9] Tools of digital repression, like surveillance

---

[1] United Nations General Assembly (1948). *The Universal Declaration of Human Rights*, Articles 12, 19. Paris.
[2] Warren, S.D. and Brandeis, L.D. (1890). The Right to Privacy. Harvard Law Review, 4(5), pp.193–220. doi:https://doi.org/10.2307/1321160.
[3]Sebastiaan Brommersma (2023). *Your Most Intimate Data Is Being Sold to the Highest Bidder – Who Might Be a Spy*. [online] Follow the Money - Platform for Investigative Journalism. Available at: https://www.ftm.eu/articles/your-intimate-data-is-being-sold [Accessed 11 Aug. 2025].
[4] Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. [online] *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en [Accessed 11 Aug. 2025].
[5] Funk, A., Vesteinsson, K. and Baker, G. (2024). *Freedom on the Net 2024: The Struggle for Trust Online*. [online] Freedom House. Available at: https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online [Accessed 11 Aug. 2025].
[6] Fortinet (2024). What Is Spyware? Definition, Types And Protection. [online] Fortinet. Available at: https://www.fortinet.com/resources/cyberglossary/spyware [Accessed 11 Aug. 2025].
[7] Davenport, C. (2007). State Repression and Political Order. *Annual Review of Political Science*, 10(1), pp.1–23. doi:https://doi.org/10.1146/annurev.polisci.10.101405.143216.
[8] Levitsky, S. and Way, L.A. (2010). *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. Cambridge University Press.
[9] Feldstein, S. (2021). *The Rise Of Digital Repression : How Technology Is Reshaping Power, Politics, And Resistance*. New York, NY: Oxford University Press.

technology, help states track and control dissidents, execute low-intensity coercion, and ultimately implement other, more extreme forms of repressive violence. Spyware is definitionally a form of surveillance, and helps states accelerate repression. CSVs typically only sell to government clients and claim to limit sales to governments that use their products for "legitimate" reasons. Spyware customers have been documented to abuse the products to violate human rights—identifying unwanted citizen behavior and repressing it. In this way, spyware also violates victims' human right to freedom of expression.[10] [11] [12]

Despite the infamy, spyware variants like NSO Group's Pegasus have earned over the past decade, governments across the world have continued to be caught using—or suspected of using—spyware. The Carnegie Endowment for International Peace notes that over a third of all countries purchased spyware or similar technologies from 2011 to 2023.[13] Nearly all states within the WANA region have been exposed as likely using spyware—the focus of this research.[14] Despite the work of digital watchdog organizations like Access Now, Amnesty International, Citizen Lab, and SMEX, there is no indication that governments are using spyware less frequently.

One of the biggest challenges in researching spyware and its users is that CSVs intentionally hide their behavior and clients and obfuscate their corporate identity. For example, SMEX's investigation in this report revealed that NSO Group is run through at least five layers of holding companies, the highest level of which is based in Luxembourg. Because of this, there is a lack of understanding of what CSVs operate and where, particularly within the WANA region. Ultimately, this research aims to fill that gap by identifying which CSVs operate the most frequently in WANA.

One way to estimate where CSVs are active is by looking at what vendors' spyware is operating in the wild and attributable to governments in the region. Following in the footsteps of researchers Steven Feldstein and Brian Kot (2023), this paper looks at publicly available information, news sources, court documents, data leaks, and corporate records to catalogue spyware activity in the region. It appears that **NSO Group**, **Cytrox/Intellexa Group**, **Cellebrite**, and **Saito Tech/Candiru** operate the most in the region. Moreover, CSVs based out of Israel seem to dominate the market in the WANA region, though in the past CSVs like the Italy-based Hacking Team (now Memento Labs) were favorites among regional governments. Throughout the bulk of this report, SMEX details the corporate structure, marketing, premier products, and prominent attacks associated with the four top CSVs

[10] Dunja Mijatović (2023). *Highly Intrusive Spyware Threatens the Essence of Human Rights.* Council of Europe Human Rights Comment. https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights.
[11] Santiago Gomez, E. and Rodriguez Rodriguez, C., 2018. Surveillance Technologies: A review of legitimate State violence in security and control contexts. ENCRUCIJADAS REVISTA CRITICA DE CIENCIAS SOCIALES, 16. Available at: https://gateway.webofknowledge.com/gateway/Gateway.cgi?GWVersion=2&SrcApp=Summon&SrcAuth=ProQuest&DestApp=WOS&DestLinkType=FullRecord&UT=000455807000011 [Accessed 11 Aug. 2025].
[12] Papademetriou, G. (2023). Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry. *Harvard Human Rights Journal*, (Spring 2023).
[13] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en [Accessed 13 Jun. 2025].
[14] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). *HIDE AND SEEK.*

observed in the region. In doing so, the research hopes to add novel contributions to the public's understanding of spyware incidents in the WANA region, their mode of operation, and their human toll through interviews SMEX has conducted.

SMEX continues to call on all countries to immediately stop using spyware and for all CSVs to stop selling surveillance technology immediately. Civil society members and human rights defenders should take active steps to protect themselves online, including using end-to-end encrypted communications, using unique and complex passwords, using Virtual Private Networks (VPNs), and using password managers.

Contents

Part 1: Background

1.1 Introduction: What Is Spyware?

"If privacy had a gravestone, it might read: 'Don't Worry. This Was for Your Own Good.'"
—John Twelve Hawks [*The Dark River* (Fourth Realm, #2)]

Bing. A WhatsApp notification flashes on your phone—a number you do not recognize has added you to a group and sent you a PDF. Curious, you decide to open the message and inspect the file.

You get suspicious, though, noticing you do not know any members of the group. *Never mind. You know better than to open random links or documents sent by unknown numbers.* You decide not to open the file. However, because of a vulnerability in how WhatsApp handles files, it automatically parses the PDF, activating a chain of events that allows hidden malware to load into WhatsApp and propagate into other apps on your device.[15] Within moments, an attacker has potentially gained access to your phone's files, messages, call log, and location information. You almost certainly don't notice, but your privacy is now completely compromised.

While the idea is frightening, it is not a fantasy—this is a documented way the Israeli spyware company Paragon Solutions Ltd (Paragon) tried to propagate its malware product "Graphite" in late 2024 (though this exact exploit chain has since been patched).[16] Paragon's Graphite represents a larger trend in one of the gravest threats to digital human rights today: commercial spyware vendors selling spyware to governments across the world.

Spyware, a portmanteau of "spy" and "software," is a form of malicious software that enables attackers to spy on victims without their knowledge. It is, in researcher Ajay Chawla's words, a "privacy killer."[17]A commercial spyware vendor (CSV) is a company that specializes in selling malicious software used to surveil a target population. These companies represent a burgeoning industry: While exact estimates of the industry's size and value vary, according to the Carnegie Endowment for Peace, over a third of all countries purchased spyware or related technologies from commercial vendors between 2011 and 2023.[18] In that time period, almost every country in West Asia and North Africa (WANA), a major cluster for spyware operation, has either been exposed as using spyware or has had spyware infections traced to them (with the exception of Mauritania, Somalia, and Western Sahara).[19] Many government agencies worldwide have contracts with CSVs. The US Immigration and Customs

[15] Marczak, B. (2025). *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations - The Citizen Lab*. [online] The Citizen Lab. Available at: https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/.
[16] News, T.H. (2025). *Meta Confirms Zero-Click WhatsApp Spyware Attack Targeting 90 Journalists, Activists*. [online] The Hacker News. Available at: https://thehackernews.com/2025/02/meta-confirms-zero-click-whatsapp.html.
[17] Chawla, A. (2021). Pegasus Spyware – 'A Privacy Killer'. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3890657.
[18] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*
[19] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. [online] The Citizen Lab. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.

Enforcement, as a prominent and timely example, just renewed a contract with Paragon in September 2025.[20]

CSVs predominantly sell their products to governments—and, to a much lesser extent, private companies—with contracts based on the client's requested time period and number of exploits. A leaked document from the CSV Intellexa from 2022 illustrates this: The order sheet lists various types of exploits for a chosen quantity of infections—in this case, 10 concurrent iOS and Android infections for 8 million euros and a 12-month warranty.[21]

Although all WANA-region countries participate in various international human rights conferences and agreements, they routinely violate digital rights, surveil citizens, and implement information controls on their populations.[22] Gulf countries are some of the most prolific clients of CSVs, yet over half of Gulf Cooperation Council (GCC) members have ratified the United Nations' ten primary human rights treaties. Their commitments are dubious at best, or outright lies at worst.[23] Many of the largest CSVs claim a strict adherence to human rights standards, arguing they do not sell to autocratic regimes, and rely on carefully crafted rhetoric to claim that they only fight serious crime. NSO Group, for example, markets its products as "cyber intelligence for global security and stability."[24] After NSO Group garnered criticism for its human rights track record, in 2019 the New York Times reported that it claimed only to have sold its products to governments fighting crime or terrorism.[25] However, in 2018 Citizen Lab found that authoritarian governments such as Saudi Arabia and Egypt have likely used NSO Group products.[26] According to Citizen Lab, NSO's flagship spyware Pegasus has been tracked to most countries in the WANA region, and CSV QuaDream's spyware has likely been deployed in multiple WANA countries too.[27] [28] Furthermore, according to the Carnegie Endowment for Peace, 44 of 74 known governments that purchased spyware between 2011 and 2023 were autocratic.[29] While spyware companies market themselves as making the world safer—saying their technology prevents bad things from happening—many of their clients regularly abuse these technologies to surveil dissidents, minority populations, and political opponents.

There is a major knowledge gap regarding both to whom and what CSVs are selling, and how these companies are structured. Not much is known about which major CSVs are operating

---

[20] Franceschi-Bicchierai, L. (2025a). *ICE Reactivates Contract with Spyware Maker Paragon | TechCrunch*. [online] TechCrunch. Available at: https://techcrunch.com/2025/09/02/ice-reactivates-contract-with-spyware-maker-paragon/ [Accessed 3 Sep. 2025].

[21] Google Threat Analysis Group (2024). *Buying Spying: Insights into Commercial Surveillance Vendors*. [online] p.17.

[22] Shires, J. (2021). *The Politics of Cybersecurity in the Middle East.*

[23] Horak, G. (2023). P*ersonal Details Exposed: Spyware and Human Rights in the Middle East and North Africa*. Master's thesis, Harvard University Division of Continuing Education.

[24] NSO Group (2019). *NSO GROUP - Cyber intelligence for global security and stability*. [online] NSO Group. Available at: https://www.nsogroup.com/ [Accessed 21 Aug. 2025].

[25] Goel, V. and Perlroth, N. (2019). Spyware Maker NSO Promises Reform but Keeps Snooping. *The New York Times*. [online] 9 Nov. Available at: https://www.nytimes.com/2019/11/09/technology/nso-group-spyware-india.html.

[26] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). *HIDE AND SEEK.*

[27] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). *HIDE AND SEEK.*

[28] Marczak, B., Scott-Railton, J., Perry, A., Aljizawi, N., Anstis, S., Panday, Z., Lyon, E., Abdul Razzak, B. and Deibert, R. (2023). *Sweet QuaDreams.*

[29] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive?*

in the WANA region. Researchers at the Atlantic Council identify that one of the largest clusters of CSVs operating in the region originates in Israel, but less information is available about where the products are actually used. Limited research has been done into which spyware each country in the region uses most frequently. This paper aims to begin filling that gap, while also looking at these CSVs' operations and strategies, finances, and impact on human rights in the region.

To better understand the state of spyware in the WANA region, this paper asks:

1. What are some of the major CSVs operating in the WANA region, and what are their operational strategies?
2. Who finances these companies, and what are the implications of these relationships?
3. How do spyware operations affect the geopolitical and social structures in the WANA region?

By answering these questions, this analysis aims to summarize, condense, and produce new research findings on spyware used in the WANA region.

1.2 Literature Review

Privacy and Digital Human Rights

Our world is growing increasingly technologized. There are over 18 billion mobile devices connected worldwide, and, as of February 2025, over 5.56 billion individuals across the globe have access to the internet.[30] [31] As more people connect over the internet and use more devices, their *attack surface*—that is, the number of potential digital threats they are exposed to—grows. This greater attack surface creates an opportunity for threat actors—commercial, governmental, or independent—to access users' data and violate their privacy. But what is privacy, and why should we care about it?

Privacy and the right to it are at the core of understanding the threat posed by spyware. But the notion of privacy, including how societies define it and consider what should be kept private, has changed over time, and is a notoriously variable concept. Philosopher Judith Jarvis Thomson once wrote that "perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[32] Warren and Brandeis famously were among the first to tackle this in "The Right to Privacy" in 1890, in which they aptly defined privacy as "the right to be let alone."[33]

[30] Laricchia, F. (2023). Number of mobile devices worldwide 2019-2023. [online] Statista. Available at: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/.
[31] Petrosyan, A. (2025). Worldwide Digital Population 2025. [online] Statista. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/.
[32] Thomson, J.J., 1975. The right to privacy. *Philosophy & Public Affairs*, pp.295-314.
[33] Warren, S.D. and Brandeis, L.D. (1890). The Right to Privacy. Harvard Law Review, 4(5), pp.193–220. doi:https://doi.org/10.2307/1321160.

Daniel Solove, widely considered a leading scholar on privacy, notes in *Understanding Privacy* that many define privacy as a right to some variation of "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[34] Sohail Aftab (2024) adds to this in "The Concept of the Right to Privacy," arguing the concept of privacy is impossible to define due to the rich history of varied definitions of privacy, such as the right to remain secluded, the right to be left alone, the right to conceal secrets, the right to be inaccessible, and the right to control one's personal information. However, Aftab argues that every definition of privacy as a right is fundamentally based on the concepts of dignity and autonomy.[35] Scholar Woodrow Hartzog points out that Solove ultimately argues that it is less important to define privacy and more to think about "what privacy is for."[36]

The United Nations was one of the first international institutions that codified humans' right to privacy, when it released the Universal Declaration of Human Rights. Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation," and Article 19 gives "the right to freedom of opinion and expression … [including the] freedom to hold opinions without interference."[37] The International Covenant on Civil and Political Rights echoes this in Articles 17 and 19, denoting privacy and freedom of expression as protected human rights.[38] Similar sentiments are codified in the European Convention for the Protection of Human Rights and Fundamental Freedoms, the American Convention on Human Rights, and the Arab Charter on Human Rights. In 2015, the UN special rapporteur on the right to privacy reinforced the importance of privacy in The "Report on the Right to Privacy in the Digital Age," specifying that privacy "is important for the realization of the right to freedom of expression and to hold opinions without interference."[39] In this view, the special rapporteur defines privacy as being fundamentally connected to other human rights.

Different digital rights frameworks have existed over time, but in 2015 the UN's Human Rights Council created the UN's first mandate on privacy. The Special Rapporteur for Privacy actively reports on digital privacy issues and frameworks worldwide.[40] The UN-sponsored Alliance for Digital Rights took defining privacy rights a step further in 2022 by calling for a universal digital rights framework to codify more robust principles on digital human rights, such as universal and equal digital rights, personal safety and data privacy, digital

---

[34] Daniel J. Solove (2008). *Understanding Privacy.*
[35] Aftab, S. (2024). The Concept of the Right to Privacy. In: Comparative Perspectives on the Right to Privacy. Ius Gentium: Comparative Perspectives on Law and Justice, vol 109. Springer, Cham. https://doi.org/10.1007/978-3-031-45575-9_3
[36] Solove, D.J. and Yale University Press (2011). *Nothing to Hide: the False Tradeoff between Privacy and Security*. New Haven ; London: Yale University Press, Cop in Hartzog, W. (2021). *What is Privacy? That's the Wrong Question*, in 88 The University of Chicago Law Review 1677. Available at: https://scholarship.law.bu.edu/faculty_scholarship/3063
[37] United Nations General Assembly (1948). *The Universal Declaration of Human Rights*.
[38] United Nations General Assembly (1948). *International Covenant on Civil and Political Rights*, Articles 17, 19. Paris.
[39] The United Nations Special Rapporteur on the right to privacy (2015). *A/HRC/28/`6: Report of the Special Rapporteur on the right to privacy in the digital age*. The United Nations Human Rights Council.
[40] UN Special Rapporteur on the right to privacy (2015). *History of the Mandate*. [online] OHCHR. Available at: https://www.ohchr.org/en/special-procedures/sr-privacy/mandate.

self-determination, and universal digital access.[41] A newer proposal to combine international human rights frameworks with digital technologies has taken form in the Digital Rights Governance Framework, which proposes a city-led governance framework of localized foundations, structures, and tools to protect digital rights. The first draft of the Framework was released in December 2021.[42] Each of these conventions and frameworks are buttressed by international nongovernmental organizations fighting for digital human rights, such as Access Now, the Electronic Frontier Foundation, and SMEX, which legally challenge abuses worldwide and provide help in digital emergencies.

The United Nations' Office on Drugs and Crime defines privacy when it comes to cybercrime as being "linked to freedom from identification." The United Nations argues privacy provides technology users "a space free from intimidation, retaliation, and other forms of coercion or sanction for the expression of thoughts, opinions, views, and ideas, without being forced to identify themselves."[43] It is this concept, freedom from being forced to be identified and give up one's personally identifiable information, that spyware directly violates.

Spyware, by its very nature, deeply limits privacy and actively curtails freedom of expression. Software that breaks into individuals' devices, establishes persistence, and monitors their activity violates any human rights framework that protects the freedoms of privacy and expression. Many governments, including in the EU, agree to international human rights frameworks and export limitations on goods that violate human rights, yet at the same time they actively use spyware. Moreover, countries that employ spyware often do so to monitor and punish certain classes of citizens, such as political dissidents and the LGBTQIA+ community.[44] Many of these countries have conflicting interests in "combating crime" (persons of interest) and allegedly supporting human rights. Consequently, fighting this trend, especially as many societies seek novel ways to fight crime, is increasingly vital.

Tactics of Repression

Governments—whether they're autocracies, anocracies, or democracies—rely on varying degrees of repression to control their populations.[45] This is fairly straightforward and widely

[41] The Alliance for Universal Digital Rights (2023). *Securing Our Human Rights in Our Digital World*. [online] Available at: https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/230203_Alliance_for_Universal_Digital_Rights.pdf.

[42] Lähteenoja, V., Dominguez, H., Facchina, M., Westerberg, P., Nkuidje, L., Goodwin, H., Shale Sagar, A., Birchall, C., Blok, J., van Eemeren , A., Ramírez Chico, G., Pérez Batlle, M., Boet Serrano, P., Perrino, M., Portier, F. and Manso, J. (n.d.). *Digital Rights Governance Framework*. [online] UN Habitat for a Better Urban Future. Available at: https://citiesfordigitalrights.org/sites/default/files/DIGITAL%20RIGHTS%20FRAMEWORK_CONCEPT%20FOR%20FEEDBACK.pdf.

[43] United Nations Office on Drugs and Crime (2016). *Privacy and Security*. [online] Available at: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-10/key-issues/privacy-and-security.html [Accessed 14 Jun. 2025].

[44] Hagar Shezaf and Jacobson, J. (2018). *Revealed: Israel's cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays - Israel News*. [online] Haaretz.com. Available at: https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000 [Accessed 13 Aug. 2025].

[45] Davenport, C. (2007). State Repression and Political Order.

documented in academic literature: When states' grip on power slips or they perceive a threat to their power, they repress.[46]

Repression is commonly conceptualized through physical violence, like kidnapping, torture, and extrajudicial killings, but it takes many forms. As a generalized concept, it can be thought of as threatened or actual measures taken to impose costs on an individual to prevent politically undesirable ideologies from forming or actions from taking place (Goldstein 1978).[47]

Some academics argue that repression occurs more in autocracies than democracies because it is more politically costly in a democracy. As the theory goes, democratic institutions make repression harder for democrats because repressed people can vote their repressors out of power. As Davenport (2007) argues, they permit individuals to challenge those in power.[48] Repressive tactics of governance, at their core, are a form of control, and historically appear to have been used more by autocracies than democracies.[49] In 2025, nearly every country in the WANA region is autocratic.[50]

In *The Rise of Digital Repression* (2021), Steven Feldstein points out that autocracies rely on what Levitsky and Way (2010) call low-intensity coercion tactics: harassing the opposition, imposing widespread surveillance, detaining dissidents, and obstructing people standing in the way of those in power.[51] [52] Today, repression is also very often digital, and tools of digital repression help states execute low-intensity coercion.

Feldstein conceptualizes digital repression as a series of digital maneuvers that assist with more traditional forms of physical repression. He breaks digital repression down into five categories: online censorship, social manipulation and disinformation, internet shutdowns, targeted persecution of online users, and surveillance. Spyware is a tool of surveillance.

Spyware's Role

Spyware is used more specifically for targeted surveillance, or surveillance that involves digital intrusion to compromise confidentiality and access user information (Feldstein 2021). Spyware functions as a tool of low-intensity coercion—it clandestinely surveils and gathers

[46] Davenport, C. (2007). State Repression and Political Order.
[47] Goldstein RJ. 1978. *Political Repression in Modern America: from 1870 to the Present.* Cambridge, MA: Schenkman
[48] Davenport, C. (2007). State Repression and Political Order.
[49] Møller, J. and Skaaning, S.-E. (2013). Autocracies, democracies, and the violation of civil liberties. *Democratization*, 20(1), pp.82–106. doi:https://doi.org/10.1080/13510347.2013.738863.
[50] Coppedge, M., Gerring, J., Knutsen, C.H., Lindberg, S.I., Teorell, J., Altman, D., Angiolillo, F., Bernhard, M., Cornell, A., Fish, M.S., Fox, L., Gastaldi, L., Gjerløw, H., Glynn, A., Good God, A., Grahn, S., Hicken, A., Kinzelbach, K., Krusell, J., Marquardt, K.L., McMann, K., Mechkova, V., Medzihorsky, J., Natsika, N., Neundorf, A., Paxton, P., Pemstein, D., von Römer, J., Seim, B., Sigman, R., Skaaning, S-E., Staton, J., Sundström, A., Tannenberg, M., Tzelgov, E., Wang, Y-t., Wiebrecht, F., Wig, T., Wilson, S. and Ziblatt, D. (2025) V-Dem [Country-Year/Country-Date] Dataset v15. Varieties of Democracy (V-Dem) Project. doi: 10.23696/vdemds25.
[51] Levitsky, S. and Way, L.A. (2010). *Competitive Authoritarianism: Hybrid Regimes After the Cold War*.
[52]Feldstein, S. (2021). *The Rise Of Digital Repression : How Technology Is Reshaping Power, Politics, And Resistance*.

information on an individual or organization deemed to be committing acts that are dangerous to the state. Spyware companies' marketing strategy identifies their surveillance products as "legitimate" security products. But, as many observers ask: legitimate according to whom? Well, that depends on the government.

As Gomez and Rodriguez (2018), Feldstein and Kot (2023), and Papademetriou (2023) point out, governments justify using mass surveillance and spyware tools with what they deem legitimate use cases—typically fighting crime, combating terrorism, or managing crises.[53] [54] This reinforces spyware's nature as a dual-use product—an item that can be used for both military and civilian purposes.[55] The export of dual-use products is regulated by the Wassenaar Arrangement, a 1996 agreement between 42 states that controls products that could be used to violate human rights (in addition to their more "legitimate" security uses). It was amended in 2013 to include certain variations of surveillance software and deep packet inspection technology. Notably, while the US and UK are signatories (as major exporters of surveillance tech), no country in the WANA region agreed to the arrangement.[56] Israel, which is home to all of this report's CSVs, is notably not a signatory, though it claims some of the agreement's elements were adopted in the Israeli national Defence Export Control Law No. 5766-2007.[57]

However, as the UN special rapporteur on the right to privacy has pointed out, states frequently do not surveil according to any basis of law, as laws specifying legitimate surveillance targets do not exist in many states. In a UN report on the right to privacy in the digital age, the UN is specific in what it defines as legitimate per international law: measures that are used to investigate only "the most serious crimes or threats."[58] [59] In that report, the United Nations demands that states must act so that surveillance is:

1. "*Prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;*
2. *strictly and demonstrably necessary to achieve a legitimate aim; and*
3. *[adhering] to the principle of proportionality, and not employed when less invasive techniques are available or have not yet been exhausted."*[60]

---

[53] Santiago Gomez, E. and Rodriguez Rodriguez, C., 2018. Surveillance Technologies.
[54] Papademetriou, G. (2023). Disrupting Digital Authoritarians.
[55] The European Union (n.d.). *Exporting dual-use Items*. [online] Available at: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en.
[56] Shires, J. (2022). *The Politics of Cybersecurity in the Middle East*. Oxford University Press, p.8.
[57] Dilbary, D. (2019). *Israeli Export Controls and M&A/ Investment Transactions*. [online] Goldfarb Seligman Law Offices, pp.5–7. Available at: https://www.goldfarb.com/pdf1/%D7%9E%D7%A6%D7%92%D7%AA%20%D7%93%D7%A0%D7%99%20%D7%93%D7%99%D7%9C%D7%91%D7%A8%D7%99%20%D7%9C%D7%9B%D7%A0%D7%A1%2010.9.19.pdf [Accessed 10 Aug. 2025].
[58] UN High Commissioner for Human Rights (2018). *A/HRC/39/29: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights*. The United Nations Human Rights Council.
[59] It is important to note here that what ultimately defines an action as a crime or threat can be ambiguous and subjective and varies from state to state.
[60] La Rue, F. (2013). *A/HRC/23/40: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* . The United Nations Human Rights Council.

But state surveillance is used for illegitimate purposes—to spy on dissidents, minority groups, political foes, and others deemed worthy of tracking.[61] The state of government surveillance has worsened to the point where, as the former UN special rapporteur for freedom of opinion and expression bluntly puts it, "States conduct unlawful surveillance without fear of legal consequence."[62] While governments with advanced cybersecurity apparatuses have rich histories of developing their own cyberweapons (like Israel and the United States with Stuxnet[63]), other states actively encourage commercial actors to develop and sell exploits.[64]

As researcher George Papademetriou argues in "Disrupting Digital Authoritarians," there are two reasons motivating state actors to use spyware despite the blatant threat it presents to digital human rights. For one, the sheer number of devices in use around the world presents an undeniable intelligence opportunity to governments: a near-limitless source of information about nearly every person of potential interest.[65] Second, most major technology standards today use end-to-end encryption, and many major technology companies use end-to-end encryption in their products (such as WhatsApp forking Signal's encryption protocol, Apple's iMessage, etc.). This presents a dilemma to governments looking to surveil targets, as most modern encryption algorithms are incredibly difficult to crack. For example, it would take Fugaku, one of the world's most powerful supercomputers, 12 trillion years to crack AES-128, the US government encryption standard for information classified as "secret."[66] [67] [68]

CSVs offer an alternative. Instead of needing to crack widely used end-to-end encryption algorithms and decrypt data in transit between users, governments can instead use spyware to gain control of a device receiving encrypted communications.[69] After all, once encrypted communications reach an end user's application—Signal, WhatsApp, or iMessage—they are decrypted so the user can read and interact with them.[70]

In addition, purchasing and using spyware created by CSVs allows governments to distance themselves publicly from the spyware product itself and claim some degree of plausible deniability. This was on bright display when the US Department of Commerce sanctioned

[61] Dunja Mijatović (2023). *Highly Intrusive Spyware Threatens the Essence of Human Rights.* Council of Europe Human Rights Comment. https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights.
[62] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2019). *A/HRC/41/35: Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. The United Nations Human Rights Council.
[63] Britannica (2024). Stuxnet | Computer Worm. In: *Encyclopedia Britannica*. [online] Available at: https://www.britannica.com/technology/Stuxnet.
[64] Nicole Perlroth (2021). *This Is How They Tell Me The World Ends: The Cyber-Weapons Arms Race*, 389–90.
[65] Papademetriou, G. (2023). Disrupting Digital Authoritarians.
[66] Proton Team (2021). Privacy Decrypted #3: Can encryption be broken? *Privacy guides*. Available at: https://proton.me/blog/can-encryption-be-broken.
[67] Lynn Hathaway (2003). *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*. The National Institute of Science and Technology.
[68] "Top secret" intelligence requires either AES-192 or AES-256 encryption.
[69] Papademetriou, G. (2023). Disrupting Digital Authoritarians.
[70] Collier, K. (2025). *Why Signal, the App at the Center of the Leaked Yemen Strikes Messages, Can Leave the Door Open for Hackers*. [online] NBC News. Available at: https://www.nbcnews.com/tech/security/signal-app-used-hegseth-can-leave-door-open-hackers-rcna197956 [Accessed 14 Jun. 2025].

Israeli CSV NSO Group over its flagship spyware Pegasus, even though the United States secretly purchased a contract with NSO Group five days before announcing these sanctions.[71] This type of usage creates a supply-and-demand cycle for spyware and motivates CSVs to develop more.

When enough evidence has been documented by those operating spyware, such acts can be handled with more traditional forms of repressive violence. Ultimately, it is not a coincidence that nearly every country in the WANA region is autocratic and has been caught using—or is associated with using—spyware. Spyware, as an advanced tool of low-intensity coercion, helps governments repress their populations.

How Spyware and CSVs Work

One way to think about how spyware works is by analyzing its "kill chain"—the series of actions that enable the malware to successfully exploit a device and exfiltrate data. Defense manufacturer Lockheed Martin popularized this idea by creating the Cyber Kill Chain, a way of analyzing cyberattacks that breaks an attack down into reconnaissance, weaponization, delivery, exploitation, installation, command and control, and achievement of objectives.[72]

Threat intelligence researchers at Google's Threat Analysis Group break down spyware's kill chain into five distinct phases:

1. Delivery to targeted user: How CSVs deliver their malware kill chain, such as through an email, a WhatsApp message, or a text.
2. Exploitation: How attackers take advantage of software flaws to access data on a targeted device.
3. Installation of spyware: How attackers gain full (root) access to a device and secretly download the spyware.
4. Gather information: How spyware surveils the victim, gathers information, and collects data.
5. Exfiltration of data: How attackers remotely control the device and ultimately send collected data back to themselves.[73]

Through these five phases, spyware steals victims' data. From what we understand from Citizen Lab reports, CSV-exported spyware such as NSO Group's Pegasus, or QuaDream's Reign and Kingspawn, can track users, access messages on various messaging apps, record from the microphone and front and back cameras, and exfiltrate other types of information. As Fortinet highlights, mobile device spyware can access virtually all information on a user,

[71] U.S. Department of Commerce (2021). *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*. [online] U.S. Department of Commerce. Available at: https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [Accessed 11 Aug. 2025].
[72] Lockheed Martin (2025). *Cyber Kill Chain*. [online] Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[73] Google Threat Analysis Group (2024a). *Buying Spying: Insights into Commercial Surveillance Vendors*. [online] p.16.

including call logs, browser history, GPS tracking, microphone and photo use, and keystrokes.[74]

Some popular types of spyware are adware, infostealers, keyloggers, rootkits, Red Shells, system monitors, cookie trackers, and Trojan horses.[75] All types of spyware spy on a user without their consent to exfiltrate data for the attacker. While most spyware targets Windows and Android devices due to their global market dominance (Android has a global market share of 71.88%[76] and Windows has a global market share of 72% in 2025[77]), some spyware variants also target Apple or Linux devices. An infamous example highlighting this occurred in 2016, when Citizen Lab reported that the UAE purchased Pegasus from NSO Group and used iPhone iOS exploits to target human rights defender Ahmed Mansoor.[78]

Spyware is sold much like other forms of software. A firm creates a product, markets it, meets with clients to demonstrate how it works, and sells it contractually. However, because spyware vendors specialize in software that functions as a cyberweapon and sell their products to state actors who often violate human rights, these companies operate a little differently.

Spyware vendors operate in a cycle of three main stages:[79]

1. Obtain exploits by identifying vulnerabilities and developing them, or purchasing exploits from suppliers.
2. Create a surveillance product based on those vulnerabilities or exploits.
3. Market and sell finished spyware products to customers (primarily governments).

Researchers at Google's Threat Analysis Group found in 2024 that 50% of known zero-day exploits targeting Google devices and products were created by spyware companies.[80] However, there is no way to know how many of these products were developed in-house versus purchased through a different third-party vendor. Like the commonly described cat-and-mouse game between threat actors and cybersecurity researchers, spyware vendors are constantly purchasing or researching new vulnerabilities and exploits as major technology companies patch exploits.

---

[74] Fortinet (2024). What Is Spyware? Definition, Types, and Protection.
[75] Fortinet (2024). What Is Spyware? Definition, Types, and Protection.
[76] Sherif, A. (2025). *Market share of mobile operating systems worldwide from 2009 to 2025, by quarter*. [online] Available at: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/.
[77] Sherif, A. (2025). *Global market share held by operating systems for desktop PCs, from January 2013 to March 2025*. [online] Available at: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/.
[78] Marczak, B. and Scott-Railton, J. (2016). *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*. [online] *The Citizen Lab*. Available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.
[79] Google Threat Analysis Group (2024). Buying Spying: Insights into Commercial Surveillance Vendors. [online] p.11. Available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.
[80] Google Threat Analysis Group (2024). The Next Step in our Fight against Spyware. *The Keyword*. Available at: https://blog.google/outreach-initiatives/public-policy/spyware-amicus-brief/ [Accessed 10 Aug. 2025].

1.3 Glossary

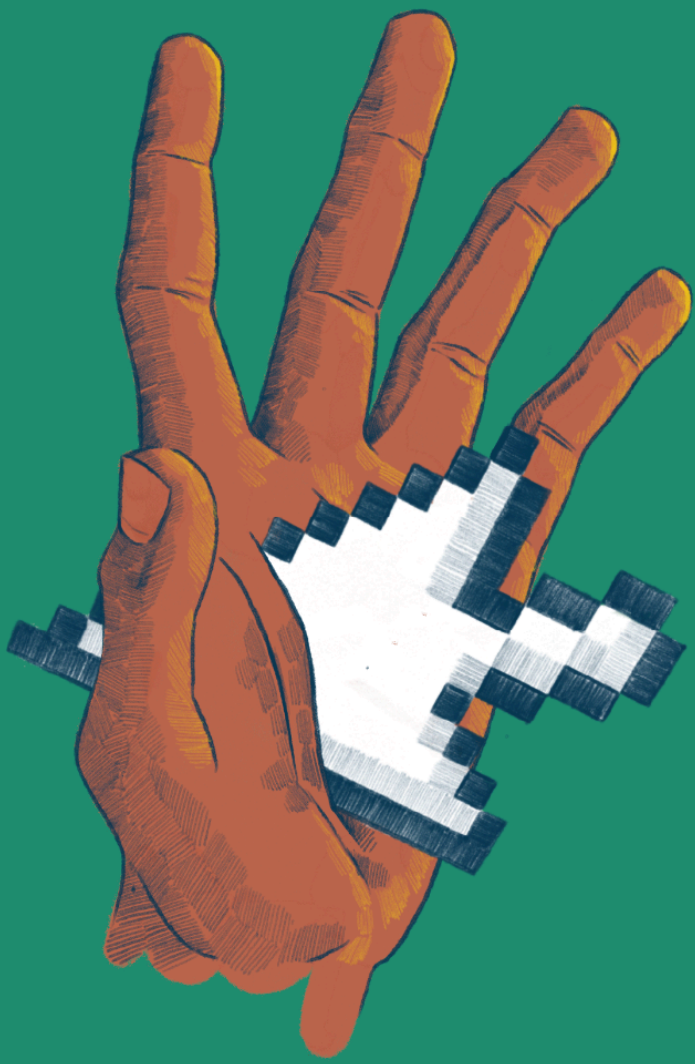
Table 1: Glossary

Commonly used cybersecurity terms throughout this report.

Term ▲	Definition
CSV	A commercial suveillance vendor. A company that creates, markets, and/or sells spyware or similar technologies.
Dual-use exports	A product that can be used for civilian and military purposes. Spyware is a dual-use product. The export of dual-use products is regulated by the 1996 Wassenaar Arrangement. Amnesty International defines dual-use items as also being "a product with a high level of technological capabilities and security risks."
Exploit	A program that takes advantage of a vulnerability on a computer or within a computer system.
Holding company	A company that owns in part or wholly a stake in another company. Holding companies control their subsidiaries.
Kill chain	A chain of actions that enable malware to successfully infect a device.
Malware	A portmanteau of malicious software. Malware broadly describes malicious software that aim to harm a user/their devices.
Network injections	A technique in which threat actors gain access to victims through manipulated data packets "injected" in the target's internet traffic to obtain some goal, such as blocking/intercepting/manipulating traffic.
Single-click exploit	A threat vector that requires some sort of action from a target to enable a malware's kill chain. A common example is a malicious link.
Spyware	A portmanteau of spying and malware, spyware is a form of malware that surveils victims without them knowing.
Threat vector	Often used interchangeably with attack vector, threat vectors are the methods threat actors use to breach a target's infrastructure.
Vulnerability	A vulnerability can be thought of as a digital security flaw.
WANA region	The West Asia and North Africa (WANA) region is a geographic term used to in part to avoid the colonial legacies of terms like the “Middle East.” The WANA region includes Algeria, Bahrain, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, Turkey, the United Arab Emirates, Western Sahara, and Yemen.
Zero-click exploit	A threat vector that requires no action from a target to enable a malware's kill chain. Zero-click exploits use the internet and typically take advantage of vulnerabilities in mobile apps, such as WhatsApp.
Zero-days	Zero-days, or zero-day vulnerabilities, are a kind of vulnerability that is unknown to a software developer and has no known fix. Zero-day exploits use zero-days to target systems with this kind of software flaw.

Table: SMEX • Source: Amnesty International Security Lab's Glossary; Cisco's "What is an Exploit?"; Crowdstrike's "What are Attack Vectors,"; Malwarebytes' "What is Malware?" • Created with Datawrapper

Part 2: Methdology



2.1 Data Sources and Scope

This report aims to shed more light on the types of spyware employed by some of the largest purveyors of spyware in the WANA region. But how does one decide which CSVs qualify? Researching CSVs and spyware is inherently tricky due to the secretive nature of spyware vendors. Because they sell to state actors and are subject to export controls in many countries due to their dual-use nature, CSVs typically operate with secrecy and have intentionally complex corporate relationships. Consequently, not much is known about which CSVs operate where.

Feldstein and Kot (2023) were some of the first researchers to combat this trend, creating datasets cataloguing and tracking major global spyware incidents from 2011 through 2023. Feldstein and Kot created their datasets from findings by news outlets, whistleblowers, watchdog organizations, and international human rights defenders such as Amnesty International, Citizen Lab, Human Rights Watch, and SMEX. Citizen Lab at the University of Toronto is one of the leading research labs that has helped us better understand spyware. It has released several reports exposing the activities and tactics, techniques, and procedures associated with CSVs across the WANA region, including most famously Pegasus and NSO Group, but also Hacking Team, Paragon, Cytrox, and QuaDream.[81] [82] Publicly available information offers a path toward better understanding what spyware has been used and where. This report follows in Feldstein and Kot's footsteps and relies on data reported or categorized by major watchdog and human rights organizations—including Amnesty International, Citizen Lab, the Carnegie International Endowment for Peace, and Human Rights Watch—in addition to tracking reputable news outlets, court documents, and corporate records. Lastly, SMEX interviewed several victims targeted by spyware/malware who contacted its Digital Safety Helpdesk. In doing so, this research asks: What major CSVs operate in the WANA region?

Since Feldstein and Kot last updated their catalogue of spyware incidents in early 2023, this paper will build on their dataset by looking at instances of publicly deployed spyware from early 2023 to 2025 in the WANA region. The WANA region ranges from Morocco, West Sahara, and Mauritania to Egypt, Sudan, Djibouti, and Somalia in Africa, to the Gulf states, the Levant, Iraq, and Turkey to the north.[83] This report analyzes active spyware vendors whose spyware has reportedly been deployed by countries in the WANA region the most frequently. This report estimates CSV activity through reported spyware incidents to approximate which vendors appear most active—that is, which appear to have more contracts, greater revenue, and more targets. In descending order, these are as follows.

---

[81] Siena Anstis (2018). Litigation and other formal complaints related to mercenary spyware - The Citizen Lab. [online] The Citizen Lab. Available at: https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ [Accessed 14 Jun. 2025].

[82] Marczak, B., Scott-Railton, J., Perry, A., Aljizawi, N., Anstis, S., Panday, Z., Lyon, E., Abdul Razzak, B. and Deibert, R. (2023). Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers. [online] The Citizen Lab. Available at: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[83] In total, this includes Algeria, Bahrain, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, Oman, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, Turkey, the United Arab Emirates, Western Sahara, and Yemen.

Table 2: Most Active CSVs in SWANA Region

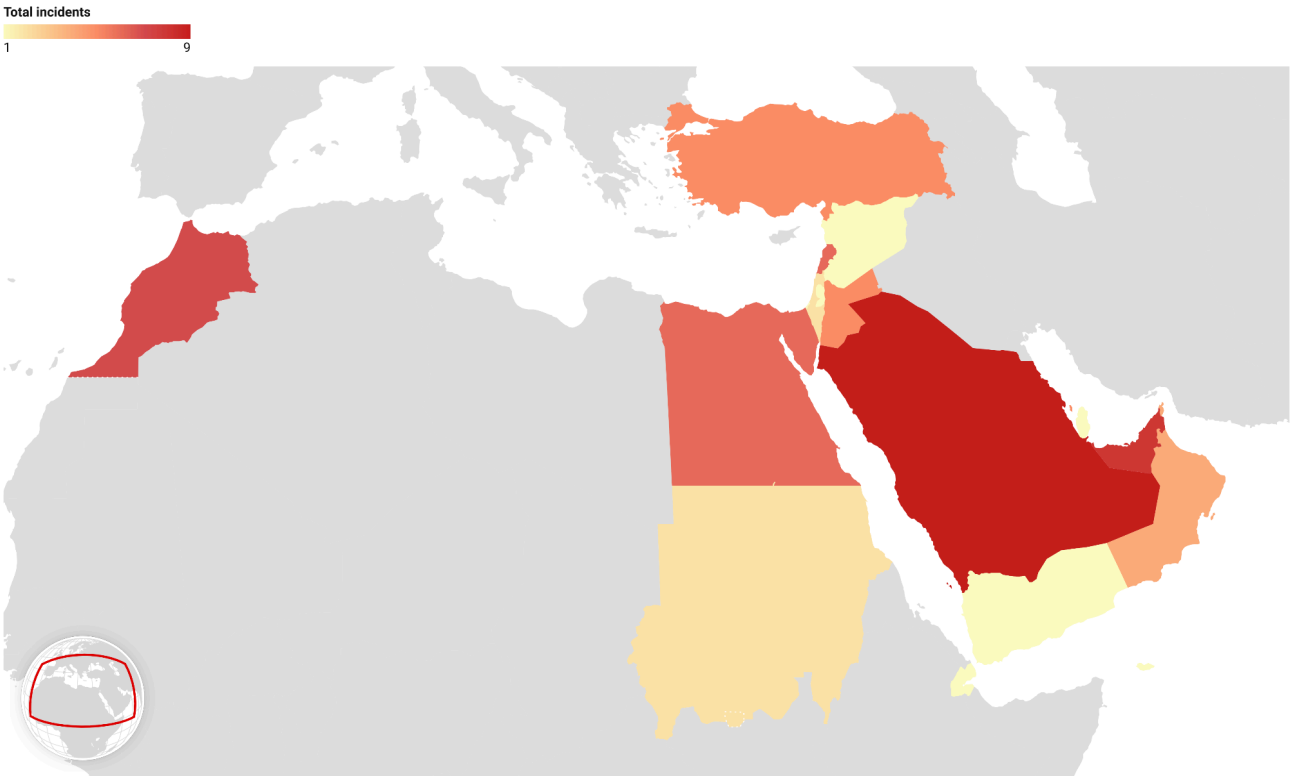
Commercial surveillance vendor ▲	Number of SWANA countries suspected of being customers	Number of employees	Annual Profit	Number of customers across the world
Cellebrite	At least 5	1,167 as of 2024	$56.9 million in 2024	Customers in more than 100 countries
Cytrox/Intellexa	At least 4	26 in 2021 via Thalestris	$7,649,829 in 2021	At least 14; the US Treasury claims it has a “global” customer base
NSO Group	At least 12	Approximately 350 in 2025	Allegedly -$12 million in 2024	54 customers in 31 countries as of 2024
Saito Tech	At least 6	Between 70 and 150	$20 million in 2017	Customers in over 60 countries, as of 2017

Sources: "WhatsApp Inc. v. NSO Group Technologies Limited," NSO Group's 2024 Transparency and Responsibility Report, Feldstein and Kot's "Why Does the Global Spyware Industry Continue to Thrive?," US Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium, and "Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed" •

Annual profit in this table records the most recent reporting for each respective company's or group's profit in a given year.

Number of Spyware Incidents per WANA country from 2011-2025

This map displays the number of publicly reported spyware incidents in the West Asia and North Africa (WANA) region from 2011-2025. Spyware incidents are defined according to the European Digital Rights' definition of spyware, explicated in section 2.4 in this report.



This dataset was built using data reported by major watchdog and human rights organizations (e.g. Amnesty International and the Citizen Lab), reputable news outlets, court documents, and corporate records.

Map: SMEX • Source: SMEX • Created with Datawrapper

2.2 Limitations

There are several limitations with this approach, primarily due to its reliance on publicly available information. Whenever possible, this report aims to verify findings with at least two sources across different media. For data on spyware infections, SMEX relied on reports published by expert threat labs, such as Citizen Lab, and Amnesty International's Security Lab. For company information, SMEX relied mainly on primary official sources (e.g., corporate registries, legal filings). In limited circumstances where official information was not publicly accessible, SMEX used reputable third-party data aggregators.

However, some large CSVs operating in the region still nevertheless may not be included due to a lack of publicly available and verifiable information (for example, Paragon). Some information is simply not currently available or verifiable. Common examples include:

- Ownership of companies in low-transparency jurisdictions (e.g., the British Virgin Islands), unless divulged in legal proceedings or corporate disclosures in other more transparent jurisdictions.
- Procurement filings confirming any given WANA government's purchase of a specific spyware tool.
- Export licences obtained by CSVs.

In addition, this strategy may result in a chicken-or-egg identification scenario, in which it is unclear whether the CSVs being analyzed are operating the most frequently in the region or whether they are simply being caught the most. In other words, are they truly operating more than other firms in the region and getting reported on because they target more victims, or are they sloppier and getting caught more frequently because they make preventable mistakes? Both are possible. A good example of the latter happening is when Amnesty International released a report in 2021 in which it claimed NSO Group made several operational security errors that enabled Amnesty to develop a forensic method for identifying Pegasus spyware.[84]

Spyware incidents are often geographically identified by researchers associating indicators of compromise with certain geographies, such as DNS server locations. This can lead to some uncertainty when identifying where spyware is being used. As Citizen Lab explained in its 2018 report on 45 countries with suspected Pegasus infections, Pegasus operators using VPNs or satellite internet connections may produce inaccuracies in how infections had been attributed to specific countries.[85] In addition, as noted throughout this report, some CSVs sell add-ons for customers to target victims in different countries. Thus, while this report aims to use multiple data sources to better identify potential spyware operator locations, it cannot with perfect accuracy identify which countries are using a CSV's spyware.

It is ultimately unclear which vendors truly operate with the greatest footprint in the region and have the most clients and contracts. This is worth further investigation. Because data is so scant in the field, this report operates under the assumption that publicly reported spyware incidents are a proxy for estimating which CSVs are most active in the region. While

[84] Amnesty International Security Lab (2021). *Forensic Methodology Report: How to Catch NSO Group's Pegasus*. [online] Amnesty International. Available at: https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

[85] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). *HIDE AND SEEK*.

this report's authors updated Feldstein and Kot's findings whenever possible, the report is by no means exhaustive or a complete list of all spyware incidents and vendor activity in the WANA region.

2.3 Goals of This Report

This paper aims to accomplish three main objectives.

1. To catalogue spyware incidents from 2011 to 2025. Feldstein and Kot (2023) were the first researchers to catalogue major spyware incidents across the world. They last updated their catalogue in 2023. Additionally, no major research report has emerged analyzing which CSVs operate more in the WANA region based on incident reports. This report aims to update Feldstein and Kot's work concerning WANA countries and catalogue major spyware incidents across the WANA region. Extrapolating from that information, this report will analyze the CSVs that appear to be operating more aggressively in the region.
2. To add novel contributions to the public's understanding of how these CSVs operate, with support from FIND.
3. To show the human toll of spyware through interviews SMEX has conducted with its victims. Spyware violates fundamental human rights, and this report sheds light on what that means day-to-day for journalists, human rights defenders, and dissidents.

2.4 Notes and Definitions

Looking at incidents from 2011 to 2025, several important notes must be made. First, several of the most prolific and/or infamous CSVs operating in the WANA region, such as FinFisher and QuaDream, are no longer active and thus are not being analyzed.[86] Second, it is noteworthy that while Memento Labs is tied for appearing the second-most in this dataset, its last publicly reported incident occurred in 2015. If this report analyzed different disclosure years, Memento Labs would appear less often (for example, once during 2015 to 2020 or no times from 2020 to 2025). More information on why this report's authors are not including Memento Labs is provided in Appendix A.
To more precisely document what qualifies as a spyware incident, this research defines spyware according to the definition of the European Digital Rights (EDRi) consortium of NGOs, as of June 2025. Spyware is "...software that meets the following conditions:

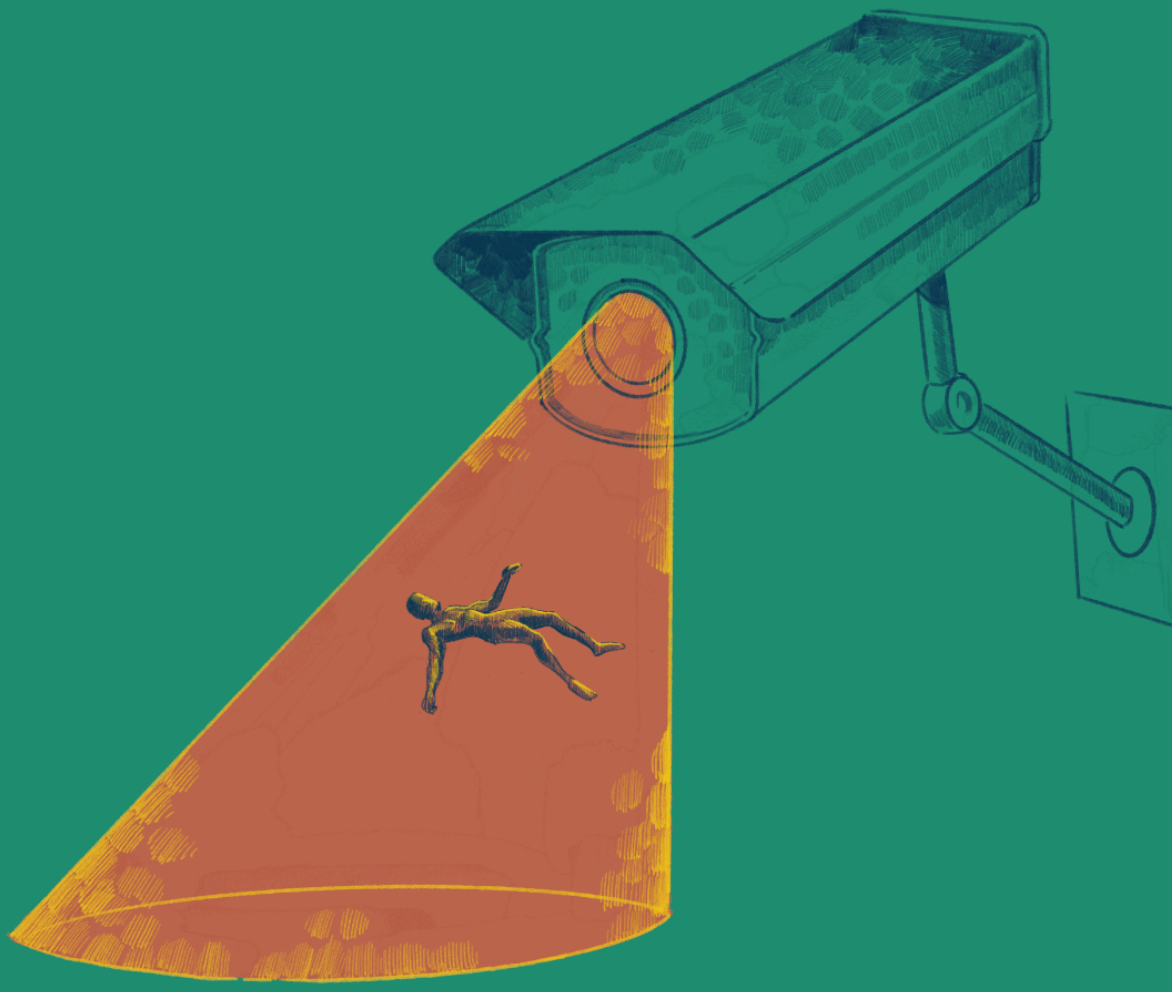
1. It is installed or run on a device without the free and informed consent of [an end-user];
2. It compromises the integrity of the device;

[86] Based on public reports, FinFisher was the second most used commercial spyware vendor in the region, but in 2022 shut down over legal troubles tied to human rights abuses. QuaDream also operated to great infamy in the WANA region over the past half decade, but shut down after controversies emerged surrounding its activity in 2023.

3. Its deployment is primarily facilitated by exploiting existing or created vulnerabilities in digital systems;
4. After installation, its operation is performed either automatically or remotely;
5. And it can be targeted at individuals or groups, or deployed indiscriminately."[87]

While Cellebrite does not technically sell spyware as such based on this definition, this paper includes it for several key reasons. As the EDRi highlights, Cellebrite's premier product, the Universal Forensics Extraction Device (UFED), meets almost all conditions of the EDRi spyware definition, except for enabling continuous exfiltration of data after being installed. UFED requires physical access to a device, though it offers solutions to remotely control data exfiltrated from devices.[88] However, like many spyware products, Cellebrite's "forensics tools" exploit vulnerabilities to gain access to devices and can create functional copies of victims' entire digital identity—their messages, files, and communications, even on encrypted messaging apps. Furthermore, Amnesty International documented multiple instances of Cellebrite customers in Serbia in late 2024 using UFED products to gain illicit access to victims' phones without due process and then installing the NoviSpy spyware on their phones.[89] Consequently, Cellebrite is within the scope of this report.

[87] Berthélémy, C., Lund, J., Le Querrec, B., Ristic, A., Hammoud, R., Neyenhuys, L., Lichtenthäler, H., Zenger, R., Nakyama Shapiro, M. and van Holst, W. (2025). *Spyware and State Abuse: The Case for an EU-Wide Ban*. European Digital Rights (EDRi), p.https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/.
[88] Cellebrite.com. (2024). *Inseytes by Cellebrite*. [online] Available at: https://cellebrite.com/en/cellebrite-inseyets/ [Accessed 12 Jul. 2025].
[89] Amnesty International. (2024). *Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*. [online] Available at: https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/ [Accessed 3 Aug. 2025].



Part 3: Finidings: CSVs of Interest

Spyware companies often seek to hide their actions, client lists, and technological capabilities behind shell companies, nondisclosure agreements, and complex corporate structures.[90] [91] As Bansal et al. (2024) at the Atlantic Council note, the entities that design and sell spyware to end users often work with partners. Spyware vendors may also operate via subsidiaries, rely on independent investors, use suppliers (such as initial access brokers), and function as part of holding companies. For example, according to research by Amnesty International, NSO Group in 2021 was directly or indirectly connected to at least four individual shareholders, thirteen holdings companies, and 12 subsidiaries across multiple jurisdictions.[92] These dendritic relationships become intentionally confusing, and firms often strategically change their names and extend their operations beyond international borders to avoid stricter regulations.

Upon expanding Feldstein and Kot's (2023) dataset and analyzing the past several years of spyware incidents in the WANA region, SMEX observed a few key trends among these companies:

1. NSO Group was implicated most frequently in spyware incidents in this dataset, followed in descending order of frequency by Saito Tech, Cellebrite, and Cytrox/Intellexa.
2. CSVs based in Israel appear to dominate the market in the WANA region, though others also exist, like MSAB from Sweden, RSC Labs from Italy, and Meiya Pico from China.
3. Key players that once dominated the market in the WANA region, like FinFisher and Hacking Team (now Memento Labs), no longer appear to have as large a share of the market, measured by public reports of their spyware being used by governments in the region.
4. The United Arab Emirates and Saudi Arabia were implicated the most in reported spyware incidents: *at least eight each*. Morocco (seven reported incidents), Egypt (six), Bahrain (five), and Jordan (five) were all regularly reported on as likely CSV customers.
5. Some lesser-known CSVs also appeared in the dataset. More research is needed into smaller, boutique CSVs.

In the following four subsections, this report analyzes the top CSVs in this report's dataset: NSO Group, Cytrox/Intellexa, Cellebrite, and Saito Tech (Candiru).

---

[90] Roberts, J., Herr, T., Bansal, N. and Messieh, N. (2024). *Mythical Beasts and Where to Find them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. [online] The Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#methods.

[91] Horak, G. (2023). *Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa*. [Master's Thesis] Available at: https://dash.harvard.edu/server/api/core/bitstreams/cb8802b2-a4c2-4733-8229-cb0495f0c3dc/content [Accessed 10 Aug. 2025].

[92] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: inside NSO Group's Corporate Structure*. [online] p.58.

3.1 NSO Group

"[Pegasus is] analogous to a traditional wiretap… tailored to the modern world's use cases… [It] is not a mass surveillance tool."

—NSO Group in its 2024 Accountability and Responsibility Report

Company Structure and Finances

Niv Karmi, Shalev Hulio, and Omri Lavie founded NSO Group Technologies Ltd. in 2010 in Israel (corporate ID: 514395409).[93] The three founders claim they created the company to develop technology products for law enforcement agencies and governments to tackle crime and prevent terrorism.[94] Hulio once noted that an initial goal of NSO Group was to provide law enforcement and intelligence agencies with the means to bypass encryption and gain access to desirable mobile devices to fight crime.[95] [96] This is brightly on display in NSO Group's 2021 Transparency and Responsibility report, in which it claims "NSO Group was founded…with one key mission: to make the world a safer place."[97] Of course, NSO Group's actions over the past decade have told another story.

Image 1: NSO Group's website logo in 2019.

Since 2010, NSO Group has established its presence through entities in the British Virgin Islands, Bulgaria, the Cayman Islands, Cyprus, Luxembourg, the Netherlands, the United Kingdom, and the United States. Over time, many of these entities have been restructured, liquidated, or changed ownership under different investors. NSO Group began offering its first iterations of Pegasus in 2011.[98]

---

[93] NSO is an initialism for the founders' names.
[94] NSO Group (2021). *About Us*. [online] Nsogroup.com. Available at: https://www.nsogroup.com/about-us/ [Accessed 3 Aug. 2025].
[95] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: inside NSO Group's Corporate Structure*. p.29.
[96] Note: in general, NSO Group refers to the whole corporate group, while NSO Group Technologies Ltd refers to the flagship entity / operating entity of the group's headquarters in Israel.
[97] NSO Group (2021). *Transparency and Responsibility Report 2021*. [online] Available at: https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [Accessed 14 Jul. 2025].
[98] Bergman, R. and Mazzetti, M. (2022). The Battle for the World's Most Powerful Cyberweapon. *The New York Times Magazine*. [online] 28 Jan. Available at: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [Accessed 10 Aug. 2025].

Francisco Partners Acquisition

In 2014, the private equity firm Francisco Partners acquired a 70% stake in NSO Group for $115 million.[99] Francisco Partners oversaw numerous major structural changes during its control of the NSO Group from 2014 to 2019. At this time, several trading and holding companies became part of a corporate structure associated with NSO Group. This includes:

- L.E.G.D. Company Ltd. based in Israel, which later changed its name to Q Cyber Technologies Ltd. (registration no: 514971522) and became the majority shareholder in NSO Group Technologies.[100] In 2019, NSO Group's website described it as a "Q Cyber Technologies company."[101]
- OSY Technologies S.à r.l. (registration no: B184226), based in Luxembourg[102];
- OSY Holdings Ltd. (registration no: 284745), a holding company based in the Cayman Islands that became the sole shareholder of OSY Technologies S.à r.l.[103]; and
- Q Cyber Technologies S.à r.l (registration no: B203124)., an entity incorporated in Luxembourg on January 8, 2016 with OSY Technologies as its sole shareholder.[104] NSO Group later defined Q Cyber Technologies S.à r.l. in a letter to Amnesty International as a commercial distributor, primarily issuing invoices and receiving payments from customers.[105]

Numerous acquisitions of smaller technology companies in 2014 led Francisco Partners to change NSO Group's structure multiple times, expanding it to include at least 15 international companies across eight jurisdictions.[106] This featured several companies in Cyprus and Bulgaria, including:

- IOTA Holdings Ltd. in Cyprus (registration no: 337445; registered on November 4, 2014[107]), which is the parent company of Cyprus-based CS-Circles Solutions Ltd.;

---

[99] Bloomberg L.P., Francisco Partners III LP current portfolio, retrieved 8 February 2019 from Bloomberg terminal

[100] State of Israel Corporations Authority, Company Incorporation Certificate of L.E.G.D. Company Ltd., 2 December 2013, available as Exhibit 6 to the Complaint, *WhatsApp Inc. v. NSO Group Technologies Limited* [2025] (District Court, N.D. California) Available at: https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/ [Accessed 10 Jul. 2025].

[101] NSO Group. (2019). *About Us - NSO Group*. [online] Available at: https://web.archive.org/web/20190215201627/https://www.nsogroup.com/about/ [Accessed 10 Aug. 2025].

[102] Registre de Commerce et des Sociétés Luxembourg (2014). *Certificate of Registration for Osy Technologies S.à r.l.: 3 February 2014*.

[103] Minutes of Extraordinary General Meeting Held on 1 December 2014. (2014). [online] Triangle Holdings. Available at: www.etat.lu/memorial/2014/C/Html/4019/2014197910.html [Accessed 2 Aug. 2025].

[104] Registre de Commerce et des Sociétés Luxembourg (2016). *Certificate of Registration for Q Cyber Technologies: 12 January 2016*.

[105] Amnesty International (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. [online] *Amnesty International*, p.84.

[106] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. [online] p.31.

[107] IOTA Holdings Ltd. (n.d.). Registration Details for IOTA Holdings Ltd. [online] Available at: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=IOTA+Holdings&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [Accessed 25 Aug. 2025].

- CS-Circles Solutions Ltd. in Cyprus (registration no: 336847, registered on October 15, 2014[108]), which fully owns Cyprus-based CI-Compass Ltd.);
- CI-Compass Ltd. in Cyprus (registration no: 310769, registered on August, 23, 2012[109]);
- Global Hubcom Ltd. in Cyprus (registration no: 323665, registered on July 18, 2013[110]);
- MS Magnet Solutions Ltd. in Cyprus (registration no: 309073, registered on July 10, 2012[111]), which fully owns Cyprus-based MI Compass Ltd.[112];
- MI Compass Ltd. in Cyprus (registration no: 347278, registered on September 24, 2015).
- Circles Bulgaria EOOD[113] in Bulgaria (registration no: 175408771, registered in July 2017[114]), which is owned by Cyprus-based CS-Circles Solutions Ltd.;
- Magnet Bulgaria EOOD[115] in Bulgaria (registration no: 203012611, registered in April 2014, though now dissolved), which is owned by Cyprus-based MS Magnet Solutions Ltd.

All Cyprus-based subsidiaries list Luxembourg lawyer Anthony Levy as their director.[116] Levy is also currently counsel for OSY Technologies S.à r.l.[117] According to Amnesty International, both Bulgarian entities were registered to obtain Bulgaria export licenses, though NSO Group in a letter to Amnesty noted that Magnet Bulgaria was inactive in 2021.[118]

Francisco Partners' ownership of NSO Group was organized through OSY Holdings Ltd. (the holding company based in the Cayman Islands), and the NSO Group network of companies grew to at least 20 companies, trusts, and holding structures by 2017.[119]

[108] OpenCorporates (2025). CS - Circles Solutions Ltd. *OpenCorporates* . [online] Available at: https://opencorporates.com/companies/cy/HE336847 [Accessed 25 Aug. 2025].
[109] OpenCorporates (2025). CI - Compass Ltd. *OpenCorporates*. [online] Available at: https://opencorporates.com/companies/cy/HE310769 [Accessed 25 Aug. 2025].
[110] OpenCorporates (2025). Global Hubcom Ltd. *OpenCorporates* . [online] Available at: https://opencorporates.com/companies/cy/HE323665 [Accessed 25 Aug. 2025].
[111]OpenCorporates (2025). MS Magnet Solutions Ltd. *OpenCorporates* . [online] Available at: https://opencorporates.com/companies/cy/HE309073 [Accessed 25 Aug. 2025].
[112]OpenCorporates (2025b). MI Compass Ltd. *OpenCorporates* . [online] Available at: https://opencorporates.com/companies/cy/HE347278 [Accessed 25 Aug. 2025].
[113] Republic of Bulgaria Ministry of Justice Registry Agency (n.d.). Commercial and Non-Profits Organization Register: Entry for Circles Bulgaria Ltd.
[114] OpenCorporates (2025a). Circles Bulgaria. *OpenCorporates* . [online] Available at: https://opencorporates.com/companies/bg/175408771 [Accessed 25 Aug. 2025].
[115] Republic of Bulgaria Ministry of Justice Registry Agency (n.d.). Commercial and Non-Profits Organization Register: Entry for Magnet Bulgaria Ltd.
[116] Open Corporates. (2025). *Officer search: Anthony Levy*. [online] Available at: https://opencorporates.com/officers/cy?q=ANTHONY+LEVY&user=true [Accessed 14 Aug. 2025].
[117] OSY Technologies S.à r.l. (2025). Commercial Registry Extract. [online] Registre de Commerce et des Sociétés Luxembourg, p.16. Available at: https://gd.lu/rcsl/85HXkB [Accessed 14 Aug. 2025].
[118] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p.34.
[119] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p.58.

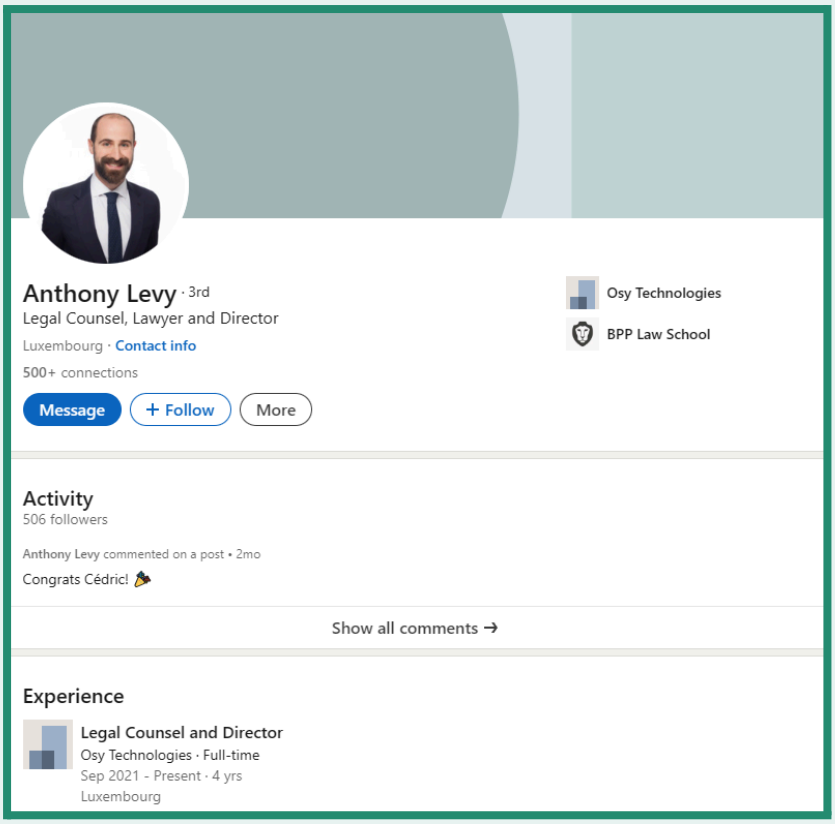


Image 2: Anthony Levy lists his role as Director and Legal Counsel for OSY Technologies S.à r.l. on LinkedIn.[120]

Novalpina Capital Transition

On February 14, 2019, global private equity firm Novalpina Capital bought out Francisco Partners' stake in NSO Group (including subsidiaries and related companies), effectively becoming the new owners of NSO Group and its accompanying structure.[121] [122] Novalpina Capital further changed the group's structure, incorporating an increasingly complex holding company structure across Bulgaria, Cyprus, Luxembourg, and the British Virgin Islands. Notably, ownership of OSY Technologies S.à r.l. was transferred in April 2019 to Luxembourg company NorthPole Newco S.à r.l. (registration no: B230411), which became a key holding company later in 2025.[123] NSO Group at this point acquired at least three subsidiary companies, including Convexum Ltd (registration no: 515495554).[124] Convexum develops anti-drone technology.[125] NorthPole Bidco S.à.r.l. (registration no: B228505), a

[120] Levy, A. (2025). *Anthony Levy's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/anthony-levy-3a664522/
[121] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p.50
[122]Novalpina Capital, NSO Group Acquired by its Management, 14 February 2019, www.novalpina.pe/nso-group-acquired/
[123]Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p.58.
[124] NSO Group purchased or became the majority shareholder of surveillance tech company Wayout; anti-drone tech provider Convexum in 2020; and UK-based PFOS Technologies Ltd., which assists with marketing services.
[125] Orbach, M. (2020). NSO Buys Counter-Drone Company Convexum. *CTech*. [online] 2 Dec. Available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3792634,00.html [Accessed 30 Aug. 2025].

Luxembourg-based holding company NSO Group incorporated into its structure in 2018, acquired Goatilev Ltd. (registration no: 516105657) in February 2020. Goatilev, itself an Israeli holding company, acquired surveillance tech provider Wayout Ltd. (registration no: 515773513) in 2020.[126]

Novalpina Capital also pushed NSO Group to change its governance standards, creating the Governance, Risk, and Compliance Committee to review all potential customers' human rights records.[127] Under Novalpina Capital management, NSO Group introduced new human rights due diligence policies, and began requiring all new customer contracts to include clauses relating to human rights compliance. According to NSO Group's 2021 Transparency and Responsibility report, NSO Group denied contracts worth over $300 million after conducting human rights due diligence review with potential customers.[128] But even if that is accurate, reports emerged a year and a half ago alleging that Pegasus was likely used by the Jordanian government to spy on human rights defenders—a flagrant human rights abuse using NSO Group's products.[129]

At this point, NSO Group's jurisdiction expanded into East Asia too. In CS-Circles Solutions' 2023 financial statement, it claims it owns 100% of an inactive Hong Kong-based subsidiary that made $1,288 in 2023: LI-Trade Company Limited (registration number: 61379026).[130] LI-Trade Company Limited, formerly known as World Faith Trading Limited, was dissolved on December 10, 2021.[131] It is unclear what LI-Trade Company Limited's role was.

By 2020, at least 29 corporate entities, investors, and holding companies were connected with NSO Group.[132] Sky News reported on July 27, 2021, that Novalpina Capital was to be liquidated after internal squabbles led to an irreconcilable dispute between its three

[126] NorthPole Bidco S.à r.l. (2021). *Balance Sheet: Financial Year from 10/05/2018 to 12/31/2019*. [online] Registre de Commerce et des Sociétés Luxembourg, p.19. Available at: https://gd.lu/rcsl/26Qz0v [Accessed 14 Aug. 2025].
[127] Veld, S. in 't (2023). *REPORT of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware*. [online] Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN [Accessed 21 Aug. 2025].
[128] NSO Group (2021b). *Transparency and Responsibility Report 2021*. [online] p. 20. Available at: https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [Accessed 14 Jul. 2025].
[129] Access Now (2024). *Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan* . [online] *Access Now*. Available at: https://www.accessnow.org/publication/between-a-hack-and-a-hard-place-how-pegasus-spyware-crushes-civic-space-in-jordan/ [Accessed 11 Aug. 2025].
[130] PMA & Co Chartered Accountants. (2023) *CS - Circles Solutions Limited Financial Statements: Year Ended 31 December 2023*. Limassol, Cyprus: CS - Circles Solutions Limited.
[131] The Government of the Hong Kong Special Administrative Region (n.d.). Companies Register: Entry for LI-Trade Company. [online] Available at: https://www.e-services.cr.gov.hk/ICRIS3EP/system/home.do [Accessed 25 Aug. 2025].
[132] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p.58.

directors.[133] Ownership of NSO Group changed hands yet again in 2021 to Berkeley Research Group, based in California.[134] By this point, OSY Holdings was removed from the structure.[135]

EY valued NSO Group at $2.3 billion in 2021, but the company soon began to experience a series of financial hits that changed its financial trajectory entirely.[136] This ranged from being publicly valued as worth zero by Berkeley Research Group in 2021, despite EY's valuation;[137] needing emergency infusions of cash from Berkeley worth $10 million in 2021; and being blacklisted by the U.S. Department of Commerce in 2022 in the fallout of discoveries about uses of Pegasus.[138] By the end of 2021, a group of NSO Group creditors publicly wrote in a letter to majority shareholders that NSO Group was insolvent.[139]

Dufresne Holding Ownership and Updated NSO Group Structure

Amid ongoing shakeups and efforts to restructure NSO, news organizations began reporting in March 2023 that Omri Lavie, one of NSO's three cofounders, returned to become its new majority shareholder, as his Luxembourg-based holding company Dufresne Holding S.à r.l. (registration no: B275054), became the owner of a Luxembourg-based holding company that owns NSO Group.[140] Notably, on December 31, 2021, NorthPole Newco S.à r.l. entered a forbearance agreement, beginning a process that transferred preexisting credit and forbearance agreements to Dufresne Holding.[141] On January 25, 2022, NSO Group holding company Goatilev Ltd. and NSO Group subsidiaries Convexum and Wayout entered insolvency proceedings, after which Convexum was sold to Sagitta HoldCo S.à.r.l. (registration no: B268651).[142] On July 18, 2023, Convexum changed its name to Sentry CS Ltd and appears to no longer be affiliated with NSO Group.[143] [144]

---

[133] Kleinman, M. (2021). *Pegasus spyware owner Novalpina to be liquidated after failure to resolve internal bust-up*. [online] Sky News. Available at: https://news.sky.com/story/pegasus-spyware-owner-novalpina-to-be-liquidated-after-failure-to-resolve-internal-bust-up-12365638 [Accessed 11 Aug. 2025].

[134] Srivastava, M., Ortenca Aliaj, Demetri Sevastopulo and Wiggins, K. (2022). *NSO's cash dilemma: miss debt repayment or sell to risky customers*. [online] FinancialTimes. Available at: https://www.ft.com/content/5ef90e5f-1220-4ed6-a650-985272eb0334 [Accessed 11 Aug. 2025].

[135] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p. 49.

[136] Wiggins, K. and Srivastava, M. (2018). *EY valued NSO Group at $2.3bn months before emergency bailout* . [online] FinancialTimes. Available at: https://www.ft.com/content/057cece3-eb81-42b8-9a27-e295c61e76b3 [Accessed 11 Aug. 2025].

[137] Wiggins, K. and Srivastava, M. (2018). *EY valued NSO Group at $2.3bn months before emergency bailout.*

[138] U.S. Department of Commerce (2021). *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*.

[139] Wiggins, K. and Srivastava, M. (2018). *EY valued NSO Group at $2.3bn months before emergency bailout.*

[140] Kirchgaessner, S. (2023). *NSO Group Co-founder Emerges as New Majority Owner*. [online] The Guardian. Available at: https://www.theguardian.com/technology/2023/mar/01/one-of-nso-groups-founders-emerges-as-new-majority-owner [Accessed 11 Aug. 2025].

[141] Kirchgaessner, S. (2023). *NSO Group Co-founder Emerges as New Majority Owner*.

[142] Triangle Holdings (2023). *Balance Sheet: Financial Year from 01/01/2021 to 12/31/2021*. [online] Registre de Commerce et des Sociétés Luxembourg, p.16. Available at: https://gd.lu/rcsl/85HXkB [Accessed 14 Aug. 2025].

[143] Sagitta HoldCo S.à r.l. (2023). *Abridged Balance Sheet: Financial Year from 05/25/2022 to 12/31/2022*. [online] Registre de Commerce et des Sociétés Luxembourg, p.11. Available at: https://gd.lu/rcsl/1NfWvM [Accessed 14 Aug. 2025].

[144] Sentrycs Counter Drone Solutions. (2025). *Technological Alliances - Sentrycs Counter Drone Solutions*. [online] Available at: https://sentrycs.com/partners/technological-alliances/ [Accessed 22 Aug. 2025].

NSO Group Technologies Ltd.'s immediate shareholders are Q Cyber Technologies Ltd. and NSO Group Technologies Ltd—Israeli law allows companies to own its own shares.[145] [146] Q Cyber Technologies is owned by OSY Technologies S.à.r.l. and Omri Lavie.[147] Luxembourg records from 2025 show that the corporate entity NorthPole Newco S.à r.l. is the sole shareholder of OSY Technologies,[148] and NorthPole Newco S.à r.l.'s sole shareholder is Dufresne Holding.[149] Omri Lavie and Anthony Levy are the board members of NorthPole Newco S.à r.l. and listed as professionally residing at 44 rue de la Vallée L-2661, Luxembourg. Omri Lavie is also Dufresne Holding's sole shareholder and board member.[150]

Part of NSO Group's dramatic revenue fluctuations over the past decade are due to numerous scandals, investigations, and reports detailing NSO Group's operations and customers' alleged human rights abuses. While NSO Group had about 350 employees as of April 2025 and made $243 million in revenue in 2020, its current finances look very different..[151] Court records released in May 2025 from a lawsuit filed by WhatsApp show that NSO Group reported making $95.9 million in gross revenues and $84.7 million in gross profit in 2023, with a net operating loss of $12.7 million.[152] In May 2025, a judge ordered NSO Group to pay over $167 million in damages to WhatsApp for its spyware campaigns exploiting the messaging service.[153] And NSO Group still faces a slew of ongoing litigation.

Corporate records from Luxembourg offer some insight into the whole corporate group's current financial state. NorthPole Newco S.à r.l.'s 2024 financial filings show it declared $79,516,731.27 in losses for FY2024, leaving the company with a total of $322,449,975.86 in accrued losses carried forward. The filings do not include detailed profit and loss statements, making it difficult to attribute profit/loss figures to specific entities. However, the figures reflect to an extent the consolidated losses of all of NorthPole Newco S.à r.l.'s undertakings, which includes NSO Group. These losses also are in line with the heavy losses reported by

[145] CheckID (2025g). *N.S.O. GROUP TECHNOLOGIES LTD - 514395409*. [online] CheckID. Available at: https://en.checkid.co.il/company/N.S.O.+GROUP+TECHNOLOGIES+LTD-VBo29GD-514395409 [Accessed 28 Aug. 2025].
[146] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p. 33.
[147] Israeli Corporations Authority (2025). *Company Details Information: Entry for Q Cyber Technologies Ltd*.
[148] Registre de Commerce et des Sociétés Luxembourg (2025). *Company Profile: Entry for OSY Technologies S.à r.l.*
[149] Registre de Commerce et des Sociétés Luxembourg (2025). *Company Profile: Entry for NorthPole Newco S.à r.l.*
[150] Registre de Commerce et des Sociétés Luxembourg (2025). *Company Profile: Entry for Dufresne Holding*.
[151] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025] (District Court, N.D. California) Available at: https://www.courtlistener.com/docket/16395340/747/3/whatsapp-inc-v-nso-group-technologies-limited/ [Accessed 10 Jul. 2025].
[152] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025b] (District Court, N.D. California) Available at: https://www.courtlistener.com/docket/16395340/758/2/whatsapp-inc-v-nso-group-technologies-limited/ [Accessed 27 Aug. 2025].
[153] Franceschi-Bicchierai, L. (2025). *NSO Group Must Pay More than $167 Million in Damages to WhatsApp for Spyware Campaign | TechCrunch*. [online] TechCrunch. Available at: https://techcrunch.com/2025/05/06/nso-group-must-pay-more-than-167-million-in-damages-to-whatsapp-for-spyware-campaign/ [Accessed 9 May 2025].

NSO Group in its 2025 court case against WhatsApp. According to Citizen Lab, there are currently 27 ongoing lawsuits filed against or impacting NSO Group across the world.[154]

Like all Israeli companies exporting "defense articles," NSO Group sales are subject to approval by the Israeli Defense Ministry's Defense Exports Control Agency, which reportedly conducts human rights assessments so that NSO Group products can only be sold to governments using it for "legitimate" purposes.[155] Furthermore, NSO Group claims it is subject to a multilayered regulatory oversight system in which clients must sign end-user certifications that allegedly obligate them to follow international law. NSO Group's compliance team also claims to assess each potential government customer according to a human rights risk matrix, and if a country scores too low, NSO Group will not pursue the opportunity. This has led NSO Group to lower the number of countries it works with to 31 countries, as of 2024.[156]

In 2021, NSO Group identified Bulgaria, Cyprus, and Israel as countries from which it exports its products, apparently with the requisite licences.[157] The company has only admitted to exporting Pegasus from Israel—while NSO Group companies have received export licenses from Cyprus and Bulgaria, there is no evidence that Pegasus (as opposed to other products) has been exported by entities in these countries.[158] In response to letters sent by the Business and Human Rights Research Centre (BHRRC) in 2019, authorities in both Cyprus and Bulgaria denied having granted export licenses to NSO Group, which appears to have been contradicted both the company's own claims in 2021 and—in the case of Bulgaria—official export license registers available online.[159] [160] In NSO's 2024 Transparency and Responsibility report, it just refers to Bulgaria, not Cyprus, as a country in which it faces export regulations.[161] NSO Group's WANA footprint is ultimately seen in its connections to Israel and its military. This report's dataset, based on public reporting, suggests that at least 12 WANA countries have used Pegasus, though Citizen Lab traced suspect Pegasus infections to seventeen countries in the WANA region.[162]

---

[154] Anstis, Siena (2018). *Litigation and other formal complaints related to mercenary spyware - The Citizen Lab*. [online] The Citizen Lab. Available at: https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ [Accessed 14 Jun. 2025].

[155] NSO Group (2024). *Transparency and Responsibility Report 2024*. [online] p.4. Available at: https://web.archive.org/web/20250518154902/https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf [Accessed 25 Jun. 2025].

[156] NSO Group (2024). *Transparency and Responsibility Report 2024.* p.12.

[157] NSO Group (2021b). *Transparency and Responsibility Report 2021*. [online] p. 4. Available at: https://web.archive.org/web/20250408183946/https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [Accessed 14 Jul. 2025].

[158] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p. 82-85.

[159] Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure*. p. 34.

[160] Business & Human Rights Resource Centre (2025). *Novalpina Capital Claims NSO Group Received Export Licences from Bulgaria & Cyprus, but Both States Deny Claims - Business & Human Rights Resource Centre*. [online] Business & Human Rights Resource Centre. Available at: https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/ [Accessed 29 Sep. 2025].

[161] NSO Group (2024). Transparency and Responsibility Report 2024.

[162] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B. and Deibert, R. (2018). *HIDE AND SEEK.*

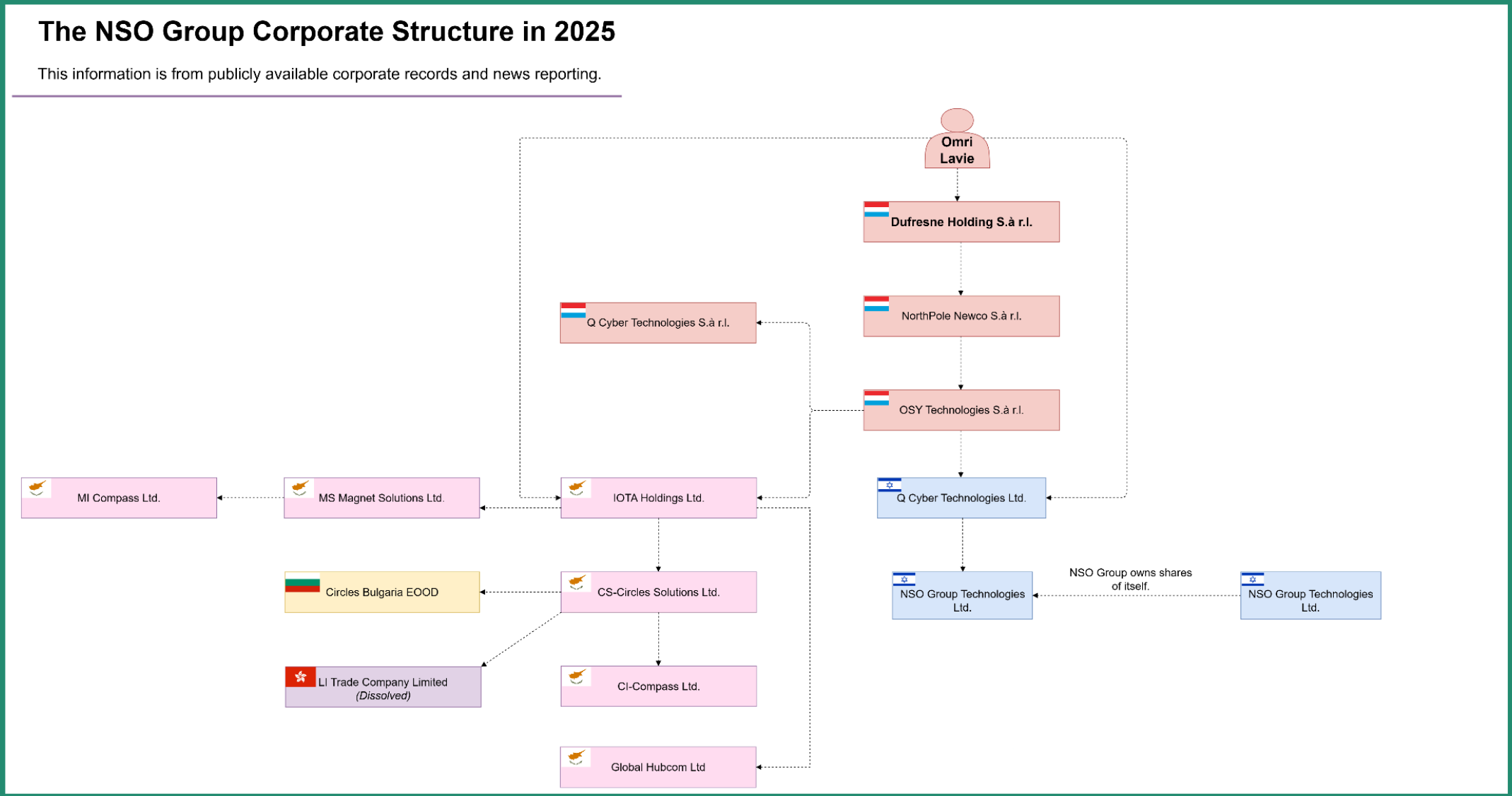


Image 3: NSO Group corporate structure in 2025.

Marketing: "Necessary and Legitimate"

Like many CSVs, NSO Group's marketing strategies involve manufacturing legitimacy and necessity for its products. On its website, NSO Group claims its mission is to create "innovative, ethical cyber-intelligence technologies that empower government agencies to prevent and investigate terror and crime."[163] It claims to follow the four values of accountability, boldness, excellence, and integrity, and notes its products are only used by law enforcement agencies and intelligence agencies.

As researchers Elinor Carmi and Dan Kotliar highlighted in 2024, NSO Group relies on four tactics to legitimize its products: securitization, ethics washing, normalization, and Zionist patriotism.[164] NSO Group's social media posts offer insight into these four tactics. For example, NSO Group frequently posts on LinkedIn about the importance of human rights. On November 20, 2024, NSO Group posted to celebrate World Children's Day, quoting the UN Convention on the Rights of the Child alongside an image of a superhero clad in an NSO Group cape, standing on top of a building and holding a teddy bear.[165]

[163] NSO Group (2021a). *About Us*. [online] Nsogroup.com. Available at: https://web.archive.org/web/20250701175532/https://www.nsogroup.com/about-us/ [Accessed 3 Aug. 2025].
[164] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage. Information, Communication & Society, pp.1–31. doi:https://doi.org/10.1080/1369118x.2023.2245873.
[165] NSO Group. (2024). *November 20th is World Children's Day*. [LinkedIn], November 2024. Available at: https://www.linkedin.com/posts/nso-group_november-20th-is-world-childrens-day-activity-7264944950981578754-WtHN/ [Accessed 28 Aug. 2025].

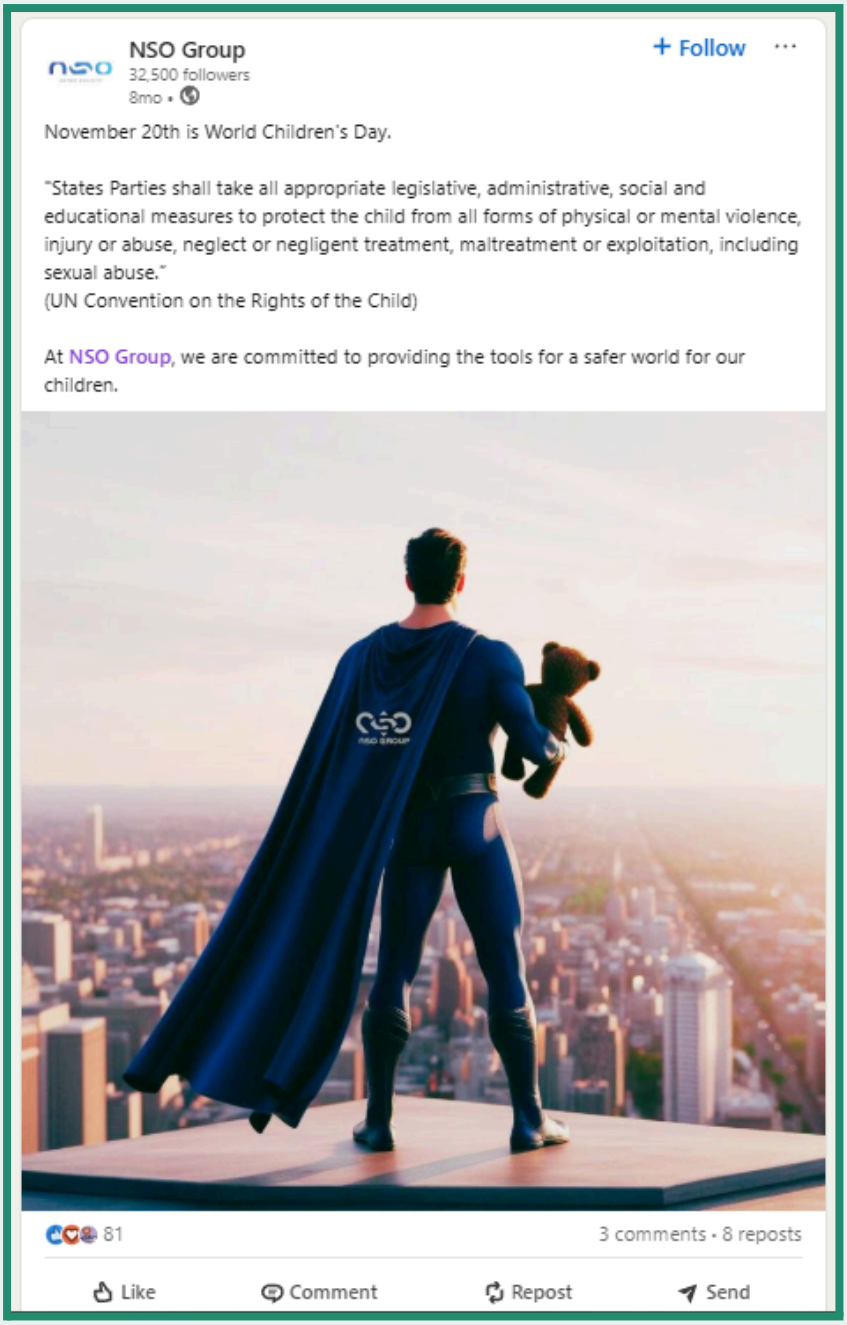


Image 4: NSO Group posts marketing on LinkedIn.

In January 2022 NSO Group posted a series of "Myth Blaster" LinkedIn posts, in which it attempted to dispel rumors about its products. The following is the first of these posts, stating:

#fiction : NSO Group carries out surveillance and has access to all the data that is being collected.
*#fact : We supply our technologies to selected vetted governmental clients, but we *never* operate them ourselves, nor are we exposed to the collected data.*

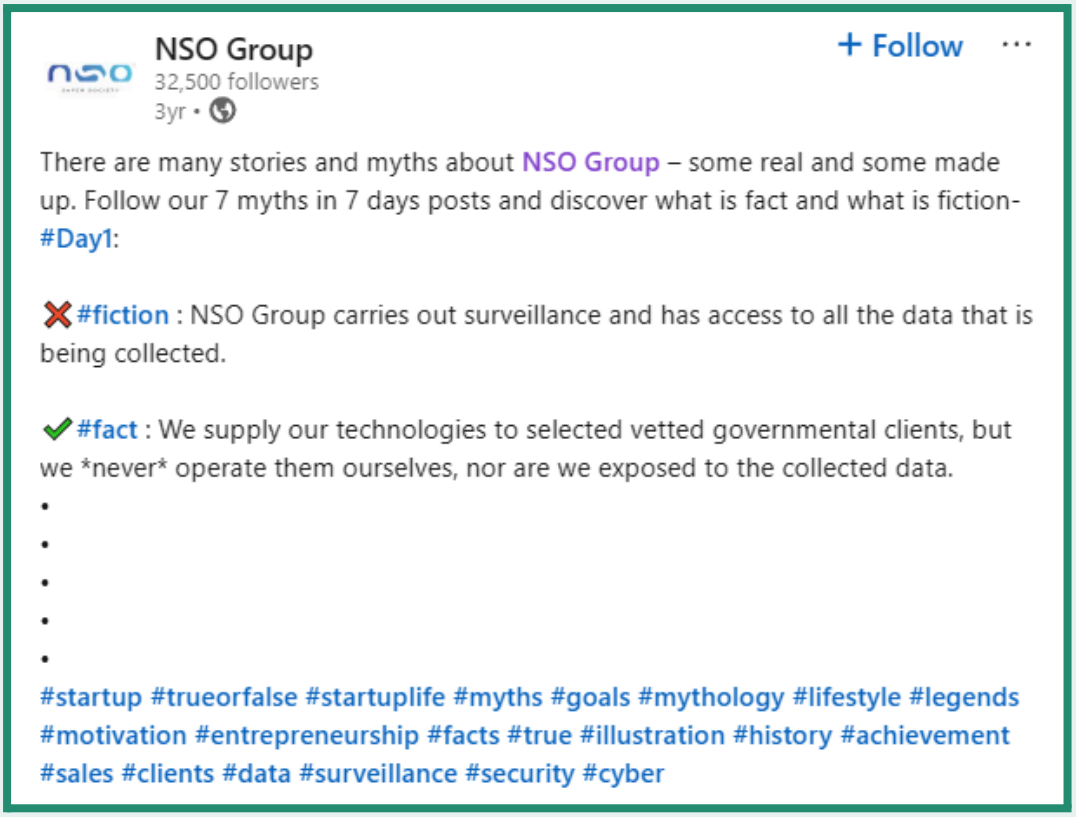


Image 5: NSO Group attempts to bust rumors about its products.[166]

NSO Group frequently describes its products as necessary and legitimate because of their use in catching "pedophiles" and "criminals," as founder Shalev Hulio said in a Washington Post interview in 2021.[167] Carmi and Kotliar (2023) note NSO Group also defaults to describing its offerings vaguely and benignly as "technology".[168] Following its marketing logic, NSO Group cannot be held liable for what its customers do, because it claims it vets all customers for potential human rights abuses, it only sells legitimate technology to legitimate customers fighting crime and terrorism, and it does not have access to what its customers are doing. Put another way: the good guys supply the good guys with good technology.

Carmi and Kotliar (2023) note that NSO Group's social media presence attempts to normalize its image by posting only in English, sharing holiday greetings and photos of employees at parties and conferences, and even celebrating diversity (e.g., with a LinkedIn post celebrating Pride).[169] NSO Group also attempts to normalize its image by marketing other products it sells. Carmi and Kotliar (2023) note that nearly 20% of NSO Group's 2020 posts were about the new anti-drone technology it developed after purchasing Convexum. NSO Group has also moved to market products involving COVID-19 contact tracing, data analytics,

[166] NSO Group. (2024). *Myth Blasters!* [LinkedIn], January 2022. Available at: https://www.linkedin.com/posts/nso-group_myth-blasters-day-6-activity-6889607776767635456-Y8v6/ [Accessed 28 Aug. 2025].
[167] Dwoskin, E. and Rubin, S. (2021). 'Somebody has to do the dirty work': NSO Founders Defend the Spyware They Built. *Washington Post*. [online] 21 Jul. Available at: https://www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/ [Accessed 22 May 2025].
[168] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage.
[169] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage.

and anti–crypto money laundering.[170] [171] In an attempt to humanize employees, NSO Group launched several social media campaigns highlighting the faces and lives of employees, including the "IAMNSO" campaign in 2021.[172]

This is not to say that it is shying away from its primary product. In June 2025, NSO Group posted photos of a celebration of its 15-year anniversary in Prague, including what appears to be a cake topped with a winged horse—a nod to its infamous spyware suite.[173]

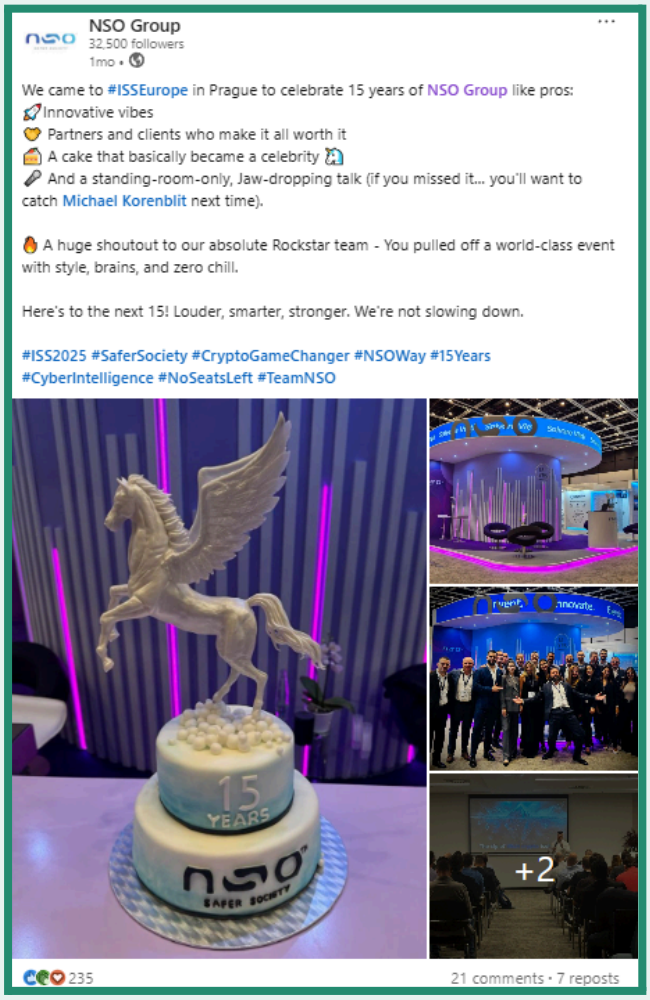


Image 6: NSO Group shares a cake with a Pegasus on top at its 15-year anniversary party in Prague.

NSO Group makes an effort to market its products by attending and/or sponsoring international security conventions, such as Security & Policing in 2020, the 3rd International

[170] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage.
[171] NSO Group. (2025). *Illicit crypto is the engine of global crime and terrorism*. [LinkedIn], May 2025. Available at: https://linkedin.com/posts/nso-group_nsogroup-actionableintel-illicitcrypto-activity-7330597266652655616--v_0/?rcm=ACoAABeY6zUBgiQBDJC-OlTmvQ_cJOLPk7ztqDE/ [Accessed 28 Aug. 2025].
[172] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage.
[173] NSO Group. (2025). *15 years of NSO Group*. [LinkedIn], June 2025. Available at: https://www.linkedin.com/posts/nso-group_isseurope-iss2025-safersociety-activity-7336407248438464512-zNNs?utm_source=share&utm_medium=member_desktop&rcm=ACoAABeY6zUBgiQBDJC-OlTmvQ_cJOLPk7ztqDE [Accessed 25 Aug. 2025].

Security Symposium, or different iterations of ISS World. NSO Group was the lead sponsor of ISS World Europe in 2025.[174] [175]

In its marketing, NSO Group also clearly ties its corporate identity to strong elements of Zionist patriotism. In April 2021, for example, it helped organize an Israel Independence Day convention, and on International Holocaust Remembrance Day it shared on LinkedIn that it was a "proud Israeli and Zionist" company. When it received heavy criticism in 2021 after the nonprofit investigative outlet Forbidden Stories released its bombshell report on a leak of 50,000 phone numbers targeted by Pegasus, then-CEO Hulio alleged the criticism had more to do with the company's Israeli identity than the spyware.[176]

NSO Group also takes the time to spar with international officials, especially after accusations of human rights abuses. For example, after Francesca Albanese, UN special rapporteur on the situation of human rights in the Palestinian territories occupied since 1967, accused NSO Group of being complicit in the "economy of genocide" after October 7, CEO Yaron Shohat claimed it was hard to view her reporting as anything but "morally inverted" and "antisemitism."[177] [178] Shohat relied on red herrings, alleging that the UN and Albanese have remained silent on the "rape, torture, kidnapping, and massacre of Israeli civilians on October 7." In this way, NSO Group also ties its image and product intimately with "morality," and a self-righteous patriotism that its detractors refuse.

Premier Products: Pegasus

NSO Group's premier product is its spyware suite Pegasus, a sophisticated mercenary spyware. It is specifically zero-click surveillance malware, meaning a victim does not need to click a link or interact with an attacker to become infected.[179] However, Pegasus can also be deployed as a single-click or physically installed.[180] A recently released court declaration from NSO Group CEO Yaron Shohat suggests how the company conceptualizes the product:

[174] NSO Group. (2021). *Conferences Archive - NSO Group*. [online] Available at: https://web.archive.org/web/20250619091830/https://www.nsogroup.com/conferences/ [Accessed 2 Jul. 2025].
[175] ISS World Training. (2025). *ISS World Europe - Sponsors*. [online] Available at: https://www.issworldtraining.com/ISS_EUROPE/sponsors.html [Accessed 2 Jul. 2025].
[176] Kotliar, D.M. and Carmi, E. (2023). Keeping Pegasus on the wing: legitimizing cyber espionage.
[177] NSO Group. (2025). *When faced with unfounded accusations, silence is not an option!* [LinkedIn], June 2025. Available at: https://www.linkedin.com/posts/yarons_un-nso-letters-ugcPost-7338833305217253376-Z-7i/ [Accessed 2 Aug. 2025].
[178] Albanese, F. (2025). *From Economy of Occupation to Economy of Genocide*. [online] UN Human Rights Council.
Available at: https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf [Accessed 2 Aug. 2025].
[179] Farrier, E. (2022). *What Is Pegasus Spyware and Is Your Phone Infected with Pegasus?* [online] What Is Pegasus Spyware and Is Your Phone Infected with Pegasus? Available at: https://www.avast.com/c-pegasus-spyware [Accessed 11 Aug. 2025].
[180] Zetter, K. (2021). *Pegasus Spyware: How It Works and What It Collects*. [online] ZERO DAY. Available at: https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/ [Accessed 11 Aug. 2025].

"Among NSO's products are a suite of different technologies and functions that are collectively branded and marketed as 'Pegasus.'"[181]

NSO Group describes Pegasus as a "targeted surveillance system," emphasizing that it has limited scope in targeting individual devices. As NSO Group noted in its 2024 report on transparency and accountability, Pegasus is:

> *"...a targeted surveillance system designed to be installed on a single mobile device, with strictly limited licenses and usage subject to comprehensive legal restrictions and frameworks specific to each customer's jurisdiction… we do not operate Pegasus nor do we have any involvement in the specific investigations conducted by law enforcement—we never access the data collected, nor do we know who is being investigated."*
>
> *"[It is] analogous to a traditional wiretap…tailored to the modern world's use cases… [it] is not a mass surveillance tool."*[182]
>
> *"[Pegasus] merely enable[s] law enforcement agencies to do their jobs while adhering to both local laws and international human rights standards."*[183]

In this way, NSO Group denies any responsibility for Pegasus and its operators.

Pricing for Pegasus depends on what specific product is being used, the exact capabilities (and number of requested capabilities), and the number of requested licenses. In 2016, *The New York Times* reported that NSO Group prices spyware access according to the number of requested targets.[184] For "unlimited access to a target's mobile devices," in 2016, NSO Group charged a $500,000 installation fee, $650,000 for 10 iPhone users or Android users, $800,000 for 100 additional targets, $500,000 for 50 additional targets, $250,000 for 20 additional targets, and $150,000 for 10 additional targets. NSO Group also charges an annual product maintenance fee—17% of the total each year after the first.[185]

More recently, according to court testimony in the WhatsApp vs. NSO Group case, prices primarily range between $1 million and $10 million for one mobile endpoint product license. Targeting phones outside of customers' countries costs an additional $1 million.[186] NSO Group also charges "upsell," or add-on, items in addition to base Pegasus capabilities.

---

[181] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025c] (District Court, N.D. California) Available at: https://www.courtlistener.com/docket/16395340/760/1/whatsapp-inc-v-nso-group-technologies-limited/ [Accessed 27 Aug. 2025].
[182] NSO Group (2024). *Transparency and Responsibility Report 2024*. [online], p.6 Available at: https://web.archive.org/web/20250518154902/https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf [Accessed 25 Jun. 2025].
[183] NSO Group (20224). *Transparency and Responsibility Report 2024*, p. 7.
[184] Perlroth, N. (2016). How Spy Tech Firms Let Governments See Everything on a Smartphone. *The New York Times*. [online] 2 Sep. Available at: https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html [Accessed 11 Aug. 2025].
[185] Perlroth, N. (2016). How Spy Tech Firms Let Governments See Everything on a Smartphone.
[186] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025d] (District Court, N.D. California) Available at: https://www.courtlistener.com/docket/16395340/679/7/whatsapp-inc-v-nso-group-technologies-limited/ [Accessed 27 Aug. 2025].

Examples cited in the court case show that NSO Group charged $6,835,000, $1,412,000, and $5,630,000 to three clients respectively for upsell items for Android infections between 2018 and 2019.[187] In a deposition to the court, NSO Group's Vice President of Global Business Operations Sarit Bizinsky Gil confirmed that the standard price for hacking 15 different devices at a time between 2018 and 2020 was $7 million. Between the second quarter of 2018 and the second quarter of 2020, NSO Group charged 90 separate accounts amounts ranging from $9,899 to $6 million for costs relating to Pegasus.[188]

WhatsApp, et al. v. NSO Group, et al.
Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments (Q2 2018 - Q2 2020)
Supplemental Exhibit 1.1

	Account No.	Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
1	Acc-01	$ -	$ -	$ -	$ -
2	Acc-02	$ -	$ -	$ -	$ -
3	Acc-03	$ 933,500	$ 1,402,390	$ 660,831	$ 2,996,721
4	Acc-04	$ 6,069,231	$ 2,410,849	$ 763,671	$ 9,243,751
5	Acc-05	$ -	$ 604,000	$ 633,306	$ 1,237,306
6	Acc-06	$ -	$ 1,412,348	$ 180,620	$ 1,592,969
7	Acc-07	$ -	$ -	$ 807,022	$ 807,022
8	Acc-08	$ -	$ -	$ -	$ -
9	Acc-09	$ -	$ -	$ -	$ -
10	Acc-10	$ 455,792	$ 1,055,518	$ 545,751	$ 2,057,060
11	Acc-12	$ -	$ -	$ -	$ -
12	Acc-13	$ 54,963	$ 69,431	$ 35,709	$ 160,102
13	Acc-14	$ -	$ 60,706	$ 37,238	$ 97,944
14	Acc-16	$ -	$ 693,527	$ 87,913	$ 781,440
15	Acc-18	$ -	$ 945,151	$ 54,849	$ 1,000,000
16	Acc-19	$ -	$ -	$ -	$ -
17	Acc-20	$ -	$ -	$ -	$ -
18	Acc-21	$ 990,725	$ 1,256,314	$ 654,452	$ 2,901,491
19	Acc-22	$ -	$ -	$ -	$ -
20	Acc-23	$ -	$ 1,570,849	$ 189,981	$ 1,760,831
21	Acc-24	$ -	$ -	$ -	$ -
22	Acc-25	$ -	$ -	$ -	$ -
23	Acc-26	$ 779,683	$ 188,844	$ 74,452	$ 1,042,979
24	Acc-27	$ -	$ 917,783	$ 105,149	$ 1,022,932
25	Acc-29	$ -	$ 1,593,128	$ 212,159	$ 1,805,287
26	Acc-31	$ 169,166	$ 200,592	$ 100,830	$ 470,588
27	Acc-32	$ -	$ 1,446,189	$ 296,739	$ 1,742,928
28	Acc-33	$ 694,000	$ 567,096	$ 431,750	$ 1,692,846
29	Acc-34	$ 211,916	$ 21,577	$ -	$ 233,493
30	Acc-37	$ -	$ -	$ -	$ -
31	Acc-38	$ -	$ -	$ -	$ -
32	Acc-39	$ -	$ 479,698	$ 38,702	$ 518,400
33	Acc-40	$ 442,500	$ 180,096	$ 176,168	$ 798,764
34	Acc-41	$ -	$ -	$ -	$ -
35	Acc-43	$ -	$ -	$ -	$ -
36	Acc-44	$ 96,250	$ 368,959	$ 185,959	$ 651,167
37	Acc-45	$ 914,805	$ 378,237	$ 160,112	$ 1,453,155
38	Acc-46	$ 791,169	$ 214,157	$ 98,598	$ 1,103,924
39	Acc-47	$ 129,736	$ (15,909)	$ -	$ 113,828
40	Acc-48	$ 574,075	$ 1,182,686	$ 745,545	$ 2,502,306
41	Acc-49	$ 343,289	$ (42,096)	$ -	$ 301,193
42	Acc-50	$ -	$ -	$ -	$ -
43	Acc-51	$ -	$ -	$ -	$ -

Image 7: A partial breakdown of Pegasus revenue streams from Q2 2018 to Q2 2020.[189]

[187] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025d].
[188] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025d].
[189] *WhatsApp Inc. v. NSO Group Technologies Limited* [2025d].

Capabilities

The core functionality of Pegasus is monitoring real-time user activity and exfiltrating data from targeted phones without notifying a user they were compromised.[190] Pegasus can target Android and iPhone devices; Google calls the Android variant "Chrysaor."[191]

Leaked marketing information from 2016 gives insight into Pegasus capabilities. Pegasus can collect virtually all data stored on phones, including text messages, emails, photos, videos, voice memos, event history, call history, browsing history, and username-password combinations. It also can monitor user locations, use the microphone to eavesdrop on conversations, and activate phone cameras to take images of the user remotely.

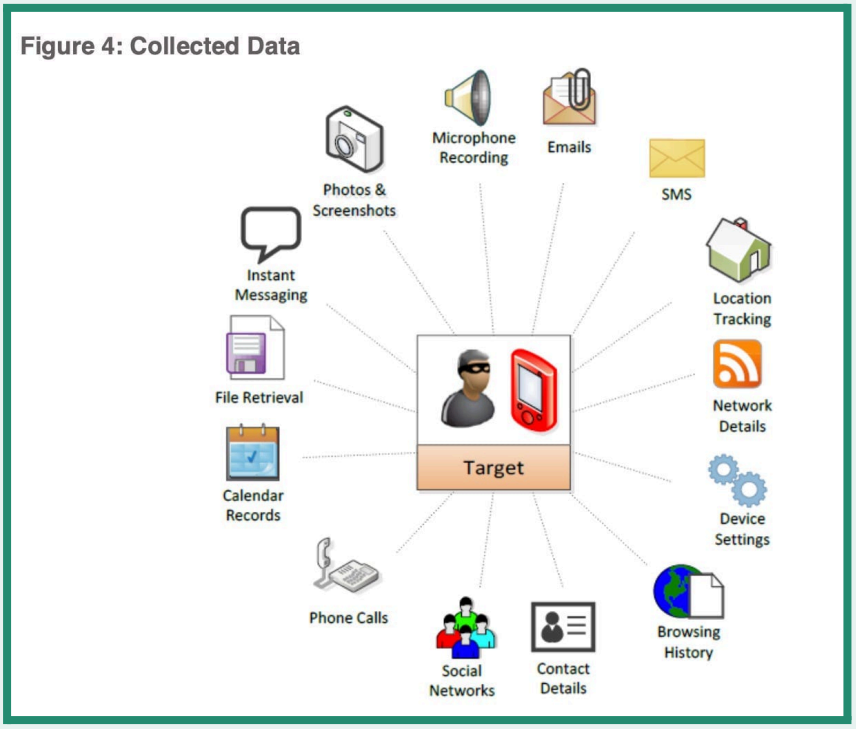


Image 8: A leaked Pegasus marketing brochure from 2016 highlights the types of data it can collect.[192]

Pegasus can be installed on phones physically, via one-click or zero-click exploits.[193] For single-click vectors, Pegasus operators send phishing texts or emails that include a malicious link. After they click, the user is taken to a page that surreptitiously downloads Pegasus. For zero-click vectors, Pegasus is delivered in a way that does not require a target to click on a link. In the past, for example, this has involved users receiving a silent iMessage that

[190] Zetter, K. (2021). *Pegasus Spyware: How It Works and What It Collects*. [online] ZERO DAY. Available at: https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/ [Accessed 11 Aug. 2025].
[191] Cobb, M. (2017). *How is Pegasus malware different on Android than on iOS?* [online] Search Security. Available at: https://www.techtarget.com/searchsecurity/answer/How-is-Pegasus-malware-different-on-Android-than-on-iOS [Accessed 11 Aug. 2025].
[192] NSO Group (2016). *Pegasus – Product Description*. [online] Kim Zetter. Available at: https://www.zetter-zeroday.com/content/files/documents/4599753/nso-pegasus.pdf [Accessed 7 Jul. 2025].
[193] Zetter, K. (2021). *Pegasus Spyware: How It Works and What It Collects*.

activates a kill chain, leading to Pegasus being installed on their phone. Pegasus operators can also exploit rogue cell towers in the close vicinity of a target phone, allowing an intermediary-in-the-middle attack, in which a victim is connected to a fake cell tower that infects the device with Pegasus. NSO Group accomplishes these attacks by developing and/or purchasing zero-day exploits affecting iPhones and Android devices. These exploits target software vulnerabilities unknown to phone manufacturers.

Once Pegasus infects a phone, it copies and compresses targeted data, and encrypts it using AES 128-bit encryption.[194] Then it sends the data to a command-and-control server within the client's network. According to security researcher Kim Zetter, Pegasus hides data in "hidden and encrypted" buffers and transmits it via Wi-Fi or cellular networks, and because the data is compressed, it negligibly affects device performance and uses little data. Lastly, NSO Group claims it transmits data through "anonymizers" to mask information about the data and who is receiving the data. According to Amnesty International, NSO Group's Pegasus attack infrastructure is located primarily in North America and Europe (with one server located in Bahrain), and most are owned by the US-owned companies Amazon Web Services, Digital Ocean, and Linode.[195]

NSO Group claims Pegasus operates on the kernel level of devices and can self-destruct, so it is nearly impossible to detect.[196] However, Amnesty International has released a tool helping victims identify if they were infected.[197]

Prominent Attack

In December 2021, *The Washington Post* released a report investigating one of the most infamous uses of Pegasus spyware.[198] In 2018, Hanan Elatr, the wife of Saudi journalist Jamal Khashoggi, was working as an Emirates flight attendant. As she passed through the Dubai airport on April 21, 2018, she was surrounded by security agents. They kidnapped her, blindfolded her, and confiscated her two Android cellphones, laptop, and relevant passwords. She was then interrogated about Khashoggi and activities perceived as being seditious to Gulf monarchies.

The next day, a security official installed Pegasus on one of her Android devices by accessing a website designed by NSO Group for a UAE customer that downloaded the spyware over the course of a few minutes. Elatr received her phones back a few days later. While technology researchers reviewing her devices could not verify whether the spyware had successfully infected the phone, the Emirati security officials did not enter the URL to

---

[194] Zetter, K. (2021). *Pegasus Spyware: How It Works and What It Collects*.
[195] Amnesty International Security Lab (2021). *Forensic Methodology Report: How to Catch NSO Group's Pegasus*.
[196] Zetter, K. (2021). *Pegasus Spyware: How It Works and What It Collects*.
[197] Amnesty International Security Lab (2021). *Forensic Methodology Report: How to Catch NSO Group's Pegasus*.
[198] Priest, D. (2021). *A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*. [online] Washington Post. Available at: https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/ [Accessed 11 Jul. 2025].

download the spyware a second time, suggesting it was installed successfully.[199] Although NSO Group vehemently denied its involvement in the affair, which occurred months before Khashoggi's murder, a data leak of 50,000 numbers potentially targeted by Pegasus revealed Elatr and Khashoggi's Turkish fiancée, Hatice Cengiz, among the targets.[200] Amnesty Internatioanal further reported that UAE customers of NSO Group had been attempting to use Pegasus to spy on Elatr since November 2017.[201]

The event left Elatr scarred. In an interview reported by the Post, she maintained, "Every day when I see the daylight, I don't know why I'm still alive … I lost my life … I used to provide for my family and now I can't even find my own food."[202] Cengiz's life was also dramatically altered over fears for her life after Khashoggi's assassination and the revelations into Pegasus—she hired bodyguards and no longer felt safe. That is ultimately what Pegasus accomplishes: It strips victims of their fundamental human right to privacy and potentially accelerates other forms of repression, including kidnapping and even murder.

3.2 Cytrox and Intellexa Alliance

"The universe in a way needs our product."
—Tal Dilian, founder of the Intellexa Alliance

Cytrox Company Background

Cytrox's story begins in 2017, when it was founded as a "cyber solution" start-up.[203] Cytrox AD (registration no: 7191391, aka "САЈТРОКС АД") was founded in Skopje on March 27, 2017, by five Israeli businessmen—Alon Arabov, Avraham Rubinstein, Eyal Avraham Oren, Dror Harpaz, and Sharon Adler—and Hungarian businessman Rotem Farkash.[204] [205] As Citizen Lab noted in its first major report on Cytrox and its Predator spyware, Cytrox on Pitchbook

[199] Priest, D. (2021). *A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*.
[200] Priest, D., Mekhennet, S. and Bouvart, A. (2021). *Jamal Khashoggi's wife targeted with spyware before his death*. [online] Washington Post. Available at: https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/ [Accessed 11 Jul. 2025].
[201] Priest, D. (2021). *A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*.
[202] Priest, D. (2021). *A UAE Agency Put Pegasus Spyware on Phone of Jamal Khashoggi's Wife Months before His Murder, New Forensics Show*.
[203] Crunchbase (2024). *Cytrox - Crunchbase Company Profile & Funding*. [online] Crunchbase. Available at: https://www.crunchbase.com/organization/cytrox [Accessed 27 Aug. 2025].
[204] Central Registry of the Republic of North Macedonia (2025). Basic Profile of a Registered Legal Entity: Entry for САЈТРОКС АД. [online] Available at: https://crm.com.mk/en/open-data/basic-profile-of-a-registered-entity?embs=7191391 [Accessed 28 Aug. 2025].
[205] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*. [online] Investigative Reporting Lab Macedonia. Available at: https://irl.mk/israeli-company-developed-spyware-in-skopje-local-officials-looked-the-other-way/ [Accessed 26 Jul. 2025].

describes itself as a company that helps government clients "gather intelligence from … end devices … [and] cloud services."[206]

According to North Macedonian investigative journalists at IRL Macedonia, Cytrox's initial CEO was Ivo Malinkovski, a 26-year-old North Macedonian entrepreneur from a family of arms dealers and winemakers. A December 17, 2017, capture of Cytrox's early website shows Malinkovski's email listed as a point of contact at ivo@cytrox[.]com.[207] Meir Shamir, an Israeli air force veteran with alleged ties to spyware entrepreneur Tal Dilian, was listed as the beneficial owner of Cytrox. On October 6, 2017, Malinkovski, through two of the companies he ran, formally asked North Macedonia's Ministry of Interior for permission to sell software products for intercepting personal data for government clients. Malinkovski filed again with additional details on November 7, 2017, which explained Cytrox's primary product, Predator.[208] [see below for more information on Predator]

Image 9: Cytrox business logo, as reported on IT[.]mk.[209]

Three corporate entities apparently associated with Cytrox were also founded in 2017 in Israel and Hungary. The two Israeli companies, Cytrox EMEA Ltd. (registration no: 515692135) and Cytrox Software Ltd. (registration no: 515693893), were respectively renamed to Balinese Ltd. and Peterbald Ltd. in 2019. The Hungarian entity, Cytrox Holdings Zrt (registration no: 01-10-049372), appears to be in the process of liquidation as of 2025, according to Hungarian corporate records.[210] The Balkan Investigative Reporting Network in Macedonia reported on December 30, 2021, that Cytrox filings in 2020 show that it had 1.5 million euros in revenue, 16 employees, and 100,000 euros in expenses.[211]

Four other cybersecurity-themed companies were founded between 2017 and 2020 with the same address as Cytrox in Skopje—Cintellexa (registration no: 7398085, "СИНТЕЛЕКСА ДООЕЛ Скопје"),[212] Cyberlab (registration no: 7319339, "САЈБЕР ЛАБ

[206] Crunchbase (2024). *Cytrox - Crunchbase Company Profile & Funding.*
[207] Cytrox. (2017). *Cytrox – Cyber Intelligence Home Page*. [online] Available at: https://web.archive.org/web/20171217071850/http://cytrox.com/ [Accessed 1 Aug. 2025].
[208] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.
[209] IT.mk Editorial Team (2021). *Зошто Мета ја бануваше македонската компанија за шпионски софтвер, Cytrox ⋆ IT.mk*.
[210] Hungary Company Information and Electronic Company Procedure Service of the Ministry of Justice (2025). National Company Register and Company Information System: Entry for Cytrox Holdings Zrt. [online] Available at: https://www.e-cegjegyzek.hu/?cegkereses [Accessed 28 Aug. 2025].
[211] Apostolov, V. (2021). *Елитна сајбер-шпионажа На Македонски Погон*. [online] Balkan Investigative Reporting Network, Macedonia. Available at: https://prizma.mk/elitna-sajber-shpionazha-na-makedonski-pogon/ [Accessed 12 Jul. 2025].
[212] CompanyWall Business (2019). *СИНТЕЛЕКСА ДООЕЛ Скопје*. [online] CompanyWall Business. Available at: https://www.companywall.com.mk/kompanija/%D1%81%D0%B8%D0%BD%D1%82%D0%B5%D0%BB

ДООЕЛ Скопје"),[213] Cygnet (registration no: 7473222, "САЈГНЕТ ДООЕЛ Скопје"),[214] and Cyshark (registration no: 7187254, "САЈШАРК ДООЕЛ Скопје").[215][216] Avraham Rubinstein and Rotem Farkash are connected as beneficial owners to Cytrox and Cyberlab, and Moshe Farkash (Rotem's father) co-owned Cyshark with Malinkovski.[217] All allegedly have ties to Tal Dilian.[218] The ties between this web of companies and the Israeli military also began to grow at this time.

According to a former software engineer who worked at the complex of the five companies, Cyberlab was run by Shahak Shalev, an Israeli who was the head of research and development at Intellexa and a former "cyber security expert" at the Israeli Defense Forces.[219] Intelligence Online in 2017 reported Shalev as the R&D director for Cytrox.[220] While Malinkovski managed CyberLab on paper, the actual owner of the venture was Inpedio, a Dutch company owned by Rubenstein and Farkash. Shalev was the vice president of technology at Inpedio until 2020.[221] Inpedio and Cytrox both received investments from Israel Aerospace Industries (IAI) in 2017, and Cytrox appears to also be connected with the Israeli investment fund Atooro Fund.[222] In a touch of irony, Shalev now works at

%D0%B5%D0%BA%D1%81%D0%B0-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMvwvEq [Accessed 28 Aug. 2025].

[213] CompanyWall Business (2018). *САЈБЕР ЛАБ ДООЕЛ Скопје*. [online] CompanyWall Business. Available at: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%BB%D0%B0%D0%B1-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMx2VZyY [Accessed 28 Aug. 2025].

[214] CompanyWall Business (2020). *САЈГНЕТ ДООЕЛ Скопје*. [online] CompanyWall Business. Available at: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D0%B3%D0%BD%D0%B5%D1%82-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMf8srq [Accessed 28 Aug. 2025].

[215] CompanyWall Business (2017). *САЈШАРК ДООЕЛ Скопје*. [online] CompanyWall Business. Available at: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D1%88%D0%B0%D1%80%D0%BA-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMxrrUsD [Accessed 28 Aug. 2025].

[216] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

[217] Several Cytrox-affiliated entities have listed seemingly unaffiliated individuals on corporate filings and contacts to obfuscate their corporate networks. For example, according to IRL Macedonia, Malinkovski's maternal grandmother was listed as the owner of Cyshark. It is unclear whether she agreed to this. In another example, Investigate[.]cz reported in 2024 that Cytrox listed an elderly Czech woman in a small village as its director, unbeknownst to her. A few days after a reporter visited her in 2023, Cytrox changed its director to Sylwia J., a 25-year-old Polish woman. Reporters visited her listed Polish address, but there was no record of her living there. They made contact with Sylwia over Instagram, and confirmed she was the same individual from Cytrox's business filings. She denied any connection and then deleted her account, creating a new one with another username.

[218] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

[219] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

[220] Intelligence Online (2017). Cytrox and Inpedio, IAI's New Cyber Stars. *Intelligence Online*. [online] 7 May. Available at: https://www.intelligenceonline.com/corporate-intelligence/2017/07/05/cytrox-and-inpedio-iai-s-new-cyber-stars,108252955-bre [Accessed 28 Jun. 2025].

[221] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

[222] Atooro Fund. (2024). *Atooro Fund Home Page*. [online] Available at: https://www.atooro.com/ [Accessed 28 Aug. 2025].

Malwarebytes—an antivirus, anti-malware, and scam protection service provider—as a senior director of technology and engineering for consumer privacy.

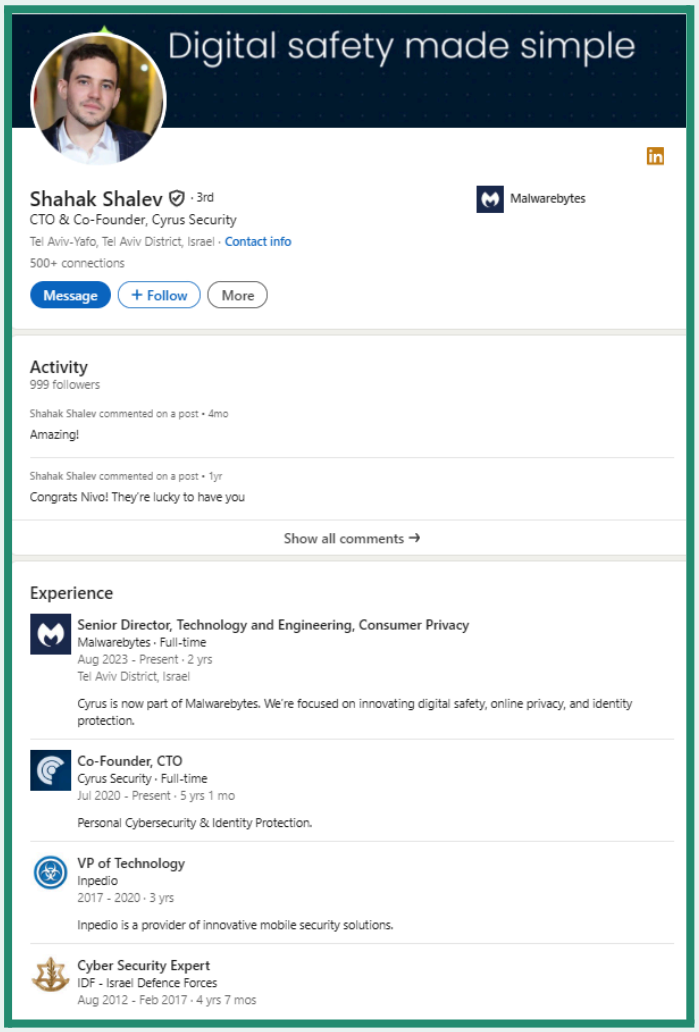


Image 10: Shahak Shalev's public LinkedIn page shows his work history at Inpedio.[223]

Today, Cytrox, Cyshark, CyberLab, and Cintellexa have all been dissolved, been declared inactive, or filed for bankruptcy. Cintellexa, according to publicly available filings, had no income since 2021 and was dissolved on November 15, 2023.[224] Cytrox in 2024 generated 5,026,000 euros in gross revenue and claimed 150,486,000 euros in liabilities.[225] It is unclear what CyberLab has made in income, but it does not appear currently active.[226] In 2023, Cyshark claimed it made -3,519,000 euros in net income, with 4,986,000 euros in liabilities.[227] The company has since filed for bankruptcy and is now dissolved.

---

[223] Shalev, S. (2025). *Shahak Shalev's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/shahak-shalev-ba2a49135/.
[224] CompanyWall Business (2019). *СИНТЕЛЕКСА ДООЕЛ Скопје*.
[225] CompanyWall Business (2017b). *САЈТРОКС ДООЕЛ Скопје*. [online] CompanyWall Business. Available at: https://www.companywall.com.mk/kompanija/%D1%81%D0%B0%D1%98%D1%82%D1%80%D0%BE%D0%BA%D1%81-%D0%B4%D0%BE%D0%BE%D0%B5%D0%BB-%D1%81%D0%BA%D0%BE%D0%BF%D1%98%D0%B5/MMxs7WNq [Accessed 28 Aug. 2025].
[226] CompanyWall Business (2018). *САЈБЕР ЛАБ ДООЕЛ Скопје*.
[227] Drawing information from third-party financial aggregators like CompanyWall, while useful in helping understand approximate financials associated with companies, is not perfect and may feature errors.

Cygnet is currently active and has the most publicly available information via official filings. Its 100% owner is Ivo Malinkovski (the email listed for Cygnet on third-party business aggregators cygnet[.]setup@gmail[.]com). Cygnet claimed 163,469,000 euros in income in 2022, 78,453,000 euros in 2023, and 0 euros in 2024. Meanwhile, it had 139,356,000 euros in expenses in 2022, 87,379,000 in 2023, and 5,673,000 in 2024. It allegedly had between 25 and 30 employees in 2022 and 2023, but none in 2024.[228] Cygnet consequently appears to have been one of, if not the primary, operating sales entity within the Cytrox corporate network, given its substantial revenue. However, its revenue has dropped significantly since 2022 and no longer appears to be actively trading.

According to a former software engineer who worked at the complex of the five companies, all five companies worked in the same offices on the same tasks. No one knew how many companies actually existed—they just knew they worked for a murky umbrella company known as Intellexa, the complex corporate structure founded and formerly run by Tal Dilian.[229]

[228] CompanyWall Business (2020). *САЈГНЕТ ДООЕЛ Скопје*.
[229] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

The Cytrox/Intellexa Alliance Corporate Structure: The Cytrox AD Structure

This information is from publicly available corporate records and news reporting, as of 2022.

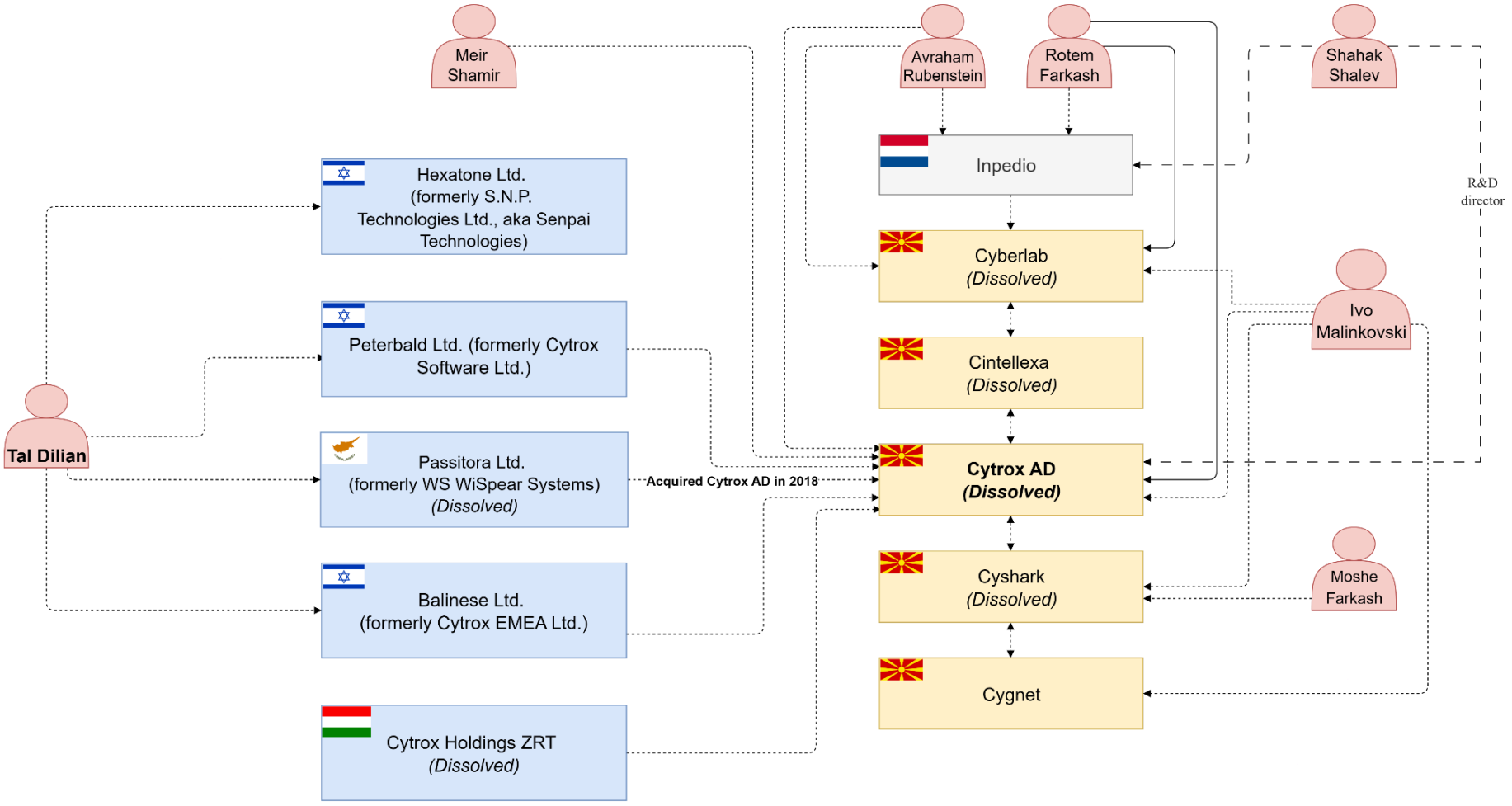


Image 11: The Cytrox AD corporate structure.

The Intellexa Alliance

In 2018, Tal Dilian's company WS WiSpear Systems Limited (registration no: 318328) acquired Cytrox for under $5 million, adding it to the so-called Intellexa Alliance of companies in 2019.[230] [231] The Intellexa Alliance is a consortium of spyware companies also including Nexa Technologies and WS WiSpear Systems Limited.[232] According to research by Amnesty International, the Intellexa Alliance is comprised of two groups of spyware companies: the Intellexa Group and the Nexa Group.[233] While the alliance is not itself a registered company, several entities with Intellexa in their names are registered in the British Virgin Islands,[234] Greece,[235] and Ireland (though the Greece corporation's registration is suspended due to late financial filings).[236] Most companies in the Intellexa Group have mutual business relationships and similar names. Some researchers and government officials use the term Intellexa Consortium to refer to the grouping of Intellexa entities with commercial and/or research relationships.[237]

The Intellexa Group

Dilian designed the Intellexa Group as a group of companies that complemented each other through their technology offerings. He began building Intellexa Group by 2018, when he acquired Cyprus-based WS WiSpear Systems Limited, which specialized in exfiltrating sensitive data from long ranges through Wi-Fi interception.[238] WS WiSpear Systems was later renamed to Passitora Ltd. Through WS WiSpear Systems, he purchased Cytrox AD also in 2018. He later acquired in 2018 Israel-based SENPAI Technologies Ltd. (registration no: 515385748), which specialized in open-source intelligence and analyzing data stolen through spyware.[239]

---

[230] Brewster, T. (2019). *A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*. [online] Forbes ME. Available at: https://www.forbesmiddleeast.com/innovation/technology/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van [Accessed 2 Aug. 2025].

[231] According to Cyprus corporate records, Passitora Ltd. has been dissolved.

[232] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R., Aljizaw, N. and Anstis, S. (2021). *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*. [online] *Citizen Lab*. University of Toronto. Available at: https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/ [Accessed 5 Aug. 2025].

[233] Amnesty International (2023). *The Predator Files: Caught in the Net*. [online] *Amnesty International*, London: UK: Amnesty International Ltd. Available at: https://www.amnesty.org/en/documents/act10/7245/2023/en/.

[234] Dun & Bradstreet (n.d.). *Intellexa Limited*. [online] Dun & Bradstreet. Available at: https://www.dnb.com/business-directory/company-profiles.intellexa_limited.2610c71eee08982e83b1dc8bb7899ea6.html [Accessed 28 Aug. 2025].

[235] Hellenic Republic Ministry of Development (2025). GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ. [online] Available at: https://publicity.businessportal.gr/company/154460701000 [Accessed 28 Aug. 2025].

[236] Companies Registration Office (2025). CORE: Entry for Intellexa Limited. [online] Available at: https://core.cro.ie/e-commerce/company/search/697890 [Accessed 28 Aug. 2025].a

[237] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024). *Markets Matter: a Glance into the Spyware Industry*.

[238] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.

[239] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.

SENPAI Technologies was founded by Eric Banoun, Guy David, Jonathan Lampert, Omri Raiter, and Roy Shloman.[240] While it is commonly referred to and branded as SENPAI Technologies, the company's actual name transliteration is S.N.P. Technologies Ltd. (original Hebrew: ס.נ.פ טכנולוגיות בע"מ). SENPAI Technologies has undergone at least two name changes, and as of 2025 it is known as Hexatone Ltd. (original Hebrew: האקסטון גרופ בע"מ).[241] In 2020 Dilian added the Greece-based Intellexa S.A. to the mix of companies under his control, which in 2024 was revealed by the US Treasury Department as the main entity through which Intellexa Group sells Predator.[242]

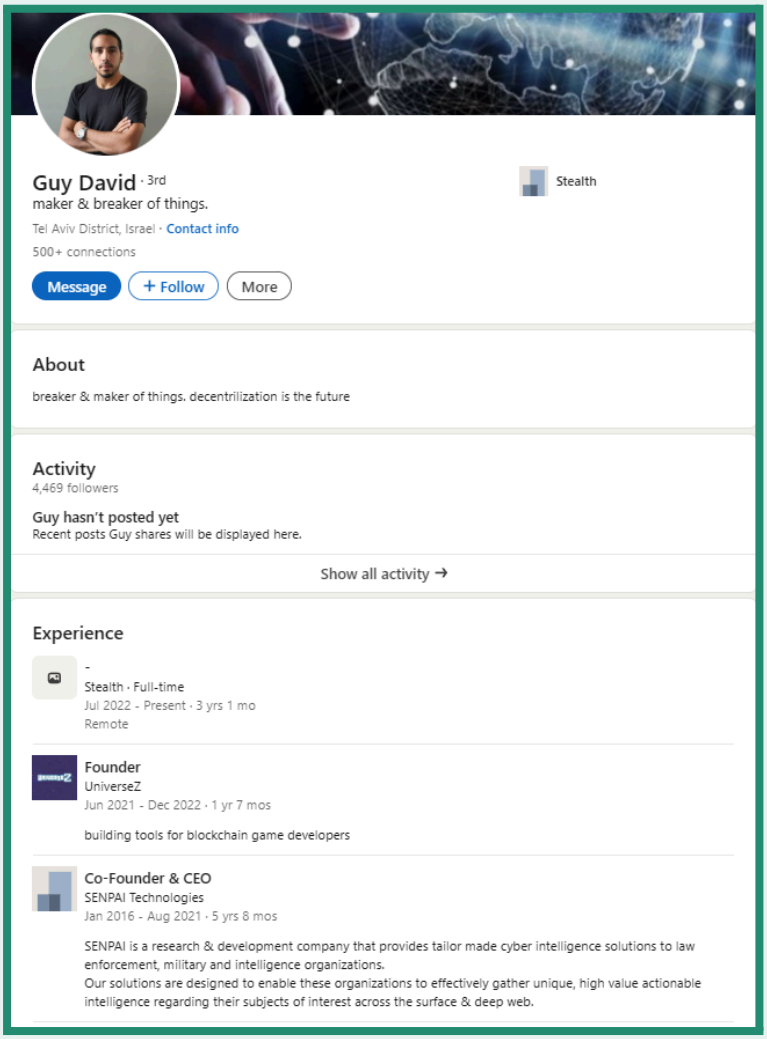


Image 12: Guy David, cofounder of SENPAI Technologies, describes his experience with the company on LinkedIn. He appears to be the only cofounder who publicly lists his work with SENPAI Technologies.[243]

---

[240] Orbach, M. (2019). The Cyber Company, the Former Officer, and the Lost Money. *CTech*. [online] 17 Oct. Available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3772040,00.html [Accessed 28 Aug. 2025].
[241] CheckID (2025). *Haxton Group Ltd. / HEXATONE GROUP LTD - 515385748*. [online] CheckID. Available at: https://en.checkid.co.il/company/HEXATONE+GROUP+++LTD-g3LW9ky-515385748 [Accessed 28 Aug. 2025].
[242] U.S. Department of the Treasury. (2024). *Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*. [online] Available at: https://home.treasury.gov/news/press-releases/jy2155 [Accessed 10 Aug. 2025].
[243] David, G. (2025). *Guy David's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/guy-david-5a99a731/.

Changing Intellexa Ownership Structure: From Aliada to Thalestris

In 2020, all shares of Balinese Ltd. (previously Cytrox EMEA) held by Cytrox Holdings Zrt were transferred to Aliada Group, a corporate entity based in the British Virgin Islands (registration no: 1926732).[244] Aliada appears to be Balinese's main shareholder.[245] Because Cytrox Holdings Zrt dissolved, it seems that Tal Dilian is the only remaining owner of Peterbald (formerly Cytrox Software).[246] Aliada Group received funding from the private equity firm Mivtach-Shamir Holdings Ltd. (מבטח שמיר אחזקות בע"מ), founded by Meir Shamir—one of the original founders of Cytrox AD in North Macedonia.[247] [248] Mivtach-Shamir (registration no: 520034125) is listed on Tel Aviv Stock Exchange (ticker: MISH).[249] In 2020, Cytrox cofounder Avi Rubinstein sued Dilian in a district court in Tel Aviv, accusing him and Meir Shamir of diluting Rubinstein's shares with a complex array of overseas companies.[250] Before Cytrox AD was dissolved, it was collectively held by Cytrox Holdings Zrt, Balinese Ltd., and Peterbald Ltd.[251]

In 2017, Intelligence Online reported Aliada was the owner of WS WiSpear Systems Limited (which bought Cytrox AD).[252] In 2020 Miros Development Group Inc purchased WS WiSpear Systems Limited.[253] Miros was then purchased by the holding company Thalestris Limited in Ireland, whose director is Sara Hamou, Dilian's ex-wife.[254] [255]

[244] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R., Aljizaw, N. and Anstis, S. (2021). *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*.
[245] CheckID (2025). *BALINESE LTD - 515692135*. [online] CheckID. Available at: https://en.checkid.co.il/company/BALINESE++LTD-P02VO4w-515692135 [Accessed 28 Aug. 2025].
[246] CheckID (2025c). *PETERBALD LTD - 515693893*. [online] CheckID. Available at: https://en.checkid.co.il/company/PETERBALD++LTD-rMeDN2x-515693893 [Accessed 28 Aug. 2025].
[247] Crunchbase (2024). *Mivtach Shamir Holdings LTD - Crunchbase Company Profile & Funding*. [online] Crunchbase. Available at: https://www.crunchbase.com/organization/mivtach-shamir-holdings-ltd [Accessed 27 Aug. 2025].
[248] Intelligence Online (2017b). With WiSpear, GSM Interception Champion Tal Dilian Gets into WiFi. *Intelligence Online*. [online] 20 Sep. Available at: https://www.intelligenceonline.com/surveillance--interception/2017/09/20/with-wispear-gsm-interception-champion-tal-dilian-gets-into-wifi,108262318-art [Accessed 28 Jun. 2025].
[249] StockAnalysis. (2025). *Mivtach Shamir Holdings*. [online] Available at: https://stockanalysis.com/quote/tlv/MISH/ [Accessed 27 Jul. 2025].
[250] Sadeh, S. (2020). A Shady Israeli Intel Genius, His Cyber-spy Van and Million-dollar Deals. *Haaretz*. [online] 31 Dec. Available at: https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000 [Accessed 27 Aug. 2025].
[251] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.
[252] Intelligence Online (2017b). With WiSpear, GSM Interception Champion Tal Dilian Gets into WiFi.
[253] Χαριάτης, M. (2022). *Τα Πορίσματα ΣΥΡΙΖΑ - ΠΑΣΟΚ Για Τις υποκλοπές: Και Σκάνδαλο Και Συγκάλυψη*. [online] iEidiseis. Available at: https://web.archive.org/web/20221010203948/https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi [Accessed 24 Aug. 2025].
[254] Χαριάτης, M. (2022). *Τα Πορίσματα ΣΥΡΙΖΑ - ΠΑΣΟΚ Για Τις υποκλοπές: Και Σκάνδαλο Και Συγκάλυψη*.
[255] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.

Today, Miros is a 45% subsidiary of Mivtach-Shamir Holdings Ltd.[256] According to Mivtach-Shamir's 2024 annual report published in March 2025, Miros held shares in Thalestris Limited. In 2020, Miros received a 10% share of Thalestris in exchange for transferring Thalestris all of Aliada Group's assets and liabilities it acquired earlier that year.[257] According to the US Treasury Department, Thalestris holds distribution rights to Predator.[258]

Thalestris' Subsidiaries

Through its acquisition of Aliada Group's assets, Thalestris took on several subsidiaries, according to the company's 2021 financial statements.[259] On February 3, 2021, Ireland-based Elpidina Ltd. (registration no: 687102) was established and later added to Thalestris. Thalestris listed Elpidina in its financial documents as a "dormant" company.[260] Intellexa Ltd., "a reseller of technologies," was established in Ireland in 2019 (registration no: 665443).[261] Thalestris also at this time acquired Greece-based Hermes Technologies S.A. (registration no: 154461601000)[262] and Apollo Technologies S.A. (registration no: 154460301000).[263] Apollo and Hermes were established on March 11, 2020, though both companies' registration are in suspension as of 2025. Thalestris describes both companies as being involved in the "design and development of information technologies for applications."[264]

From Aliada, Thalestris also acquired Nurul Ltd.[265] (registration no: 405667) and Mistrona Ltd.[266] (registration no: 405562) in Cyprus.[267] In its 2024 financial statement, Nurul noted it

---

[256] Mivtach-Shamir Hodings Ltd. (2024). *Mivtach-Shamir Hodings Ltd.: Annual Report for 2024*. [online] p.81. Available at: https://msgroup.co.il/wp-content/uploads/2025/03/%D7%93%D7%95%D7%97-%D7%AA%D7%A7%D7%95%D7%A4%D7%AA%D7%99-%D7%95%D7%A9%D7%A0%D7%AA%D7%99-%D7%9C%D7%A9%D7%A0%D7%AA-2024-merged-6.pdf.

[257] Mivtach-Shamir Hodings Ltd. (2024). *Mivtach-Shamir Holdings Ltd.: Annual Report for 2024*. [online] p.179.

[258] U.S. Department of the Treasury. (2024). *Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*.

[259] Thalestris Limited (2022). *Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*.

[260] Power, J. (2023). *Who Are Intellexa, the Irish Spyware Company Placed on a US 'blacklist'?* [online] The Irish Times. Available at: https://www.irishtimes.com/technology/2023/07/19/who-are-intellexa-the-irish-spyware-company-placed-on-a-us-blacklist/ [Accessed 28 Aug. 2025].

[261] Power, J. (2023). *Who Are Intellexa, the Irish Spyware Company Placed on a US 'blacklist'?*

[262] Hellenic Republic Ministry of Development (2025). GEMI Public Records: Entry for HERMES TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ. [online] Available at: https://publicity.businessportal.gr/company/154461601000 [Accessed 28 Aug. 2025].

[263] Hellenic Republic Ministry of Development (2025). GEMI Public Records: Entry for APOLLO TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ. [online] Available at: https://publicity.businessportal.gr/company/154460301000 [Accessed 28 Aug. 2025].

[264] Thalestris Limited (2022). *Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*. Dublin, Ireland: CORE, p.29.

[265] Nurul Ltd. (2024). Registration Details for Nurul Ltd. [online] Available at: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=dernova+limited&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [Accessed 28 Aug. 2025].

[266] Mistrona Ltd. (2023). Registration Details for Mistrona Ltd. [online] Available at: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=mistrona&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [Accessed 28 Aug. 2025].

[267] Thalestris in its 2021 Financial Statement listed Nurul, formerly known as Derrnova, as "dormant." It also listed Mistrona as working on the "development and licensing of software cloud programs."

had a credit balance of 9,863 euros with Thalestris Switzerland SA (registration no: 1437847).[268] Thalestris Switzerland was dissolved on March 28, 2024.[269] Mistrona's last available financial filings for 2021 show a vaguely defined "finance" relationship with Thalestris (in Ireland) and a trade relationship with Intellexa Limited (in the British Virgin Islands), and it appears today that Mistrona's sole shareholder is Intellexa Limited (in Ireland).[270] Nurul and Mistrona both list Panagiota Karaoli as their director, and Nurul lists Karaoli as its sole shareholder.[271] [272] On September 16, 2024, the US Treasury Department sanctioned Panagiota Karaoli for her role in directing "multiple Intellexa Consortium entities that are controlled by or are a subsidiary of Thalestris Limited."[273]

Thalestris appears to have maintained 100% ownership of most of Intellexa's Cypriot and Greek subsidiaries, except Intellexa S.A. in Greece, of which it owned 65% per Thalestris' most recent financial statements. Dilian reportedly sold the remaining 35% of the company to Felix Bitzios, allegedly a fixer for Dilian, via Cypriot company Santinomo Limited (registration no: 402203).[274] [275] Bitzios was also later sanctioned by the US Treasury Department on September 16, 2024.[276] Public reports vary in their representation of Intellexa S.A.'s ownership. The Atlantic Council reported in 2024 that Intellexa S.A. was owned by Intellexa Limited in the British Virgin Islands and Intellexa Ltd. in Ireland.[277] Meanwhile, investigative outlets—such as Lighthouse Reports, Haaretz, and Inside Story, as well as Solomon—have consistently reported since 2022 (until as recently as March 2025) that the ownership is split between Bitzios and Thalestris.[278] [279] This report's authors have not corroborated Intellexa S.A.'s full ownership structure with official filings.

---

[268] Eliades, C. (2024) *Financial Statements Period from 1 January 2024 to 31 August 2024.* Nicosia, Cyprus: NURUL Ltd, P. 11.
[269] Thalestris (Switzerland) SA (2024). Registration Details for Thalestris (Switzerland) SA. [online] Available at: https://traderegistry.ch/company-search/ [Accessed 28 Aug. 2025].
[270] Belifor Ltd. (2021) *Financial Statements Year ended 31 December 2021.* Nicosia, Cyprus: NURUL Ltd., p. 24.
[271] Nurul Ltd. (2025). *Organizational Details*. [online] Department of Registrar of Companies and Official Receiver, Cyprus, p.2.
[272] Mistrona Ltd. (2025). *Organizational Details*. [online] Department of Registrar of Companies and Official Receiver, Cyprus, p.2.
[273] U.S. Department of the Treasury. (2024a). *Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium*. [online] Available at: https://home.treasury.gov/news/press-releases/jy2581 [Accessed 20 Aug. 2025].
[274] Telloglou, T., Triantafillou, E., Black, C., Benjakob, O., Scharf, A., Statius, T., Geiger, G., vas Dijken, K., Deeb, B., Sapoch, J., Howden, D., Gibbs, M. and Faull, L. (2022). *Flight of the Predator*. [online] Lighthouse Reports. Available at: https://www.lighthousereports.com/investigation/flight-of-the-predator/.
[275] Santinomo Limited (2024). Registration Details for Santinomo Limited. [online] Available at: https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=Santinomo&number=%25&searchtype=optStartMatch&index=1&tname=%25&sc=0 [Accessed 28 Aug. 2025].
[276] U.S. Department of the Treasury. (2024a). *Treasury Sanctions Enablers of the Intellexa Commercial Spyware Consortium*.
[277] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.
[278] Telloglou, T., Triantafillou, E., Black, C., Benjakob, O., Scharf, A., Statius, T., Geiger, G., vas Dijken, K., Deeb, B., Sapoch, J., Howden, D., Gibbs, M. and Faull, L. (2022). *Flight of the Predator*.
[279] Μαραγκουδάκη, Δ. and Τριανταφύλλου, Ε. (2025). *Interceptions: the Last Act of a Cover*. [online] Solomon. Available at: https://wearesolomon.com/el/mag/format-el/reportaz/ypoklopes-i-teleftaia-praxi-mias-sygkalipsis/ [Accessed 21 Sep. 2025].

Lastly, Thalestris notes it also owned "Intellexa Solutions Ltd." in the British Virgin Islands as of 2021, though it noted its role in the entity structure was "dormant."[280] As at the end of 2021, Thalestris claimed to have 26 employees.[281]

Thalestris' 2021 financial statements offer insight into the revenue generated by the corporate group. The records show that it made 34,362,408 euros in revenue in 2021 and 29,260,165 euros in gross profit. **Notably, when broken down geographically, Thalestris made 29,490,695 euros in sales to the "Middle East," representing nearly 86% of all sales in 2021.**[282]

Table 3: Thalestris Revenue in 2021, broken down into geographic region

SMEX obtained corporate filing records belonging to Thalestris from the 2021 financial year.

Revenue in euros, broken down by market	Year: 2020	Year: 2021
Africa	1,023,000	901,300
Asia	1,997,000	1,497,000
Europe	4,269,311	2,267,193
LATAM	2,295,718	206,220
Middle East	11,229,050	29,490,695

Table: SMEX • Source: SMEX • Created with Datawrapper

[280] Thalestris Ltd. (2022). *Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*. [online] Companies Registration Office, Republic of Ireland, p.29.
[281] Thalestris Ltd. (2022). *Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*. p.23.
[282] Thalestris Limited (2022). *Annual Report and Consolidated Financial Statements for the Year Ended 31 December 2021*. p22.

The Cytrox/Intellexa Alliance Corporate Structure: The Thalestris Structure

This information is from publicly available corporate records and news reporting, as of 2022.

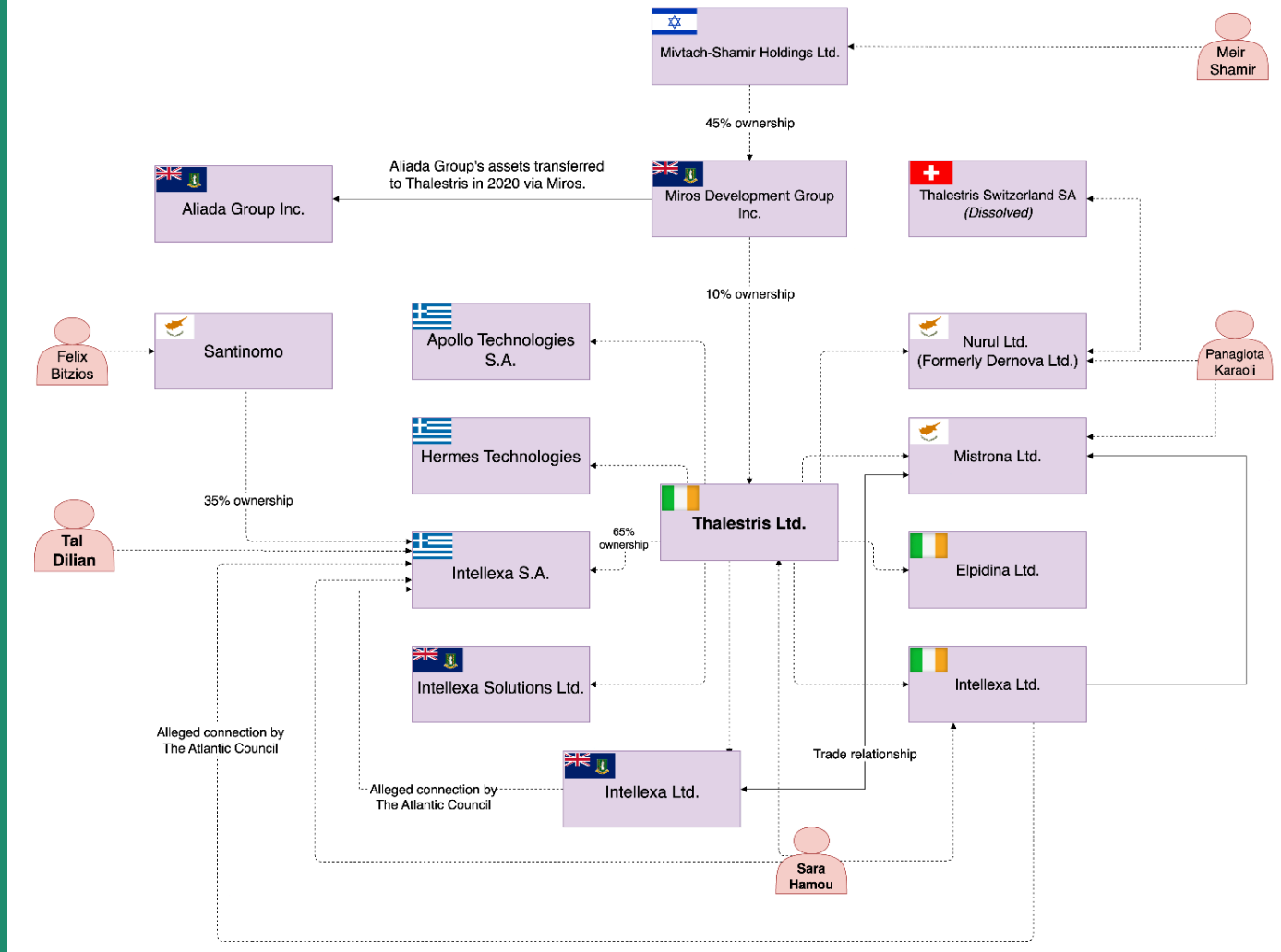


Image 13: The Thalestris corporate structure.

Intellexa Alliance Structure

In 2019, the Intellexa Alliance was announced as a partnership between the companies within the Intellexa Group and the Nexa Group.[283] An archived version of Intellexa[.]com from October 14, 2019, shows that Intellexa describes its founding members as Nexa Technologies, WiSpear, Cytrox, and SENPAI Technologies.[284] The Nexa Group, which is not a formal legal entity, has reportedly comprised of several entities including RB 42 (formerly Nexa Technologies), based in France; Setco Technology Solutions Ltd. (formerly Nexa Technologies CZ s.r.o.), based in the Czech Republic (currently being liquidated[285]); Advanced Middle East Systems FZ llc (also known by its acronym, 'AMES'), based in the UAE; Serpikom, based in France; DF Systems FZ-LLC (formerly Trovicor FZ-LLC, part of a group of companies now rebranded as Datafusion Systems), based in the UAE; and Boss Industries SAS, based in France. Boss Industries (registration no: 853 120 541) is the group's investor parent company.[286]

Nexa Technologies (registration no: 751 230 681) was founded in 2013 in France to take over French surveillance tech company Amesys's signature Eagle surveillance product, after Bull Group SA bought Amesys in 2010 (which later became Cerebro under Nexa). Nexa Technologies CZ was created in 2015 to pursue research and development (registration no: 04654951).[287] Advanced Middle East Systems FZ LLC (AMES, registration no: 21063) was founded in the UAE to sell Nexa Technologies products. It was also reportedly used to circumvent EU export restrictions.[288] In 2019, Boss Industries SAS acquired Trovicor Solutions FZ-LLC (registration no: 91646), which develops interception technology.[289] The Atlantic Council notes Serpikom likely joined the structure after 2019 (registration no: 492 531 371).[290] Nexa Group companies also have complex corporate histories and name changes, and tracing their history is beyond this report's scope.[291]

---

[283] Nexa Technologies (2019). *Intellexa Alliance*. [online] Nexa Technologies. Available at: https://web.archive.org/web/20200109072024/https:/www.nexatech.fr/intellexa-alliance-press-news [Accessed 29 Aug. 2025].
[284] Intellexa. (2019). *Intellexa | the Intelligence Alliance*. [online] Available at: https://web.archive.org/web/20191014000753/https://intellexa.com/ [Accessed 29 Aug. 2025].
[285] Kurzy.cz (2015). *Setco Technology Solutions s.r.o. V Likvidaci - Obchodní rejstřík, Úplný Výpis | Kurzy.cz*. [online] Kurzy.cz. Available at: https://rejstrik-firem.kurzy.cz/rejstrik-firem/DO-04654951-setco-technology-solutions-sro-v-likvidaci/ [Accessed 29 Aug. 2025].
[286] Amnesty International (2023). *The Predator Files: Caught in the Net*. [online] *Amnesty International*, London: UK: Amnesty International Ltd. Available at: https://www.amnesty.org/en/documents/act10/7245/2023/en/.
[287] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024). *Markets Matter: a Glance into the Spyware Industry*.
[288] Becker, S., Buschmann, R., Hoppenstedt, M., Naber, N. and Rosenbach, M. (2023). *The Predator Files: European Spyware Consortium Supplied Despots and Dictators*. [online] Der Spiegel. Available at: https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978 [Accessed 29 Aug. 2025].
[289] Clairfield. (2019). *Clairfield Advises Boss Industries on the Acquisition of the Dubai-based Company Trovicor -Clairfield*. [online] Available at: https://www.clairfield.com/transaction/clairfield-advises-boss-industries-on-the-acquisition-of-the-dubai-based-company-trovicor/ [Accessed 29 Aug. 2025].
[290] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024b). *Markets Matter: a Glance into the Spyware Industry*.
[291] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024). *Markets Matter: a Glance into the Spyware Industry*.

The Atlantic Council argues the hardware-software surveillance solutions created, marketed, and sold by Nexa Group companies may complement Intellexa Group spyware products, especially Cerebro, Nexa's mass-surveillance product.[292] According to an October 5, 2023, report from Amnesty International, the "main shareholders and former executives of Nexa Group" claim that the Intellexa Alliance no longer exists.[293]

[292] Roberts, J., Herr, T., Taylor, E. and Bansal, N. (2024). *Markets Matter: a Glance into the Spyware Industry*.
[293] European Investigative Collaborations and Amnesty International Security Lab (2023). *Global: 'Predator Files' Investigation Reveals Catastrophic Failure to Regulate Surveillance Trade*. [online] *Amnesty International*. Available at: https://securitylab.amnesty.org/latest/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/ [Accessed 29 Aug. 2025].

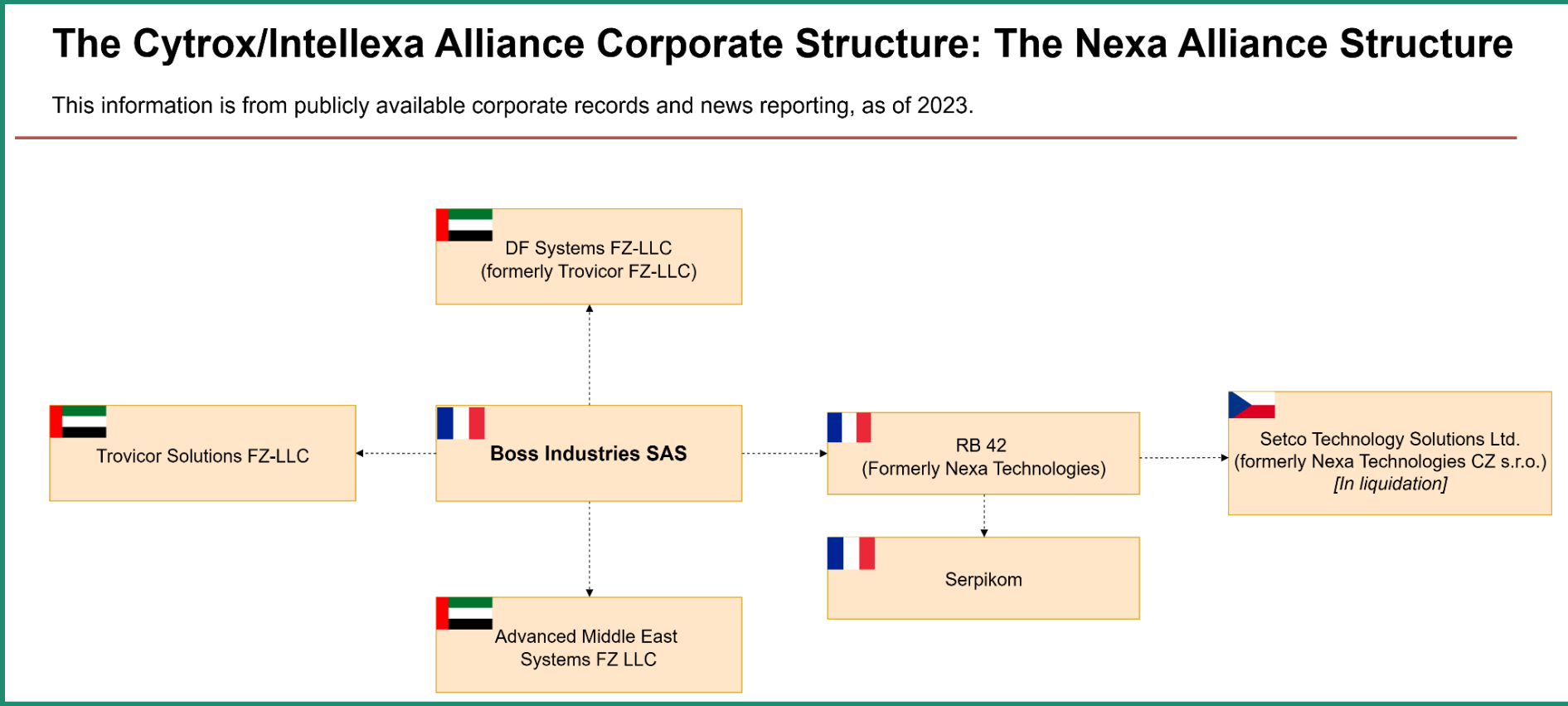


Image 14: The Nexa Alliance corporate structure.

The Czech Connection

In 2024, Czech investigative journalists at Investigate[.]cz found a new network of Czech entities that reportedly assisted Intellexa with marketing, consulting, and IT services. Dvir Horef Hazan, a Czech bistro entrepreneur with a programming background owned at least four Czech companies that appear to have worked with Intellexa.[294]

Three of his companies—Hadastech s.r.o.,[295] Zambrano Trade s.r.o.,[296] and Shilo s.r.o.[297]—all received a total of 2.9 million euros in payments from 2020 to 2023 from Intellexa companies. Hadastech appears to have ordered 40 shipments of "network equipment" and phones on behalf of Intellexa from an unnamed Ukrainian company, and Shilo hosted the same IP address as an Intellexa website.[298] Hadastech (registration no: 08980683), Zambrano Trade (registration no: 08629773), and Shilo (registration no: 10764186) are all liquidated or being liquidated. Hazan's fourth company connected to Intellexa, BenderOne s.r.o., is still active (registration no: 06627951).[299] It shares a building with another Czech company owned by a reported friend of Hazan: FoxITech s.r.o. owned by Michal Ikonomidis (registration no: 14243873).[300] According to Insikt Group, FoxITech hosts network infrastructure associated with Predator spyware.[301] It is unclear which entities from Intellexa paid Hazan for his services.

---

[294] Šotová, Z. and May, P. (2024). *The Magic Maker: Why Is a Czech Bistro Owner Working for Intellexa? - VSquare.org*.
[online] VSquare.org. Available at: https://vsquare.org/greece-czech-republic-intellexa-cytrox-spyware/ [Accessed 29 Aug. 2025].
[295] Kurzy.cz (2024). *Hadastech s.r.o. v likvidaci, Krnov IČO 08980683 - Obchodní rejstřík firem*. [online] Kurzy.cz. Available at: https://rejstrik-firem.kurzy.cz/08980683/hadastech-s-r-o-v-likvidaci/ [Accessed 29 Aug. 2025].
[296] Kurzy.cz (2024). *ZAMBRANO trade s.r.o. v likvidaci , Krnov IČO 08629773 - Obchodní rejstřík firem*. [online] Kurzy.cz. Available at: https://rejstrik-firem.kurzy.cz/08629773/zambrano-trade-s-r-o-v-likvidaci/ [Accessed 29 Aug. 2025].
[297] Kurzy.cz (2024). *Shilo s.r.o. v likvidaci, Krnov IČO 10764186 - Obchodní rejstřík firem*. [online] Kurzy.cz. Available at: http://rejstrik-firem.kurzy.cz/10764186/shilo-s-r-o-v-likvidaci/ [Accessed 29 Aug. 2025].
[298] Šotová, Z. and May, P. (2024). *The Magic Maker: Why Is a Czech Bistro Owner Working for Intellexa?*
[299] Kurzy.cz (2024a). *BENDER ONE s.r.o. , Krnov IČO 06627951 - Obchodní rejstřík firem*. [online] Kurzy.cz. Available at: https://rejstrik-firem.kurzy.cz/06627951/bender-one-sro/ [Accessed 29 Aug. 2025].
[300] Kurzy.cz (2025). *FoxITech s.r.o. , Krnov IČO 14243873 - Obchodní rejstřík firem*. [online] Kurzy.cz. Available at: https://rejstrik-firem.kurzy.cz/14243873/foxitech-sro/ [Accessed 29 Aug. 2025].
[301] Insikt Group (2025a). *Predator Still Active, with New Client and Corporate Links Identified*. [online] *Recorded Future*. Recorded Future. Available at: https://www.recordedfuture.com/research/predator-still-active-new-links-identified [Accessed 29 Aug. 2025].

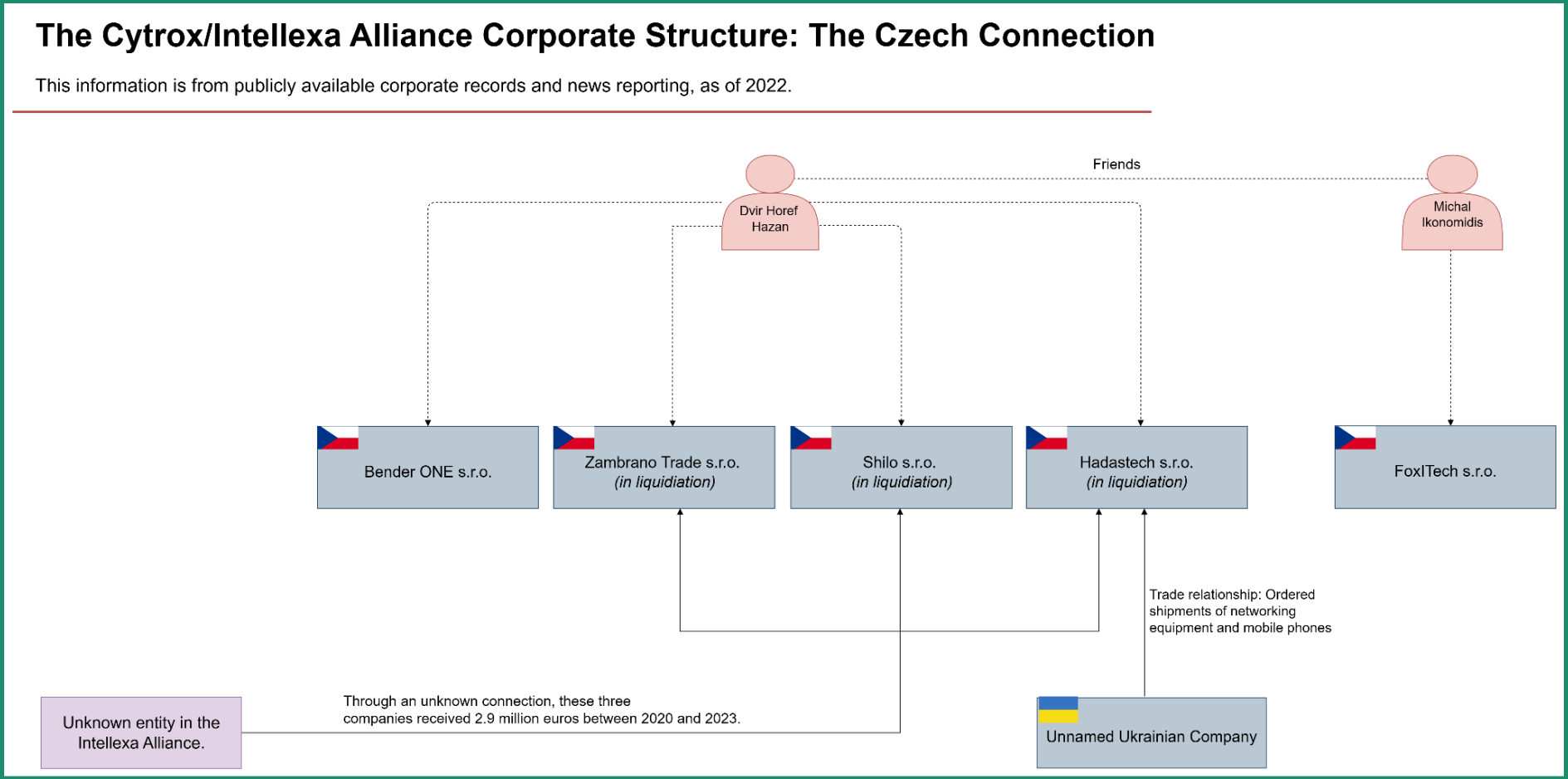


Image 15: The corporate structure of Czech entities with a relationship with Intellexa.

It is ultimately uncertain to what extent the Intellexa Group or Alliance are active in 2025. Multiple entities in the Intellexa Group and Nexa Group (which together made up the Intellexa Alliance) seem to still be active in mid-2025, according to business registration records:[302]

Israel

- Balinese Ltd.[303]
- Peterbald Ltd.[304]
- SENPAI Technologies Ltd.[305]

France

- RB 42[306]
- Boss Industries SAS[307]
- Serpikom[308]

Ireland

- Thalestris Limited[309]
- Intellexa Limited[310]
- Elpidina Limited[311]

Greece

- Apollo[312]
- Hermes[313]
- Intellexa S.A.[314] (registration is suspended)

Cyprus

- Nurul Ltd.[315]

---

[302] This is not an exhaustive list and represents what SMEX was able to obtain as of writing. SMEX was not able to confirm the registration status of some corporate entities within jurisdictions that prove a bit more difficult to to get documentation from—such as Miros Development Group Inc., Intellexa Limited, and Intellexa Solutions Limited in the British Virgin Islands.
[303] CheckID (2025). *BALINESE LTD - 515692135*.
[304] CheckID (2025c). *PETERBALD LTD - 515693893*.
[305] CheckID (2025). *Haxton Group Ltd. / HEXATONE GROUP LTD - 515385748*.
[306] National Institute of Industrial Property (2024). French Companies Register: RB 42 - SIREN 751 230 681. [online] Available at: https://data.inpi.fr/entreprises/751230681?q=RB%2042#751230681 [Accessed 28 Aug. 2025].
[307] National Institute of Industrial Property (2024). French Companies Register: BOSS INDUSTRIES - SIREN 853 120 541. [online] Available at: https://data.inpi.fr/entreprises/853120541?q=Boss%20industries#853120541 [Accessed 28 Aug. 2025].
[308] National Institute of Industrial Property (2024). French Companies Register: SERPIKOM - SIREN 492 531 371. [online] Available at: https://data.inpi.fr/entreprises/492531371?q=Serpikom#492531371 [Accessed 28 Aug. 2025].
[309] Irish Trade Registry (2023). Company Search: Entry for Thalestris Limited - 661545. [online] Available at: https://traderegistry.ie/company-search/ [Accessed 29 Aug. 2025].
[310] Irish Trade Registry (2023). Company Search: Entry for Intellexa Limited - 665443. [online] Available at: https://traderegistry.ie/company-search/ [Accessed 29 Aug. 2025].
[311] Irish Trade Registry (2023). Company Search: Entry for Elpidina Limited - 687102. [online] Available at: https://traderegistry.ie/company-search/ [Accessed 29 Aug. 2025].
[312] Hellenic Republic Ministry of Development (2025). GEMI Public Records: Entry for APOLLO TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ.
[313] Hellenic Republic Ministry of Development (2025). GEMI Public Records: Entry for HERMES TECHNOLOGIES ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ.
[314] Hellenic Republic Ministry of Development (2020). GEMI Public Records: Entry for INTELLEXA ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ. [online] Available at: https://publicity.businessportal.gr/company/154460701000 [Accessed 28 Aug. 2025].
[315] Nurul Ltd. (2024). Registration Details for Nurul Ltd.

- Mistrona Ltd.[316]

British Virgin Islands

- Aliada Group Inc.[317]

United Arab Emirates

- Advanced Middle East Systems[318]
- Trovicor Solutions FZ-LLC[319]
- DF Systems FZ-LLC[320]

We ultimately know what we know about the Alliance through leaks, public statements, and promotional materials. Yet there is no recent public evidence that suggests Intellexa Alliance-affiliated companies are currently collaborating on sales projects. While many of these corporate entities sitting under Thalestris are still legally active, it is unclear which are actively trading in 2025.

Changing Ownership of Predator

In 2023 as part of Amnesty International's "Predator Files" investigation, Der Spiegel reported that AMES was the official entity through which Intellexa sold Predator to Egypt and Vietnam at the end of 2020.[321]

On March 5, 2024, the US Treasury Department Office of Foreign Assets Control formally sanctioned multiple people and entities associated with the Intellexa Alliance, including Tal Dilian, Sara Hamou, Intellexa S.A., Intellexa Limited, Cytrox AD, Cytrox Holdings Zrt, and Thalestris Limited.[322] [323] Yet in spite of the growing tide against Predator and its developers, Predator still appears to be actively in use in the wild.

On March 1, 2024, Recorded Future's Insikt Group released a report identifying evidence of Predator being operated in multiple countries over the previous twelve months, including

[316] Mistrona Ltd. (2023). Registration Details for Mistrona Ltd.
[317] OpenSanctions. (2025). *Aliada Group Inc*. [online] Available at: https://www.opensanctions.org/entities/NK-fMNGjhDzoCeprF53r9hapr/ [Accessed 29 Aug. 2025].
[318] UAE National Economic Register (2025). Business License Details: Entry for Advanced Middle East Systems. [online] Available at: https://ner.economy.ae/Search_By_BN.aspx [Accessed 29 Aug. 2025].
[319] UAE National Economic Register (2025). Business License Details: Entry for Trovicor Solutions FZ. [online] Available at: https://ner.economy.ae/Search_By_BN.aspx [Accessed 29 Aug. 2025].
[320] UAE National Economic Register (2025). Business License Details: Entry for DF Systems FZ-LLC.
[321] Becker, S., Buschmann, R., Hoppenstedt, M., Naber, N. and Rosenbach, M. (2023). *The Predator Files: European Spyware Consortium Supplied Despots and Dictators*.
[322] U.S. Department of the Treasury. (2024). *Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium*.
[323] According to the Treasury Department, Intellexa S.A. exports the Intellexa Alliance's surveillance tools to "authoritarian regimes"; Greece-based Intellexa Limited resells technology for the Alliance and maintains assets; Cytrox AD develops Predator; Cytrox Zrt helped develop Predator; and Thalestris functions as a holding company for Intellexa. The Treasury Department first sanctioned Cytrox AD, Cytrox Holdings Zrt, Intellexa Limited, and Intellexa S.A. on July 18, 2023, but has since taken down its webpage about the sanctioning.

Egypt, Oman, and Saudi Arabia.[324] On June 12, 2025, Insikt Group released another report in which it claimed it identified new infrastructure associated with Predator operators.[325] While the original Cytrox-affiliated entities set up in Hungary and North Macedonia appear to be defunct, the Intellexa Group itself now reportedly produces Predator.[326]

Intellexa's WANA footprint, like NSO Group, is largely connected to its presence and business connections in Israel. The Intellexa Alliance had a corporate presence in the UAE through Advanced Middle East Systems and the Trovicor/Datafusion Systems entities, all three of which are still active as of writing. This report's dataset, based on public reporting, suggests that at least four WANA countries have used Predator.

Marketing: "The Good Guys"

Unlike NSO Group, the Intellexa Group does not actively try to market its business on social media - and neither did Cytrox while it was active. However, the public comments made by the Intellexa Alliance and its leaders provide insight into how they frame their products.[327]

On a 2019 version of Intellexa's website, the Intellexa Alliance is branded as providing "law enforcement and intelligence agencies with a comprehensive portfolio of premium, best of breed intelligence solutions."[328] A 2021 version of the website specifically markets "tactical interception."[329] At multiple points over time, Intellexa's website and marketing materials frame the business as being "EU-based and regulated."[330] [331]

According to Amnesty International's 2023 reporting on Intellexa Alliance, former Nexa executives told Amnesty researchers that all "commercial relationship[s]" were grounded in "full compliance with applicable regulations," insisting that all engagements with the Nexa Group followed EU law.[332] However, Intellexa Group–affiliated entities have exported Predator to a number of countries that have used it for human rights abuses, such as Sudan.[333]

---

[324] Insikt Group (2024). *Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices*. [online] Recorded Future. Available at: https://www.recordedfuture.com/research/predator-spyware-operators-rebuild-multi-tier-infrastructure-target-mobile-devices [Accessed 13 Aug. 2025].
[325] Insikt Group (2025). *Predator Still Active, with New Client and Corporate Links Identified*.
[326] European Investigative Collaborations and Amnesty International Security Lab (2023). *Global: 'Predator Files' Investigation Reveals Catastrophic Failure to Regulate Surveillance Trade*.
[327] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.
[328] Intellexa. (2019). *Intellexa | the Intelligence Alliance*.
[329] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R., Aljizaw, N. and Anstis, S. (2021). *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*.
[330] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R., Aljizaw, N. and Anstis, S. (2021). *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*.
[331] Fox, M. (2023). Intellexa: Irish-linked Spyware Used in 'brazen attacks' - Report. *BBC*. [online] 21 Oct. Available at: https://www.bbc.com/news/articles/c0wxr9rnnxeo [Accessed 3 Aug. 2025].
[332] European Investigative Collaborations and Amnesty International Security Lab (2023). *Global: 'Predator Files' Investigation Reveals Catastrophic Failure to Regulate Surveillance Trade*.
[333] DR Lab (2022). Sudan: 'Men with no Mercy' now Armed with EU-linked Spyware. *SMEX*. Available at: https://smex.org/sudan-men-with-no-mercy-now-armed-with-eu-linked-spyware/ [Accessed 17 Jul. 2025].

Intellexa's LinkedIn page, which is not explicitly affiliated with any specific Intellexa Alliance/Group entity, frames its work in terms of a "digital race" between law enforcement and criminals taking advantage of "widespread encryption."

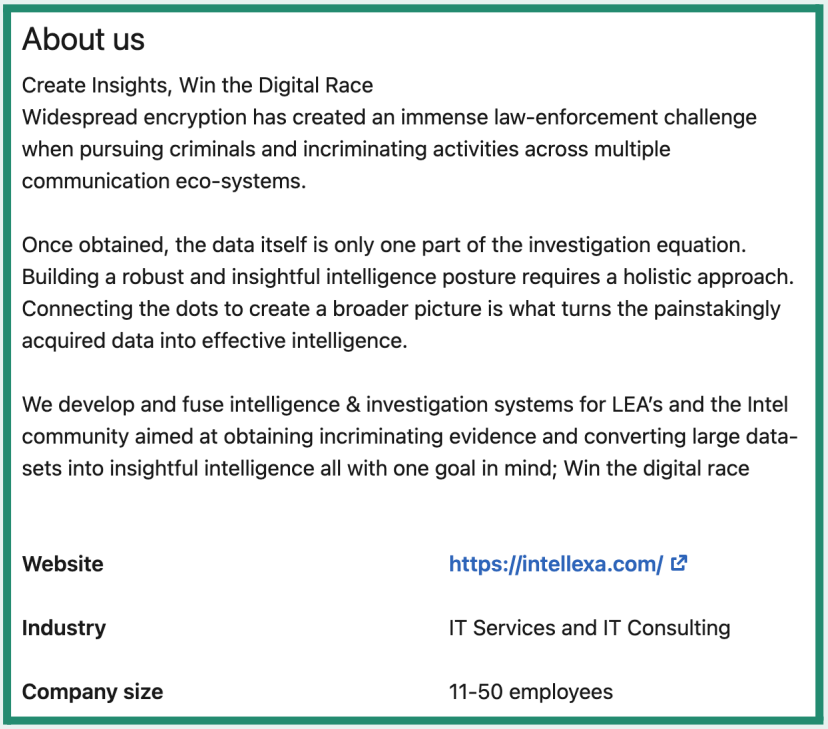


Image 16: Intellexa's LinkedIn page describes its work as delivering insightful intelligence for law enforcement agencies (LEAs) and the intelligence community.[334]

On August 6, 2019, Forbes published a rosy interview with Tal Dilian, describing in detail the capabilities of a "$9 Million WhatsApp Hacking Van" he designed.[335] According to Forbes, the "hacking van" demonstrates the capabilities of the then-new Intellexa Alliance. Depicting Dilian as "a shabbier, more hirsute George Clooney," Forbes reported that Intellexa was "talking up a new age of openness" in the CSV market, and created a "one-stop-shop, cyber arsenal for cops in the field."

Like NSO Group, Dilian's comments suggest he markets Intellexa as a business that only works with "the good guys." Dilian told Forbes he designed his products to surveil the worst of criminals. When Forbes pressed Dilian on the reported human rights abuses of the spyware industry, Dilian dismissed the concerns. He stated**, "We are not the policemen of the world … We work with the good guys. And sometimes the good guys don't behave."[336]** Dilian argued it is the job of the governments that regulate the sale and use of spyware to protect vulnerable populations from abuses—not the job of the companies that create it. That is, when the good guys misbehave (by abusing spyware and violating human rights), it

[334] Intellexa (2025). *Intellexa's About page*. [LinkedIn]. [Accessed 11 Aug. 2025]. Available from: https://www.linkedin.com/company/intellexa/about/
[335] Brewster, T. (2019). *A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*.
[336] Brewster, T. (2019). *A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*.

is not the problem of the spyware vendor. “The universe,” Dilian told Forbes, “in a way needs our product.” [337]

Much of how the Intellexa Group markets its spyware offerings revolves around the idea of not knowing exactly where and how its customers operate its products.[338] Like NSO Group, the spyware maker notes in the leaked proposal from 2022 that “cloud services, domains, and [the] anonymization chain” are the responsibility of the customer. The company thus offloads much of the responsibility associated with exposure. Intellexa reinforces this in the way it delivers its products to customers—it uses “cost insurance and freight” and/or “delivery at terminal,” meaning it delivers its products to customers at airports.[339] This further removes the company from the process and location of the spyware operator systems. As Talos Intelligence notes, this creates a useful sense of plausible deniability.[340]

Sophie in 't Veld, a former member of the European Parliament and the rapporteur on a European Parliament PEGA report investigating the use of surveillance spyware, argued in an August 2022 press conference that Intellexa used claims of EU regulation as a sales technique.[341] Veld further alleged Intellexa was in breach of EU export regulations and would not cooperate with EU authorities.[342] As the Intellexa brand grew increasingly implicated that year in a scandal in which the Greek government spied on opposition party members and journalists with Predator, lawyers representing Intellexa responded to Veld with the following:[343]

“Unfortunately, the upcoming Greek elections cause the media to recycle legends and fairy tales concerning our activities. We have no intention [of] participating in this witch hunt as we are not part of the election campaign. We are fully regulated under EU regulation, act in compliance with the law and continue cooperating with the relevant competent authorities.”[344]

Harkening back to NSO Group’s mythbusting LinkedIn posts, lawyers representing Dilian insisted the Intellexa Alliance’s work is fully compliant with EU law. Dilian also framed accusations of wrongdoing against him as a “witch hunt” in 2019, after authorities in

---

[337] Brewster, T. (2019). *A Multimillionaire Surveillance Dealer Steps out of the Shadows . . . and His $9 Million WhatsApp Hacking Van*.
[338] Ventura, V. (2023). Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware. *Talos Intelligence Blog*. Available at: https://blog.talosintelligence.com/intellexa-and-cytrox-intel-agency-grade-spyware/ [Accessed 2 Aug. 2025].
[339] Ventura, V. (2023). Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware.
[340] Ventura, V. (2023). Intellexa and Cytrox: from fixer-upper to Intel Agency-grade Spyware.
[341] Multimedia Centre at the European Parliament. (2022). *Press conference by Sophie IN 'T VELD, rapporteur on the PEGA Draft Report - Multimedia Centre*. [online] Available at: https://multimedia.europarl.europa.eu/en/webstreaming/press-conference-by-sophie-in-t-veld-rapporteur-on-pega-draft-report_20221108-1100-SPECIAL-PRESSER [Accessed 29 Aug. 2025].
[342] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.
[343] Τέλλογλου, T. and Τριανταφύλλου, E. (2022). *Greece Spyware scandal: How the Greek Government Is Tied to the Israeli Company Intellexa*. [online] Greek News on Demand . Available at: https://greeknewsondemand.com/2022/11/30/greece-spyware-scandal-how-the-greek-government-is-tied-to-the-israeli-company-intellexa/ [Accessed 29 Aug. 2025].
[344] Cvetkoska, S., Nasteska, I., Stojanovski, B., Telloglou, T., Triantafillou, E. and Simonovska, M. (2023). *Israeli Company Developed Spyware in Skopje, Local Officials Looked the Other Way - IRL*.

Larnaca, Cyprus, launched an investigation into Dilian and seized his "spy van" after he boasted about its capabilities in his interview with Forbes.[345] However, the Intellexa Alliance's use of subsidiaries located throughout the world, particularly in the UAE, tell a different story—that of avoiding the EU's dual-use export regulations.

Premier Products and Capabilities: Predator

Predator is Cytrox's signature spyware, now sold and marketed under the Intellexa brand. Predator, like Pegasus, grants operators full control over a target's phone.[346] While attempting to hide its activity, Predator can access the victim's camera, microphone, contacts, messages, photos, videos, and other data points without their knowledge. According to Insikt Group, Predator is written in Python to be modular, allowing operators to update the features they use remotely.[347] Predator can be delivered to victims via one-click or zero-click exploits. Operators can thus rely on social engineering to get a victim to interact with an operator, like clicking on a malicious link, or use a technique that does not require user interaction, like network injection attacks.[348]

Amnesty International highlights that Predator is sold as a package of software and infrastructure. Predator is sold along with a web-based interface to launch and manage spyware infections, which Intellexa markets as the Cyber Operation Platform.[349] According to Amnesty International, the Intellexa Alliance markets its spyware products with several names all relating to Predator: Green Arrow for its Android agent, Red Arrow for its iOS agent, Helios, and NOVA. Amnesty International assesses that all of Intellexa's offerings refer to the same spyware product produced first by Cytrox AD.[350]

Predator uses a specially set-up "installation" network, from which spyware is sent to target devices.[351] Infected devices connect to an Intellexa-owned command-and-control network, allowing customers operating Predator to use commands to control the infected device. The operator's commands are sent through an "anonymization network," which aims to hide the location and identity of those using Predator. Insikt Group also documented Predator customers relying on "multi-tiered infrastructure networks," aiming to further hide operators of the malware.[352]

Insikt Group notes that while previous reporting on Predator highlighted its reliance on domains spoofing well-known organizations, such as news outlets, Predator began to use other techniques toward the end of 2023.[353] Insikt Group observed a variety of malicious

---

[345] TOI Staff and AFP (2019). *Israeli spy-tech CEO Wanted for Questioning by Cypriot Police*. [online] Times of Israel. Available at: https://www.timesofisrael.com/israeli-spy-tech-ceo-wanted-for-questioning-by-cypriot-police/ [Accessed 29 Aug. 2025].
[346] Insikt Group (2025). *Predator Still Active, with New Client and Corporate Links Identified*.
[347] Insikt Group (2025). *Predator Still Active, with New Client and Corporate Links Identified*.
[348] Amnesty International (2023). *The Predator Files: Caught in the Net*. p.16.
[349] Amnesty International (2023). *The Predator Files: Caught in the Net*. [online] *Amnesty International*, London: UK: Amnesty International Ltd., p.21. Available at: https://www.amnesty.org/en/documents/act10/7245/2023/en/.
[350] Amnesty International (2023). *The Predator Files: Caught in the Net*. p.21.
[351] Amnesty International (2023). *The Predator Files: Caught in the Net*. p.22.
[352] Amnesty International (2023). *The Predator Files: Caught in the Net*. p.22.
[353] Insikt Group (2025). *Predator Still Active, with New Client and Corporate Links Identified*.

links being used as a single-click infection vector, sometimes using non-English-language words to appeal to targets' language preferences. Predator operators also appear to be using different tactics to avoid detection, such as newer server configurations and fake websites.[354] Predator operators' tactic adjustments reflect the cat-and-mouse nature of cybersecurity: as more researchers began to document, name, and shame Predator, Predator operators began developing new tactics to evade detection.

Several major leaks have emerged over the past half decade that suggest how much the Intellexa Group charges for its spyware—in brief, a hefty price. In 2022, the New York Times reported a previously unseen price proposal for Predator in 2021.[355] One order of Predator—including one-click remote data extraction from Android and iOS devices, the ability to infect 20 devices concurrently, and 400 total successful injections—cost 13.6 million euros. The contract came with a 12-month warranty, hardware and software required to run Predator, an Intellexa-designed "project plan," multimodal technology training, 24/7 support, and geographic limitations. It also offered several "optional products and services," including a second-year "maintenance contract" for 25% of the contract per year (about 3.4 million euros), the option to target phones outside of a customer's country, persistency (the ability to "survive phone shut-down and re-boot") for 2.4 million euros, and "SpearHead 360," described as a "Wi-Fi intelligence solution mounted on a covert mission vehicle," for 4.5 million euros.

In 2022, another price proposal for an Intellexa product was leaked online—this time for its NOVA spyware-data analysis package, which also offered remote data extraction from Android and iOS devices.[356] NOVA was sold under a package deal for 8 million euros. This package included a one-click infection vector, 10 concurrent infections across Android and iOS device families, and 100 total successful infections. Like the 2021 basic Predator package, NOVA was offered only within an operator's country. Customers could purchase persistence for 3 million euros for Android and iOS targets and the ability to target devices within 5 additional countries, seemingly anywhere in the world, for 1.2 million euros extra (billed as "NOVA international").[357] NOVA's offer similarly included a 12-month warranty, hardware and software required to run the product, a "complete project plan," and training sessions for operators. Both the NOVA and Predator proposals supported infections for Android and iOS versions up to 12 months older than the most recent operating system version.[358]

---

[354] Insikt Group (2025). *Predator Still Active, with New Client and Corporate Links Identified*.
[355] The New York Times (2022). *Read the Intellexa Pitch on Its Predator Spyware Tool*. [online] Archive.org. Available at:https://web.archive.org/web/20250616044003/https://www.nytimes.com/interactive/2022/12/08/us/politics/intellexa-commercial-proposal.html [Accessed 29 Aug. 2025].
[356] vxunderground. (2022) [X (formerly Twitter)] *25 August, 2022*. Available at: https://x.com/vxunderground/status/1562725121277988865 (Accessed: 20 July 2025)
[357] Amnesty International Security Lab (2023). *Predator Files: Technical deep-dive into Intellexa Alliance's Surveillance Products*. [online] *Amnesty International*. Available at: https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/ [Accessed 2 Aug. 2025].
[358] Amnesty International Security Lab (2023). *Predator Files: Technical deep-dive into Intellexa Alliance's Surveillance Products*

Indicators of compromise and MITRE ATT&CK tactics, techniques, and procedures associated with Predator have been widely shared, such as by Insikt Group in 2024.[359]

Prominent Attack

In late 2023, Citizen Lab released a report investigating a high-profile use case of Predator targeting a prominent Egyptian politician.

From May to September 2023, a Predator operator targeted former Egyptian member of Parliament Ahmed Altantawy, after announcing his intentions to challenge Egyptian President Abdel Fatah el-Sisi in the 2024 Egyptian presidential elections.[360] Following his announcement, Egyptian authorities arrested several of his family members, and he grew concerned for his digital and physical safety.[361] [362] According to Feldstein and Kot (2023) and additional reports analyzed by SMEX, Egypt under el-Sisi has repeatedly appeared to use spyware against dissidents.[363] El-Sisi is well known for running a government of repression and opposing political opponents with an iron fist.[364]

Altantawy turned his phone over to Citizen Lab, whose investigation into his device revealed multiple attempts to install Predator on the device. Their investigation found that between August and September 2023, Altantawy's mobile connection, run through Vodafone Egypt, was "persistently selected for targeting via network injection."[365] When he visited unsecure websites not using HTTPS, he was automatically redirected to malicious sites by a device within Vodafone Egypt's network to install a Predator payload and infect his phone. As Citizen Lab highlights, this points to a larger insecurity issue within the network layer, which threat actors and spyware operators can exploit to deploy malicious payloads on victim devices.[366]

---

[359] Insikt Group (2024). *Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices*.
[360] Marczak, B., Scott-Railton, J., Abdul Razzak, B., Deibert, R., Roethlisberger, D. and Anstis, S. (2023). *PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions*. [online] *Citizen Lab*. University of Toronto. Available at: https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/ [Accessed 7 Aug. 2025].
[361] Saafan, F. (2023). Egyptian ex-MP Planning Presidential Bid Says Relatives Arrested. *Reuters*. [online] 4 May. Available at: https://www.reuters.com/world/africa/egyptian-ex-mp-planning-presidential-bid-says-relatives-arrested-2023-05-04/ [Accessed 29 Aug. 2025].
[362] Human Rights Watch (2023). *Egypt: Mass Arrests Target Family, Supporters of ex-MP*. [online] Human Rights Watch. Available at: https://www.hrw.org/news/2023/05/05/egypt-mass-arrests-target-family-supporters-ex-mp [Accessed 3 Aug. 2025].
[363] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive?*
[364] Amnesty International. (2019). *Unprecedented Repression Six Years since Fall of Morsi*. [online] Available at: https://www.amnesty.org/en/latest/news/2019/07/egypt-series-of-draconian-laws-legalizes-unprecedented-repression-six-years-since-fall-of-morsi-2/ [Accessed 29 Aug. 2025].
[365] Marczak, B., Scott-Railton, J., Abdul Razzak, B., Deibert, R., Roethlisberger, D. and Anstis, S. (2023). *PREDATOR IN THE WIRES*.
[366] Marczak, B., Scott-Railton, J., Abdul Razzak, B., Deibert, R., Roethlisberger, D. and Anstis, S. (2023). *PREDATOR IN THE WIRES*.

Predator operators also attempted to target Altantawy via SMS and WhatsApp social engineering, relying on messages spoofing WhatsApp URLs. The operator said that another user logged into his WhatsApp account and that he needed to "terminate" the session for his security using a likely malicious link.[367] Social engineers characteristically push victims into making rash decisions by suggesting an action is required or timely, thus playing into human emotions to trigger a desired outcome.[368] Another individual impersonating a human rights defender also reached out to Altantawy on WhatsApp, attempting to push him into clicking a malicious link connected with Predator infection payloads. Citizen Lab attributed the actions with high confidence to the Egyptian government.[369]

In February 2024, an Egyptian court found Altantawy guilty of forging election documents and barred him from running in upcoming elections.[370] He was also forced to pay a fine of 20,000 Egyptian pounds and received a suspended one-year prison sentence. He was later sentenced in May 2024 to one year in prison with labor.[371]

[367] Marczak, B., Scott-Railton, J., Abdul Razzak, B., Deibert, R., Roethlisberger, D. and Anstis, S. (2023). *PREDATOR IN THE WIRES*.
[368] IBM (2022). *What is Social Engineering?* [online] IBM. Available at: https://www.ibm.com/think/topics/social-engineering [Accessed 5 Aug. 2025].
[369] Marczak, B., Scott-Railton, J., Abdul Razzak, B., Deibert, R., Roethlisberger, D. and Anstis, S. (2023). *PREDATOR IN THE WIRES*.
[370] Reuters Staff (2024). Ex-Egyptian Presidential Candidate Tantawy Found Guilty of forgery, Sources Say. *Reuters*. [online] 6 Feb. Available at: https://www.reuters.com/world/africa/ex-egyptian-presidential-candidate-tantawy-found-guilty-forgery-sources-2024-02-06/.
[371] Saafan, F. (2024). Egypt Jails Former Presidential Hopeful for One Year with Labour. *Reuters*. [online] 27 May. Available at: https://www.reuters.com/world/africa/egypt-jails-former-presidential-hopeful-one-year-with-labour-2024-05-27/ [Accessed 6 Aug. 2025].

3.3 Cellebrite

"Some of our solutions may be used by customers in a way that is, or that is perceived to be, incompatible with human rights."

—Cellebrite in its Form 20-F SEC Filing for 2024[372]

Company Background and WANA Footprint

Cellebrite is a large, multinational corporation selling digital forensics solutions and intelligence to law enforcement agencies and governments across the world. Avi Yablonka, Yuval Aflalo, and Yaron Baratz founded Cellebrite in Israel in 1999.[373] Unlike the other CSVs analyzed in this report, Cellebrite is a publicly traded company on the US-based NASDAQ index, meaning it must make certain information publicly available per public SEC filing requirements. As per Cellebrite's latest filings in 2024, Cellebrite (NASDAQ ticker: CLBT; CIK: 0001854587[374]) reported $401 million in revenue; $56.9 million in operating income; and 1,167 global employees.[375] Cellebrite claims that it has a customer base of 7,000 global clients, and that 90% of its revenue from 2022, 2023, and 2024 has come from contracts with law enforcement agencies and government clients.[376] Cellebrite boasts that it has customers in over 100 countries, and reported that its sales to the Europe, Middle East, and Africa geographic market constituted 53.7% of all revenue in 2024.[377] [378]

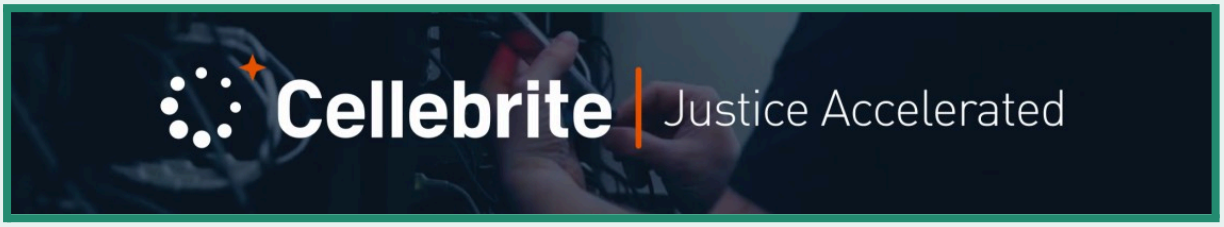


Image 17: Cellebrite's logo displayed on its LinkedIn page.[379]

[372] Cellebrite DI Ltd. (2025). *Form 20-F*. [online] Securities and Exchange Commission, p.20. Available at: https://investors.cellebrite.com/static-files/7bf7cec5-50b6-4f1e-99f4-f7f8238e1d2a [Accessed 29 Aug. 2025].
[373] Shulman, S. (2025). *From Bootstrapped Startup to a $5B powerhouse: Cellebrite's Outgoing CEO Reflects on 19 Years of Highs and Con*. [online] CTech. Available at: https://www.calcalistech.com/ctechnews/article/lhck15vtj [Accessed 29 Aug. 2025].
[374] Securities and Exchange Commission (2025). EDGAR | Company Search Results: Cellebrite DI Ltd. - 0001854587. [online] Available at: https://www.sec.gov/edgar/browse/?CIK=1854587&owner=exclude [Accessed 28 Aug. 2025].
[375] Cellebrite DI Ltd. (2025). *Form 20-F*. p.12, 80-86.
[376] Cellebrite DI Ltd. (2025). *Form 20-F*. p.22, 58.
[377] Cellebrite. (2025). *Newsroom*. [online] Available at: https://cellebrite.com/en/newsroom/ [Accessed 29 Aug. 2025].
[378] Cellebrite DI Ltd. (2025). *Form 20-F*. p.194.
[379] Cellebrite (2025). *Cellebrite's home page*. [LinkedIn]. [Accessed 13 Aug. 2025]. Available from: https://www.linkedin.com/company/cellebrite/

Cellebrite's business offerings initially focused on data transfer solutions for mobile devices.[380] A version of Cellebrite's webpage in 2000 displays this clearly, advertising its "Cellular Phones Memory Exchanger."[381]

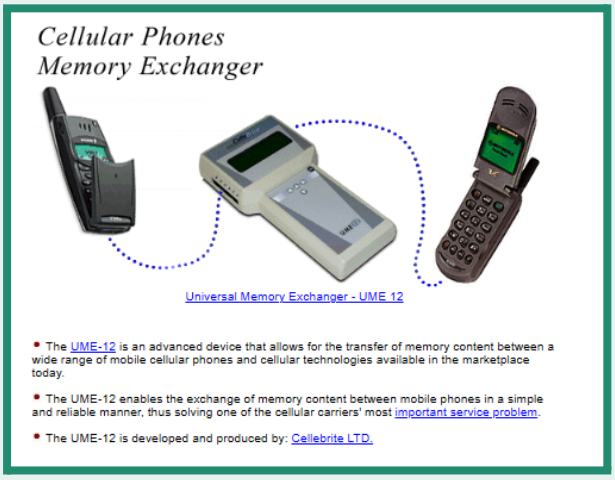


Image 18: Cellebrite's website in 2000 advertises its first data transfer services.

Cellebrite pivoted into digital forensics in 2007 when it introduced the Universal Forensics Extraction Device (UFED), a digital forensics device that claims to be the "industry standard for lawfully accessing and collecting digital data."[382]

As Cellebrite made this shift, it began to grow globally and acquired several large investments. FutureDial Incorporated and Sun Corporation, one of its majority shareholders, acquired Cellebrite in 2007.[383] All three founders sold their shares to Sun for a reported $17.5 million.[384] Israeli Growth Partners, a tech investment fund, invested $110 million into Cellebrite in 2019, valuing the corporation at $440 million.[385] In January 2020 Cellebrite expanded its product offerings to computers when it bought BlackBag Technologies, a digital forensics firm specializing in computer forensics.[386] It gained a 25% stake in the company. Cellebrite announced in April 2021 that it was planning to merge with TWC Tech Holdings II Corporation, which would lead to Cellebrite's listing on the NASDAQ exchange.[387] This valued Cellebrite at $2.4 billion. On July 16, 2024, Cellebrite acquired cybersecurity and incident

[380] Shulman, S. (2025). *From Bootstrapped Startup to a $5B powerhouse.*
[381] Cellebrite. (2000). *Cellebrite LTD - Mobile Cellular Phone Memory Exchanger*. [online] Available at: https://web.archive.org/web/20001018130340/http://www.cellebrite.com/ [Accessed 29 Aug. 2025].
[382] Cellebrite (2024). *Cellebrite UFED | Access and Collect Mobile Device Data*. [online] Cellebrite. Available at: https://cellebrite.com/en/ufed/ [Accessed 29 Aug. 2025].
[383] Crunchbase. (n.d.). *Cellebrite Acquired by FutureDial*. [online] Available at: https://www.crunchbase.com/acquisition/futuredial-acquires-cellebrite--8a593335 [Accessed 29 Aug. 2025].
[384] Shulman, S. (2025). *From Bootstrapped Startup to a $5B powerhouse.*
[385] Hazani, G. (2019). IGP Acquires 25% Stake in Mobile Forensics Firm Cellebrite for $110 Million. *CTech*. [online] 17 Jun. Available at: https://www.calcalistech.com/ctech/articles/0,7340,L-3764425,00.html [Accessed 29 Aug. 2025].
[386] Miller, C. (2020). *Cellebrite Expands to Computers with $33M Acquisition of BlackBag Technologies Forensics Firm - 9to5Mac*. [online] 9to5Mac. Available at: https://9to5mac.com/2020/01/14/cellebrite-blackball-technologies-acquistino/ [Accessed 29 Aug. 2025].
[387] Cellebrite. (2021). *Cellebrite, the Leading Digital Intelligence Solutions Provider, to List on Nasdaq through Merger with TWC Tech Holdings II Corp.* [online] Available at: https://web.archive.org/web/20210429051805/https://www.cellebrite.com/en/cellebrite-to-list-on-nasdaq-through-merger-with-twc-tech-holdings-ii-corp/ [Accessed 29 Aug. 2025].

response service firm Cyber Technology Services Inc. for $3.8 million.[388] Most recently, in June 2025, Cellebrite reportedly purchased hardware virtualization start-up Corellium for $200 million to expand its ability to break into encrypted mobile devices.[389] [390] [391]

As of 2025, Cellebrite maintains a global network of twelve subsidiaries, based in Australia, Brazil, Canada, India, France, Germany, Japan, Singapore, the United Kingdom, and the United States (in addition to its headquarters in Petah Tikvah, Israel).[392] Cellebrite operates fourteen offices across the world.[393]

According to its 2024 financial filings released this year, 44.3% of Cellebrite's shares are owned by Sun Corporation, and 5.8% are owned by True Wind Capital Management, the latter a result of the merger with TWC Tech Holdings II Corporation. Together, they own a majority of ordinary shares.[394]

Although Cellebrite does not sell spyware per se, its premier products are used to break into personal mobile devices and computers and make copies of victims' entire digital identities. Cellebrite claims its products are only used legally and cannot definitionally be spyware, because they are used after crimes have occurred.[395] This has been proven patently false. For example, reports emerged in late 2024 about how Serbian authorities abused Cellebrite technology to break into activists' phones without proving they had committed crimes.[396]

Cellebrite's UFED nearly meets this paper's definition of what qualifies as spyware, explicated in section 2. Although most of Cellebrite's products require physical access to phones, Cellebrite's Cloud UFED product allows remote data extraction from devices.[397] That, in conjunction with multiple reported instances of autocratic countries across the world

[388] S&P Capital IQ (2024). *Cellebrite DI Ltd. Acquired Cyber Technology Services, Inc. from $3.8 million.* [online] MarketScreener. Available at: https://www.marketscreener.com/quote/stock/CELLEBRITE-DI-LTD-126371088/news/Cellebrite-DI-Ltd-acquired-Cyber-Technology-Services-Inc-from-3-8-million-47401771/ [Accessed 29 Aug. 2025].
[389] Brewster, T. (2025). Cellebrite to Acquire Phone Forensics Startup Corellium for $200 Million. *Forbes*. [online] 5 Jun. Available at: https://www.forbes.com/sites/thomasbrewster/2025/06/05/trump-pardoned-corelliu m-founder-now-selling-cyber-business-to-cellebrite/.
[390] Thomson, I. (2025). *Cellebrite Buys Corellium to Help Cops Bust Phone Encryption*. [online] The Register. Available at: https://www.theregister.com/2025/06/05/cellebrite_corellium_merger/ [Accessed 29 Aug. 2025].
[391] Chris Wade, Corellium founder, was pardoned by US President Donald Trump in 2020 for cybercrimes in the mid-2000s. He is reportedly going to serve as Cellebrite's chief technology officer starting in Q3 2025, once the deal finalizes.
[392] Cellebrite DI Ltd. (2025). *Form 20-F*. p.76.
[393] Cellebrite. (2025a). *About - Cellebrite*. [online] Available at: https://cellebrite.com/en/about/ [Accessed 29 Aug. 2025].
[394] Cellebrite DI Ltd. (2025). *Form 20-F*. p.139.
[395] Cellebrite. (2025). *Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*. [online] Available at: https://cellebrite.com/en/cellebrite-facts/ [Accessed 29 Aug. 2025].
[396] Amnesty International. (2024). *Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*
[397] Amnesty International. (2024). *Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists. p.41.*

abusing its products, leads this paper to conclude Cellebrite is a CSV of concern to the WANA region.[398] [399]

Today, Cellebrite cofounder Yaron Baratz is the president and CEO of Septier, a signals intelligence company he founded in 2000 that sells "communications interception and analysis systems" to governments and law enforcement agencies. His LinkedIn appears to be private, though it does list him as CEO of Septier.[400] Septier was reported in August 2023 to have sold "lawful interception technology" to an Indian telecom company,[401] and India is known to use such surveillance tech to surveil protesters and the political opposition.[402] [403] Avi Yablonka is currently the CEO of Hypermedia Systems Ltd., a telecom company that aims to help companies upgrade their telecom infrastructure.[404] Yuval Aflalo cofounded Hypermedia Systems in 2003 and worked as CEO until 2016, after which he cofounded Naturongo,[405] a software company focusing on alternative medicine.[406]

Cellebrite's WANA presence is primarily seen through its office in Israel. This report's dataset, based on public reporting, suggests that at least five WANA countries have used Cellebrite's forensics tools.

[398] Biddle, S. and Desmukh, F. (2016). *Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident*. [online] The Intercept. Available at: https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/ [Accessed 29 Jul. 2025].
[399] Gur Megiddo (2020). *Revealed: Israeli Firm Provided phone-hacking Services to Saudi Arabia - Tech News*. [online] Haaretz. Available at: https://www.haaretz.com/israel-news/tech-news/.premium-revealed-israeli-firm-provided-phone-hacking-services-to-saudi-arabia-1.9161374 [Accessed 29 Aug. 2025].
[400] Baratz, Y. (2025). *Yaron Baratz's profile page*. [LinkedIn]. [Accessed 17 Aug. 2025]. Available from: https://www.linkedin.com/in/yaron-baratz-50371213/.
[401] Parkin, B., Srivastava, M., Gross, A., Cook, C. and Heal, A. (2023). *India's Communications 'Backdoor' Attracts Surveillance Companies*. [online] Financial Times. Available at: https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4 [Accessed 9 May 2025].
[402] Das, S. (2020). *Facial Recognition and 'Trade Secrets': What Exactly Are Police Forces Doing with Surveillance Tech?* [online] News18. Available at: https://www.news18.com/news/tech/facial-recognition-and-trade-secrets-what-exactly-are-police-forces-doing-with-surveillance-tech-3145223.html [Accessed 29 Aug. 2025].
[403] Roy, S. (2021). *I'm under 'Surveillance', Claims Trinamool MP Mahua Moitra, Writes to Delhi Police Chief*. [online] India Today. Available at: https://www.indiatoday.in/india/story/i-m-under-surveillance-claims-trinamool-mp-mahua-moitra-writes-to-delhi-police-chief-1768959-2021-02-13 [Accessed 29 Aug. 2025].
[404] Yablonka, A. (2025). *Avi Yablonka's profile page*. [LinkedIn]. [Accessed 17 Aug. 2025]. Available from: https://www.linkedin.com/in/avi-yablonka-831b18/.
[405] Naturongo. (2017). *Company - Naturongo*. [online] Available at: https://www.naturongo.com/company/ [Accessed 17 Aug. 2025].
[406] Aflalo, Y. (2025). *Yuval Aflalo's profile page*. [LinkedIn]. [Accessed 17 Aug. 2025]. Available from: https://www.linkedin.com/in/yuval-aflalo-53aa9a/.

The Cellebrite Corporate Structure

This information is available from 2024 financial filings filed with the SEC and via public reporting.

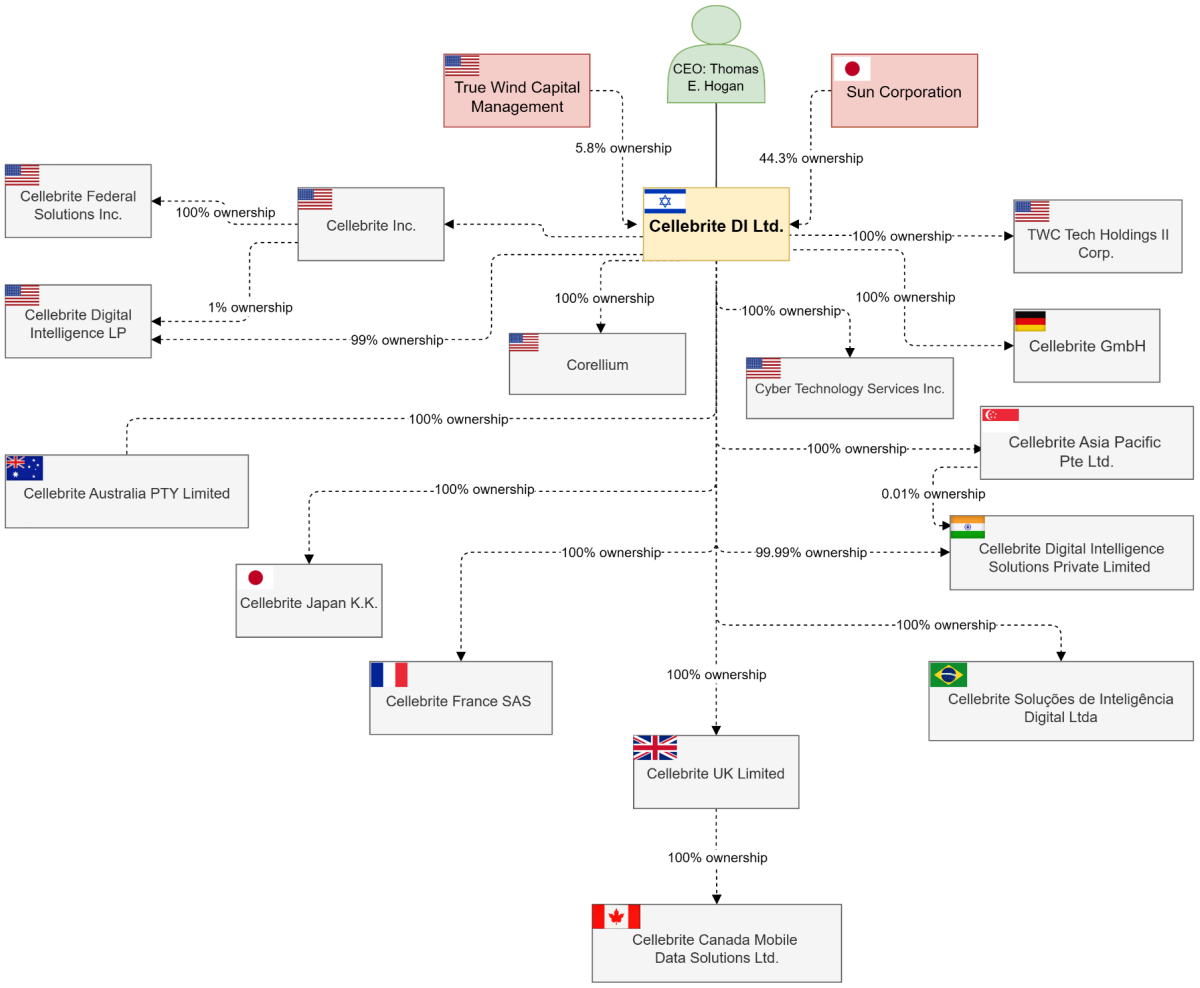


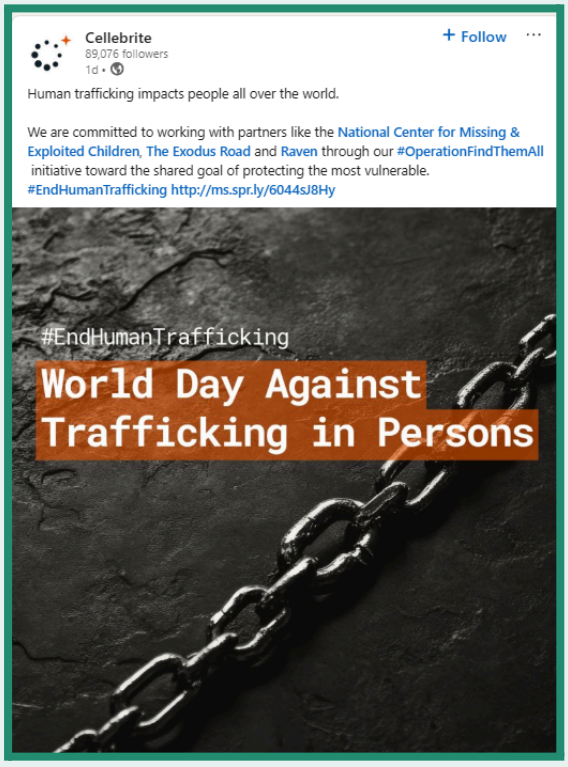
Image 19: Cellebrite's corporate structure.

Marketing: "The Boring Guys"

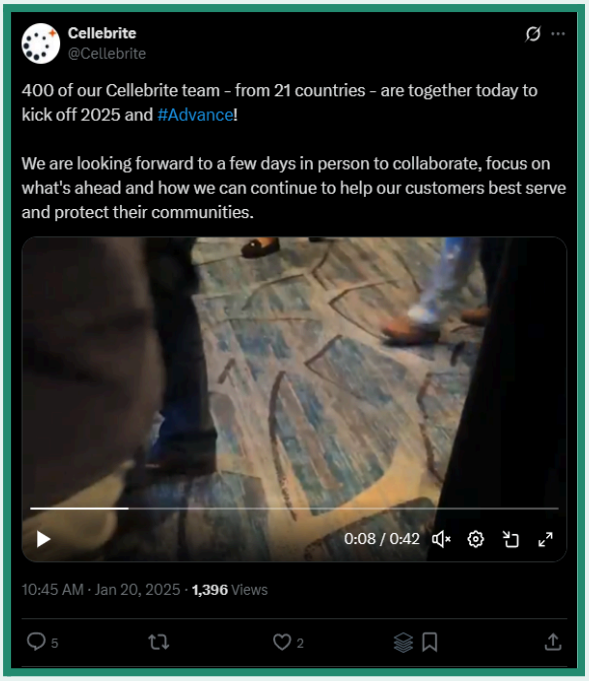
Cellebrite brands itself as a company serving a clear and legal purpose within the criminal justice system. In a 2021 investor presentation, Cellebrite presented its mission as to "protect and save lives, accelerate justice and preserve privacy in global communities."[407] It conceptualizes its digital forensics products as offering four key capabilities: collecting data, reviewing data, analyzing data, and managing data.[408]

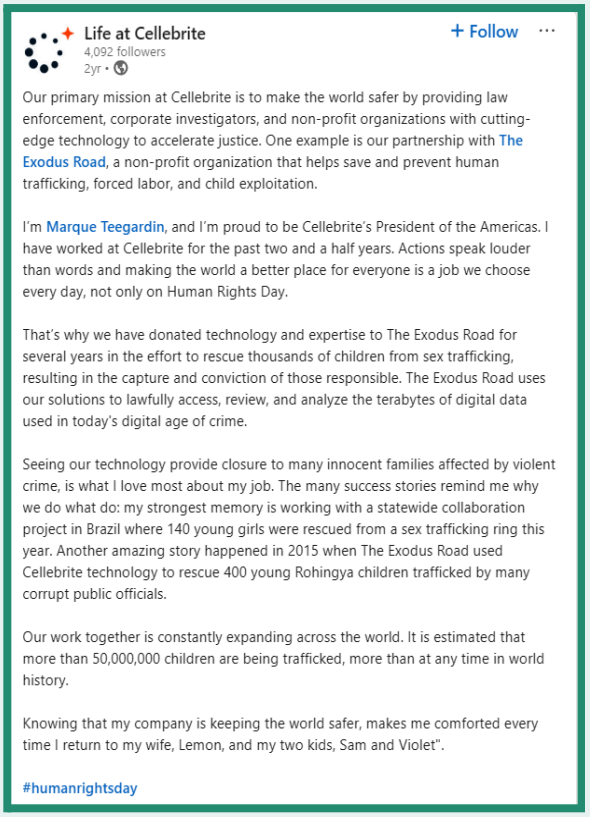
Cellebrite argues it fills a major gap in the public safety space. According to Cellebrite, too many law enforcement agencies face issues with data volume and complexity, "inefficient processes," and "ethics and accountability."[409] Remarkably, it claims it is uniquely able to tackle this ethics and accountability problem.

Cellebrite actively maintains social media pages on Facebook, LinkedIn, X (formerly Twitter), and YouTube. Cellebrite behaves similarly to NSO Group on social media, in that many of its posts recognize human rights-themed holidays, patriotic holidays, and the day-to-day activities of its employees. Like NSO Group, Cellebrite appears to engage in branding to try to distract users from its many controversies.



[407] Cellebrite. (2021) Investor Presentation April 2021 Exhibit 99.2 [Presentaiton]. Securities and Exchange Commission. April. [Accessed 19 Aug. 2025]. Available from: https://web.archive.org/web/20211206044245/https://sec.report/Document/0001213900-21-020888/.
[408] Cellebrite. (2021) Investor Presentation April 2021 Exhibit 99.2.
[409] Cellebrite DI Ltd. (2025). *Form 20-F*. p.61 .





Images 20-23: On X and LinkedIn, Cellebrite celebrates patriotic holidays, shares posts about human rights-themed days of awareness, and shares day-in-the-life employee updates, apparently in an attempt to humanize the brand and associate itself with human rights awareness.

Cellebrite frequently aims to ground its identity as one that deeply cares about human rights and strict ethics compliance. In an attempt to address potential ethics concerns with its products, Cellebrite announced the creation of an Ethics and Integrity Committee and an Ethics Advisory Panel on September 13, 2021.[410] Of Cellebrite's seven current Ethics and Integrity Board members, six have direct connections to US or Israeli law enforcement, the Israel Defense Forces, or the US Customs and Border Protection.[411] Gabriella Blum, a professor at Harvard and member of the board, formerly operated as a senior legal advisor to the Israel Defense Forces during the Second Intifada and helped develop legal standards for what kinds of extrajudicial killings were acceptable.[412] Moshe Halbertal, another board member, was an author of the Israel Defense Forces' Code of Ethics. Board member Doron Herman, an alleged "expert in the field of Online Child Protection," frequently posts on social media in support of Israel's actions in Gaza, which have been recognized as genocidal by

[410] Cellebrite (2021a). *Cellebrite Announces Formation of Ethics & Integrity Committee*. [online] Cellebrite. Available at: https://cellebrite.com/en/cellebrite-announces-formation-of-ethics-integrity-committee/ [Accessed 29 Aug. 2025].
[411] Cellebrite. (2024). *Ethics & Integrity*. [online] Available at: https://cellebrite.com/en/ethics-integrity/ [Accessed 11 Aug. 2025].
[412] Barshad, A. (2018). *Israel's Gabriella Blum Helped Write the Laws of Drone Warfare. Nearly Two Decades Later, She Has Regrets*. [online] The Intercept. Available at: https://theintercept.com/2018/10/07/israel-palestine-us-drone-strikes/ [Accessed 11 Aug. 2025].

multiple human rights organizations.[413] On October 20, 2023, Herman publicly stated "Greta Thunberg Supports ISIS" after she called for a ceasefire in Gaza and "justice and freedom for Palestinians" on X.[414]

On its webpage delving into its ethics and integrity, Cellebrite claims it employs "strict controls" to ensure its technology is only used in legal investigations.[415] It also restricts sales to countries not sanctioned by the European Union, Israel, the United Kingdom, or the United States, as well as the Financial Action Task Force (FATF) blacklist. Despite this, Cellebrite has reportedly sold to countries on the FATF blacklist (e.g., Myanmar) and graylist (e.g., Venezuela).[416]

Image 24: A word cloud of Cellebrite's Ethics and Integrity at Cellebrite webpage (with names and "Cellebrite" removed). Like other CSVs, Cellebrite identifies its work with "the good guys" by relying on marketing terms such as "solutions," "privacy," "law," "integrity," "safety," "security," and "human rights."[417]

Cellebrite notes in its 2024 Form 20-F SEC filing that some of its products "may be used by customers in a way that is, or that is perceived to be, incompatible with human rights."[418] Cellebrite warns its investors that this may harm its reputation. And while Cellebrite also claims that it strives to work with customers who use its products ethically and legally and

[413] B'Tselem: The Israeli Information Center for Human Rights in the Occupied Territories (2025). *Our Genocide*. [online] *B'tselem*. Available at: https://www.btselem.org/publications/202507_our_genocide [Accessed 11 Aug. 2025].
[414] Herman, D. (2023) [X (formerly Twitter)] 20 October, 2023. Available at: https://x.com/D0ronhe/status/1715409227332669789 (Accessed: 23 July 2025)
[415] Cellebrite. (2024). *Ethics & Integrity*.
[416] Krapiva, N. and Sugiyama, H. (2021). What Spy Firm Cellebrite Can't Hide from Investors. *Access Now News & Updates*. Available at: https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/ [Accessed 29 Aug. 2025].
[417] Cellebrite. (2024). *Ethics & Integrity*.
[418] Cellebrite DI Ltd. (2025). *Form 20-F*. p.20.

that it may not enter commercial relationships with customers whose activities are "inconsistent with our organizational mission or values," it admits two sentences later in the filing that it cannot "easily or quickly verify" whether clients use Cellebrite products "for lawful uses."[419] Cellebrite notes it requires customers to sign an end-user licensing agreement that explicitly "prohibit[s]" them from abusing Cellebrite products and breaking human rights laws.[420] If they do, Cellebrite retains the right to terminate their license and request that customers indemnify them for any losses.

To try to dispel claims of wrongdoing tied to human rights abuses, Cellebrite, similar to NSO Group, offers a "Myth vs. Fact" page on its website, claiming it is not a hacking company, does not operate spyware, and is not acting unethically.[421] Many of its "facts" rely on misleading definitions of terms to disprove claims of wrongdoing. For example, Cellebrite notes, "Hacking means unauthorized access to a system, which implies illegal activity. It is therefore inaccurate to refer to Cellebrite as a 'phone hacking company' … when these solutions are being used … legally."[422]

A January 2025 Calcalist interview with former Cellebrite CEO Yossi Carmil offers insight into how Cellebrite markets its identity, customers, intentions, and product offering. He denied allegations of wrongdoing and that "Cellebrite [is] operating in a gray area" of legality, claiming that Cellebrite "operate[s] in countries that follow the law and work exclusively with legitimate enforcement agencies. We are far more boring than people think." When summarizing the work over his two-decade tenure, he said: "If I had to describe Cellebrite with a word that starts with the letter 'S,' it wouldn't be 'sexy,' but 'safety.'"[423]

Yet Amnesty International,[424] Access Now,[425] and Privacy International[426] have all shown that Cellebrite has weak standards for human rights due diligence, which has led autocratic states to use its technology in ways that violate international law, including to help gather evidence toward the potential arrest and torture of dissidents. Moreover, Amnesty International highlights that even if Cellebrite's products do not meet Cellebrite's strict definition of spyware, they raise serious human rights concerns because they can totally compromise device privacy and functionally surveil private communications without user consent.[427]

---

[419] Cellebrite DI Ltd. (2025). *Form 20-F*. p.31.
[420] Cellebrite DI Ltd. (2025). *Form 20-F*. p.32.
[421] Cellebrite. (2025). *Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*.
[422] Cellebrite. (2025). *Cellebrite Provides Facts about Its Business and Solutions - Cellebrite*.
[423] Shulman, S. (2025). *From Bootstrapped Startup to a $5B powerhouse.*
[424] Amnesty International. (2024). *Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*
[425] Krapiva, N. and Sugiyama, H. (2021). What Spy Firm Cellebrite Can't Hide from Investors.
[426] Privacy International (2019). Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers. *Privacy International Long Reads*. Available at: https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers [Accessed 29 Aug. 2025].
[427] Amnesty International. (2024). *Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists*. p.63.

Premier Products and Capabilities

Cellebrite offers products across three broad categories: "Collect and Review," "Analyze and Investigate," and "Manage and Safeguard."[428] [429] It is best known for its Universal Forensics Extraction Device (UFED). The UFED, used along with Cellebrite's Physical Analyzer, gives customers the ability to unlock a variety of mobile devices and exfiltrate data for analysis. Cellebrite also now offers Mac and Windows computer forensic imaging products.

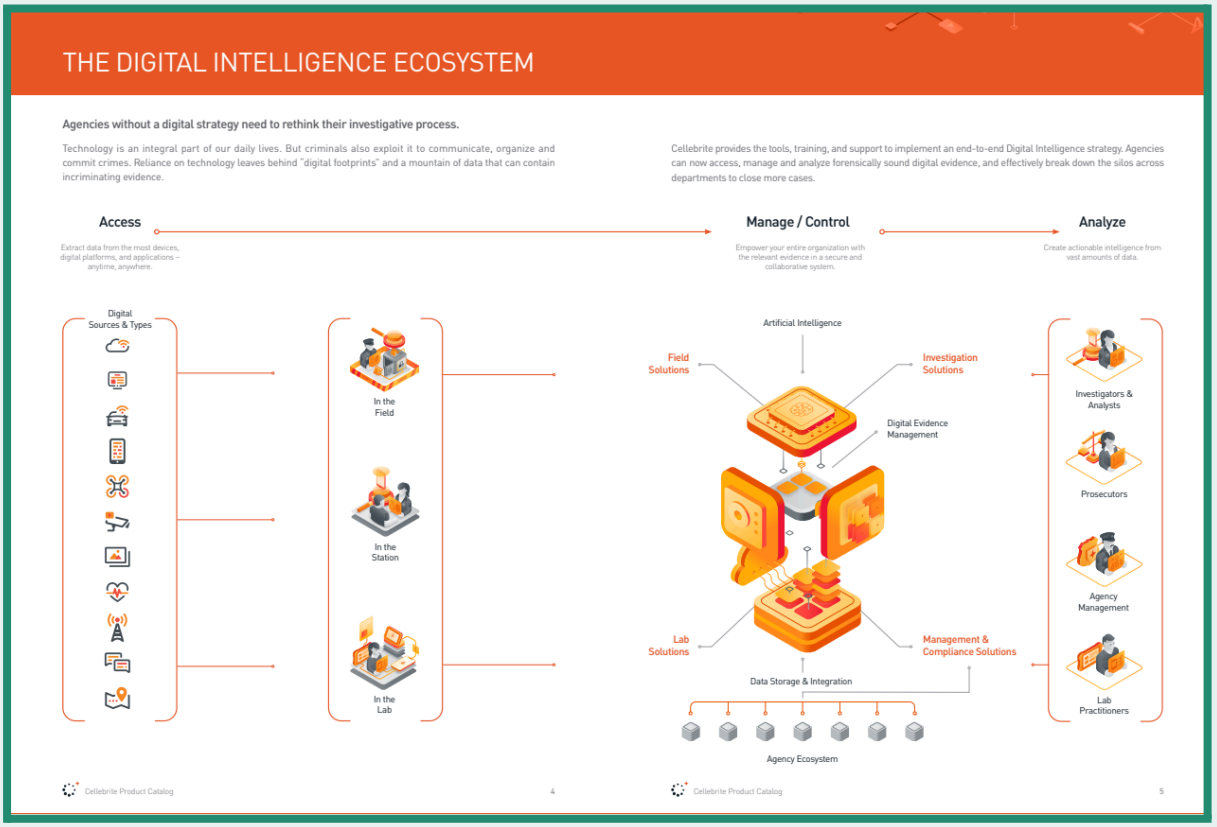


Image 25: Cellebrite discusses the "digital intelligence ecosystem" in its 2020 product catalogue, then describes which products fit into which ecosystem "silos." It offers a glimpse into the types of data Cellebrite targets.

The UFED suite of products also includes cloud capabilities that enable customers to probe cloud-based content associated with target devices, allowing them to access deleted data. Cellebrite's data management and analytics products, as Amnesty International highlights, can analyze multiple targets at once and help operators understand social and communicative networks, which can prove useful when looking to analyze dissident networks, journalists, and protest activity.[430]

[428] Cellebrite (2023). *Cellebrite Home Page*. [online] cellebrite.com. Available at: https://cellebrite.com/en/home/ [Accessed 15 Jun. 2025].
[429] Cellebrite has phrased these categories in different ways over time. In its 2020 product catalogue, for example, it classified its products as "access," "manage/control," and "analyze."
[430] Amnesty International (2024a). *Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*. [online] *Amnesty International*, London, UK: Amnesty International, p.9. Available at: https://www.amnesty.org/en/documents/eur70/8813/2024/en/ [Accessed 29 Aug. 2025].

The UFED product suite relies on highly sophisticated zero-day exploits to access and extract data from mobile devices.[431] Once customers gain device access, they use other Cellebrite products to analyze the data and gather digital evidence of alleged crimes.

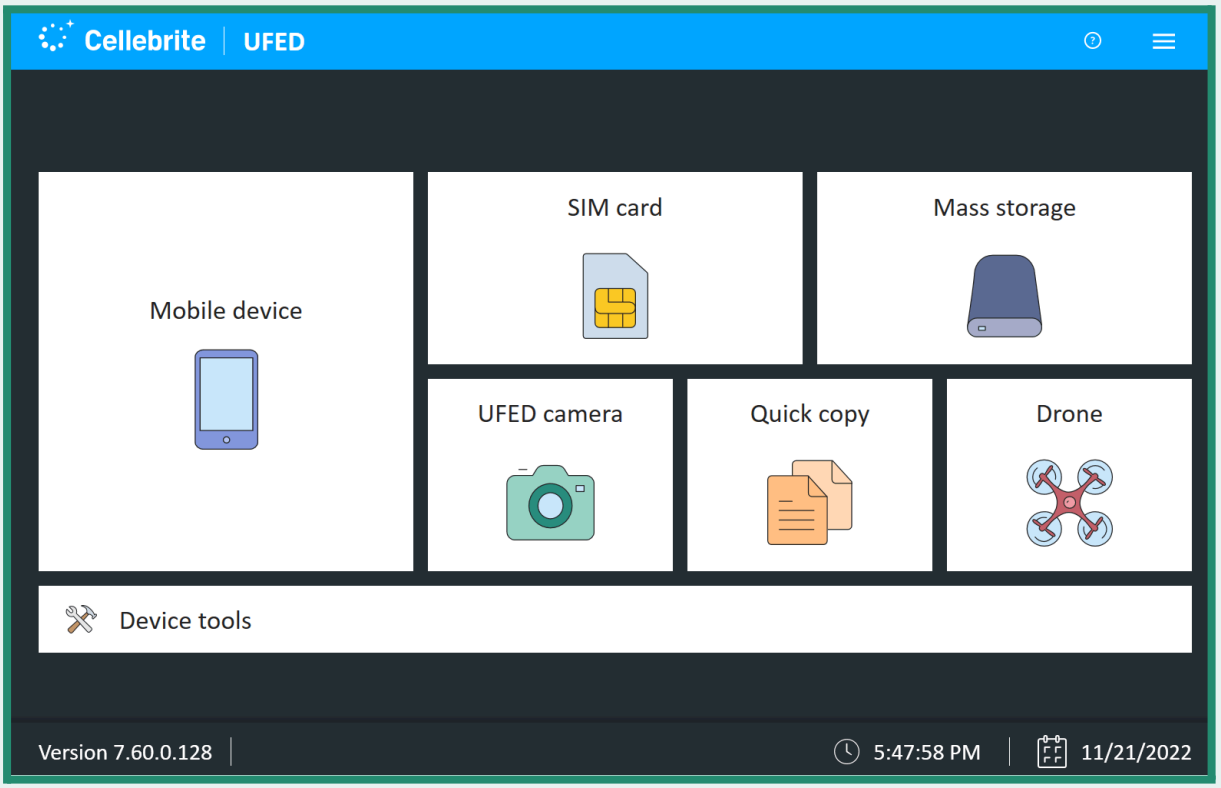
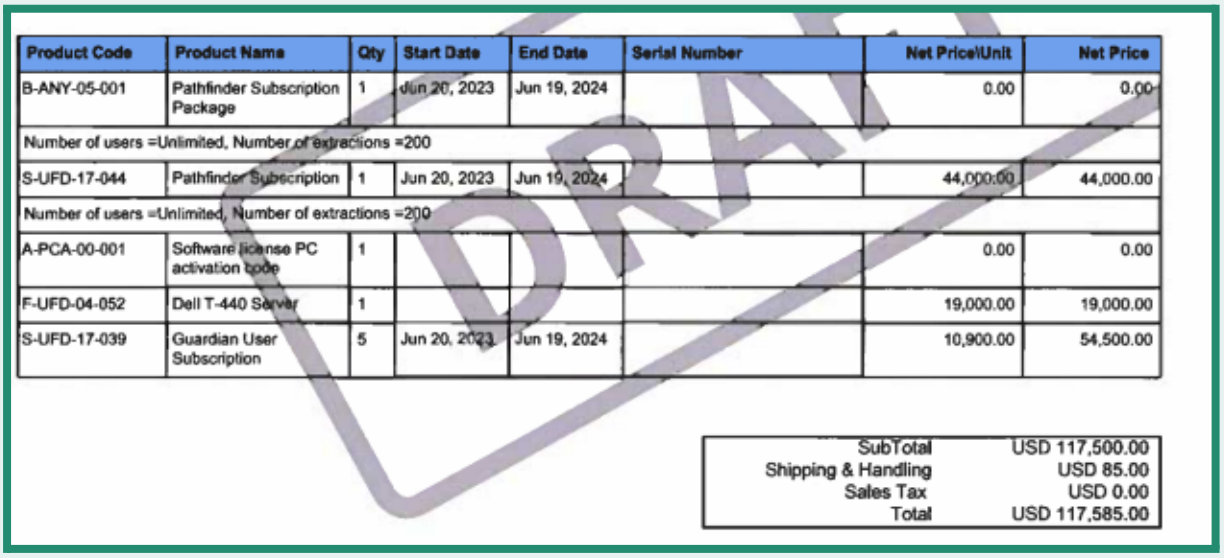


Image 26: Cellebrite's UFED home screen displayed on Cellebrite's product page for the UFED.[432]

Cellebrite offers different techniques to users based on whether the target device is locked with a known passcode or not.[433] Multiple leaks of Cellebrite manuals and software have led the company to change how it offers its most advanced unlocking services, lest the public gain access to zero-days it relies on to unlock devices.[434] It offers different types of access technology to private- and public-sector clients and offers the most sophisticated capabilities not supported by UFED to customers who mail their target devices to a Cellebrite lab.[435]

[431] Amnesty International (2024a). *Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*. p.41.
[432] Cellebrite (2024). *Cellebrite UFED | Access and Collect Mobile Device Data*.
[433] Amnesty International (2024a). *Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*. p.75.
[434] DDOSSecrets. (2024). *Search Results for 'Cellebrite' - Distributed Denial of Secrets*. [online] Available at: https://ddosecrets.com/search?query=cellebrite [Accessed 30 Aug. 2025].
[435] Amnesty International (2024a). *Serbia: 'A Digital Prison': Surveillance and the Suppression of Civil Society in Serbia*. p.75.

According to public reporting, new UFED units cost around $6,000 (though older models are apparently available for much cheaper on eBay).[436] [437] In 2022, a contract between a US police department and Cellebrite was leaked online.[438] The document suggests certain products are sold with a onetime cost and yearly subscription. The proposal suggests that Cellebrite Premium, which offers more extensive unlocking capabilities (but isn't currently on Cellebrite's website as an offered product), costs $14,000 per year for 35 unlocks per year. Pathfinder, an AI analytics program, costs $44,000 per year with a one-time cost of $19,000. Guardian costs $10,900 per year per agency for cloud storage for forensics findings.



Product Code	Product Name	Qty	Start Date	End Date	Serial Number	Net Price\Unit	Net Price
B-ANY-05-001	Pathfinder Subscription Package	1	Jun 20, 2023	Jun 19, 2024		0.00	0.00
Number of users =Unlimited, Number of extractions =200							
S-UFD-17-044	Pathfinder Subscription	1	Jun 20, 2023	Jun 19, 2024		44,000.00	44,000.00
Number of users =Unlimited, Number of extractions =200							
A-PCA-00-001	Software license PC activation code	1				0.00	0.00
F-UFD-04-052	Dell T-440 Server	1				19,000.00	19,000.00
S-UFD-17-039	Guardian User Subscription	5	Jun 20, 2023	Jun 19, 2024		10,900.00	54,500.00

SubTotal	USD 117,500.00
Shipping & Handling	USD 85.00
Sales Tax	USD 0.00
Total	USD 117,585.00

Image 27: A leaked Cellebrite quote suggests how much some Cellebrite services may cost.[439]

Major Attacks

On May 15, 2013, Bahraini authorities raided the home of Mohammed al-Singace, a political activist and the brother of the dissident Abduljalil al-Singace. Abduljalil had been arrested for his role in protests during the Arab Spring, and Mohammed worked as a longtime activist for Bahrain's working-class and poorest residents.[440]

[436] Swearingen, J. (2019). Cops' Favorite Phone Hacking Tool Is Being Sold on eBay. *NY Mag: Intelligencer*. [online] 28 Feb. Available at: https://nymag.com/intelligencer/2019/02/cellebrite-phone-hacking-tool-is-being-sold-on-ebay.html [Accessed 27 Feb. 2022].
[437] eBay. (2025). *Cellebrite UFED | eBay search*. [online] Available at: https://www.ebay.com/shop/cellebrite-ufed?_nkw=cellebrite+ufed [Accessed 30 Aug. 2025].
[438] Anon, (2022). *Leaked Cellebrite Quote Package*. [online] Available at: https://agenda.canyoncounty.id.gov/SupportDoc/GetSupportingDoc?supportDocID=1023 [Accessed 4 Aug. 2025].
[439] Anon, (2022). *Leaked Cellebrite Quote Package*.
[440] Biddle, S. and Desmukh, F. (2016). *Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident*.

Mohammed al-Singace reported he was immediately tortured and beaten, and transferred to Bahrain's Jau Prison's Building 10. He did not know why. Authorities shaved his beard against his will, and he suffered blunt-force trauma wounds to his neck and head.[441]

Bahraini police confiscated his phone upon his arrest and used Cellebrite's UFED to unlock the phone and extract his personal data. The Intercept reported that Bahrain's General Directorate of Anti-Corruption and Economic and Electronic Security generated a report on al-Singace's phone's contents using Cellebrite's technology, and presented it as evidence in a trial against him, alleging he was part of a criminal conspiracy.[442] Cellebrite's technology was used to document WhatsApp chats and photos as evidence against him. Al-Singace was sentenced to ten years in prison,[443] and was given a royal pardon in April 2024 after serving eleven years.[444]

According to Access Now, Cellebrite's UFED technology was allegedly also used to prosecute and imprison another human rights activist, who was tortured and is serving a 15-year sentence.[445]

3.4 Saito Tech (formerly Candiru)

"We are looking forward to meeting your cyber intelligence needs with the highest level of professional integrity."

—Candiru's unnamed vice president of sales ending the introduction to a leaked commercial proposal, shared in 2020.[446]

Company Background

Saito Tech Ltd. (סאייטו טק בע"מ, registration no: 515126605,[447] originally named Candiru) is an Israel-based CSV founded in 2014 by Ya'akov Weitzman and Eran Shorer. Shorer and Weitzman formerly worked at NSO Group, and before that were enlisted in the IDF's elite

[441] Biddle, S. and Desmukh, F. (2016). *Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident*.
[442] Biddle, S. and Desmukh, F. (2016). *Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident*.
[443] Bahraini Leaks (2021). يوما على إضراب السجين البحريني محمد السنكيس وسط تردي حالته الصحية 18 . [online] Bahraini Leaks. Available at: https://bahrainileaks.com/%d8%a7%d9%84%d8%b3%d9%86%d9%83%d9%8a%d8%b3/ [Accessed 22 Aug. 2025].
[444] Rickett, O. (2025). *Bahrain Detains Activist for Posts on Final Day of F1 pre-season Testing*. [online] Middle East Eye. Available at: https://www.middleeasteye.net/news/bahrain-detains-activist-social-media-posts-final-day-f1-pre-season-testing [Accessed 30 Aug. 2025].
[445] Krapiva, N. and Sugiyama, H. (2021). What Spy Firm Cellebrite Can't Hide from Investors.
[446] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*. [online] Haaretz. Available at: https://img.haarets.co.il/bs/0000017f-e0a2-d804-ad7f-f1fa63b90000/ba/ac/7c85b9d556b876b2e4a8b6fdafa8/20200902-161742.pdf.
[447] CheckID (2025d). *Saito Tech Ltd - 515126605*. [online] CheckID. Available at: https://en.checkid.co.il/company/SAITO+TECH++LTD-rMe81mK-515126605 [Accessed 28 Aug. 2025].

cyber Military Intelligence Unit 8200.[448] Saito Tech sells spyware that targets computers, servers, and mobile devices,[449] and claims to only work with government agencies across the world.[450] On November 3, 2021, the US Commerce Department sanctioned Saito Tech for selling its products to governments to "maliciously target" opponents and civil society and "conduct transnational repression."[451]

Saito Tech is shrouded in secrecy, so it is difficult to assess its revenue. However, documents from a lawsuit from a former senior employee in 2020 claim that Saito Tech made approximately $20 million in revenue in 2018 and had multiyear deals in the pipeline worth $367 million from more than 60 countries. The employee claimed that in 2020 Saito Tech had around 150 employees, up from 70 in 2018 and 12 in 2015.[452] On Pitchbook, Saito Tech is described as having 70 employees.[453]

Image 28: Haaretz shared what was allegedly Candiru's logo (credit: Ofer Vaknin).[454]

[448] Megiddo, G. (2021). 'We're on the U.S. Blacklist Because of You': the Dirty Clash between Israeli Cyberarms Makers. *Haaretz*. [online] 17 Dec. Available at: https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000 [Accessed 29 Aug. 2025].

[449] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*. [online] Haaretz.com. Available at: https://www.haaretz.com/israel-news/tech-news/2020-09-07/ty-article/.premium/mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve/0000017f-e1eb-d568-ad7f-f3eb36390000 [Accessed 10 Aug. 2025].

[450] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*. [online] *Citizen Lab*. University of Toronto. Available at: https://utoronto.scholaris.ca/server/api/core/bitstreams/3e255059-7679-48b7-b84a-f5de13929dfc/content [Accessed 2 Aug. 2025].

[451] U.S. Department of Commerce (2021). *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*.

[452] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.

[453] Pitchbook. (2025). *Saito Tech*. [online] Available at: https://pitchbook.com/profiles/company/437928-67#overview [Accessed 30 Aug. 2025].

[454] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.

According to Forbes, Saito Tech's main financial backer used to be Founders Group, which was cofounded by Omri Lavie.[455] Isaac Zack (זק יצחק),[456] a principal investor and partner at Founders Group, became Saito Tech's largest shareholder within sixty days of its founding.[457] Zack was an initial investor in NSO Group.[458] He then received a seat on Saito Tech's board of directors. According to Citizen Lab, in January 2019 Eitan Achlow was named as Saito Tech's CEO and Tomer Israeli as its finance director.[459]

Saito Tech has changed its name four times since its founding in 2014,[460] and changes office spaces regularly.[461] [462] It does not operate a public website, requires workers to sign strict NDAs, and does not permit employees to discuss their place of work on LinkedIn.[463] Even CEO Eitan Achlow does not disclose his place of work on LinkedIn.[464]

[455] Brewster, T. (2019). Meet Candiru — the Mysterious Mercenaries Hacking Apple and Microsoft PCs for Profit. *Forbes*. [online] 3 Oct. Available at: https://www.forbes.com/sites/thomasbrewster/2019/10/03/meet-candiru-the-super-stealth-cyber-mercenaries-hacking-apple-and-microsoft-pcs-for-profit/ [Accessed 29 Aug. 2025].

[456] In Citizen Lab's initial report on Candiru, the authors stated Isaac Zack's Hebrew name was יעקב, which appears to be the wrong translation of "Isaac." According to corporate documents SMEX obtained, Isaac Zack's Hebrew name is "Yitzkhak" (יצחק), the common Hebrew translation of Isaac.

[457] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

[458] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

[459] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

[460] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

[461] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.

[462] Candiru, founded in 2014, changed its name to DF Associates Ltd. (ד. אף אסוסיאייטס בעיימ) in 2017. DF Associates updated its name to Grindavik Solutions Ltd. (גרינדוויק פתרונות בעיימ) in 2018, which changed to Taveta Ltd. (טאבטה בעיימ) in 2019. Lastly, Taveta changed to Saito Tech Ltd. (סאייטו טק בעיימ) in 2020. According to the BIS Entity List, Saito Tech has also been associated with the names "Greenwick Solutions" and "Tabatha Ltd." Although the company never officially changed its English name to either of these, these appear to be alternative transliterations of the Hebrew names for "Grindavik Solutions" and "Taveta."

[463] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.

[464] Achlow, E. (2025). *Eitan Achlow's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/eitan-achlow-788949/?originalSubdomain=il.

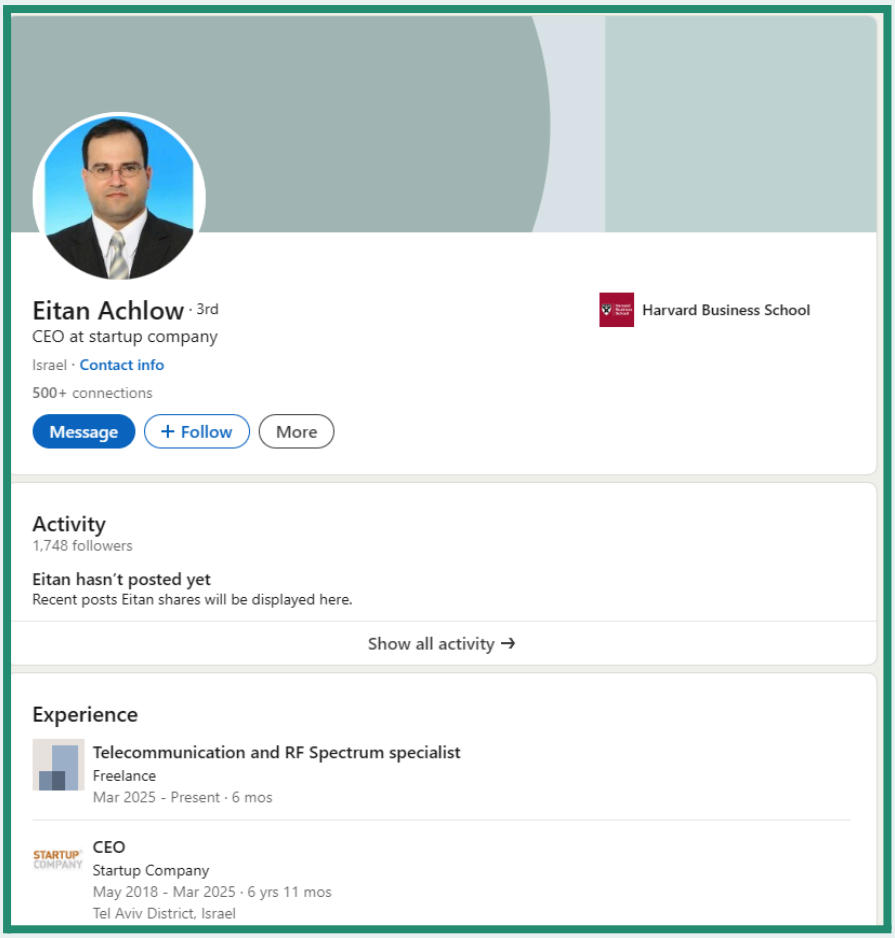


Image 29: Eitan Achlow's LinkedIn page, which shows he was the CEO of "Startup Company" from 2018 to 2025.

According to official corporate filings, Saito Tech's largest shareholders in descending order are Isaac Zack, Ya'akov Weitzman, Eran Shorer, Universal Motors Israel Ltd. (Company ID: 511809071[465]), I.B.I. Trust Management (Company ID: 515020428[466]), and Even Hemdat Trusts 1992 Ltd. (Company ID: 511678195[467]).[468] Zack is its largest shareholder, and Zack, Shorer, and Weitzman are listed as its three directors.

I.B.I. Trust Management is an investment house that offers trust portfolio management, and Even Hemdat Trusts 1992 also appears to handle trust investments. As Citizen Lab noted in its first review of Saito Tech in 2021, it is unclear whether trusts holding majority ownership of shares are doing so on behalf of other employees.[469] A Universal Motors Israel

[465] CheckID (2025). *Universal Motors Israel Ltd - 511809071*. [online] CheckID. Available at: https://en.checkid.co.il/company/UNIVERSAL+MOTORS+ISRAEL+LTD-DPvDQK6-511809071 [Accessed 28 Aug. 2025].
[466] CheckID (2025). *I.B.I. Trust Management - 515020428*. [online] CheckID. Available at: https://en.checkid.co.il/company/I.B.I.+TRUST+MANAGEMENT-BmQv59r-515020428 [Accessed 28 Aug. 2025].
[467] CheckID (2025). *Even Hemdat Trusts 1992 Ltd - 511678195*. [online] CheckID. Available at: https://en.checkid.co.il/company/EVEN+HEMDAT+TRUSTS+1992+LTD-0O0PLGj-511678195 [Accessed 28 Aug. 2025].
[468] Israeli Corporations Authority (2025). *Company Details Information: Entry for Saito Tech Ltd.*
[469] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

representative used to sit on Saito Tech's board, and it is not immediately clear why it would invest in a CSV. In July 2024, Universal Motors Israel was reported to have sold its stake in Saito Tech, though it still appears as a shareholder in official corporate filings.[470] Hemdat Trusts' two listed directors are Giora Erdinast[471] and Gideon Donny Toledano,[472] who are both lawyers.[473] Erdinast and Toledano's law firm allegedly previously represented NSO Group in court.[474] Tal Dori, David Zvi Bernstein, and Iddo Kook are listed as directors of I.B.I. Trust Management,[475] and all appear to hold leadership[476] or partner positions at the firm.[477] One of Saito Tech's former largest shareholders, Optas Industry Ltd., is based in Malta,[478] and one of its directors previously served as the Gulf Investment Fund's investment lead.[479] Saito Tech owns one known subsidiary, Sokoto Ltd. (registration no: 515996981[480]).

Official corporate documents obtained by SMEX in August 2025 do not reflect emerging news reports that claim Saito Tech was acquired by technology investment firm Integrity Partners. On April 2, 2025, Calcalist reported that Integrity Partners purchased Saito Tech for $30 million and is moving all of its assets and employees to a new entity not impacted by U.S. sanctions.[481] Integrity Partners has four partners: Chris Gaertner,[482] Elad Yoran,[483] Pat Wilkison,[484] and Thomas Morgan Jr.[485] All four appear to have backgrounds in the US military, though Morgan Jr. and Yoran do not list Integrity Partners on their LinkedIn pages (despite appearing active on the platform). According to an August 2025 analysis by Insikt Group, WHOIS records linked to Saito Tech suggest that Saito Tech's assets are being transferred to

[470] Intelligence Online (2024). Small Cyber Offensive Firm Bindecy Resists Israeli Cyber Crisis. *Intelligence Online*. [online] 7 Dec. Available at: https://www.intelligenceonline.com/surveillance--interception/2024/07/12/small-cyber-offensive-firm-bindecy-resists-israeli-cyber-crisis,110266932-art [Accessed 2 Aug. 2025].
[471] Erdinast, G. (2025). *Giora Erdinast's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/giora-erdinast-099524167/.
[472] Toledano, G. (2025). *Gideon Donny Toledano's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/doni-toledano-04b68326/details/experience/.
[473] CheckID (2025). *Even Hemdat Trusts 1992 Ltd - 511678195*.
[474] Legal500 (n.d.). *Dispute Resolution: Local Litigation and Arbitration*. [online] Legal500. Available at: https://my.legal500.fr/c/israel/dispute-resolution-local-litigation-and-arbitration/#ranking-position-1.
[475] CheckID (2025). *I.B.I. Trust Management - 515020428*.
[476] I.B.I. Trust Management. (2023). *Our Team - IBI*. [online] Available at: https://www.ibi.co.il/en/about/management/ [Accessed 30 Aug. 2025].
[477] Bernstein, T. (2025). *Tzvika Bernstein's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/tzvika-bernstein-29abba48/
[478] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[479] Intelligence Online (2020). Candiru Receives Boost from Investors Linked to Qatar. *Intelligence Online*. [online] 26 Aug. Available at: https://www.intelligenceonline.com/corporate-intelligence/2020/08/26/candiru-receives-boost-from-investors-linked-to-qatar,109602043-art [Accessed 29 Aug. 2025].
[480] CheckID (2025). *Sokoto Ltd - 515996981*. [online] CheckID. Available at: https://en.checkid.co.il/company/SOKOTO++LTD-W9bZ3yb-515996981 [Accessed 28 Aug. 2025].
[481] Kabir, O. (2025). *Blacklisted Spyware Firm Candiru Acquired by Integrity Partners in $30 Million Deal*. [online] CTech. Available at: https://www.calcalistech.com/ctechnews/article/r1er11mi61e [Accessed 30 Aug. 2025].
[482] Gaertner, C. (2025). *Chris Gaertner's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/chrisgaertner/details/experience/.
[483] Yorad, E. (2025). *Elad Yoran's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/eladyoran/.
[484] Wilkison, P. (2025). *Pat Wilkison's profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/wilkison/.
[485] Morgan Jr., T. (2025). *Thomas Morgan Jr.'s profile page*. [LinkedIn]. [Accessed 14 Aug. 2025]. Available from: https://www.linkedin.com/in/thomas-morgan-jr-b8674519/.

private Israeli company Integrity Labs Ltd. (registration no: 517081089[486], אינטגריטי לאבס בע~מ), based in Herzilya, Israel.[487] Insikt Group notes that Integrity Labs is run by an individual called Naftali Yoran, whose aliases include Elad Yoran.[488]

Based on its website (integrity[.]partners), Integrity Partners appears to be in partnership with or part of DHC Acquisitions, a special purpose acquisition company (SPAC) that merged with Brand Engagement Network Inc. in March 2024.[489] DHC Acquisitions reportedly raised $300 million in March 2021 for its activities.[490] DHC Acquisitions' website is no longer active, though an October 6, 2024, version of its website shows that Gaertner, Morgan Jr., and Wilkison operated as DHC's co-CEO, co-CEO/CFO, and COO, respectively.[491] Today, the merged entity is known as Brand Engagement Network Inc.[492] Integrity Partners previously entered talks to purchase NSO Group for $300 million, though the deal never closed.[493]

It is ultimately unclear how many companies Saito Tech works with to source, or ship, its products. However, in 2024 Amnesty International reported Saito Tech relied on Singaporean firm Heha PTE Ltd. to ship spyware products to the Indonesian National Police from May 2020 to January 2021.[494]

Saito Tech's WANA presence can be seen through its corporate headquarters in Israel, as well as its regional customers. This report's dataset, based on public reporting, suggest that at least six countries have used Saito Tech spyware in the region.

---

[486] CheckID (2025). *Integrity Labs Ltd - 517081089*. [online] CheckID. Available at: https://en.checkid.co.il/company/INTEGRITY+LABS++LTD-Q21OrBv-517081089 [Accessed 28 Aug. 2025].
[487] Insikt Group (2025). *Tracking Candiru's DevilsTongue Spyware in Multiple Countries*. [online] Recorded Future. Available at: https://assets.recordedfuture.com/content/dam/insikt-report-pdfs/2025/cta-2025-0805.pdf [Accessed 12 Aug. 2025].
[488] Insikt Group (2025). *Tracking Candiru's DevilsTongue Spyware in Multiple Countries*.
[489] Nasdaq. (2024). *DHC Acquisition Corp. Shareholders Approve Previously Announced Business Combination with BEN*. [online] Available at: https://www.nasdaq.com/press-release/dhc-acquisition-corp.-shareholders-approve-previously-announced-business-combination [Accessed 30 Aug. 2025].
[490] Srivastava, M. and Fontanella-Khan, J. (2022). *Israel's NSO Group in Sale Talks with Company Run by ex-US Soldiers*. [online] Financial Times. Available at: https://www.ft.com/content/b4ad167b-cb3a-4e0b-a6a0-bb2608679721 [Accessed 30 Aug. 2025].
[491] DHC Acquisition Corp. (2019). *DHC Acquisition Corp | Investing in Companies Solving the Challenges of the Last Mile through Technology.* [online] Available at: https://web.archive.org/web/20241006015701/https://www.dhcacquisition.partners/#team [Accessed 30 Aug. 2025].
[492] Nasdaq. (2024). *DHC Acquisition Corp. Shareholders Approve Previously Announced Business Combination with BEN*.
[493] Srivastava, M. and Fontanella-Khan, J. (2022). *Israel's NSO Group in Sale Talks with Company Run by ex-US Soldiers*.
[494] Amnesty International (2024). *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. [online] Amnesty International, p.18. Available at: https://www.amnesty.org/en/documents/asa21/7974/2024/en/ [Accessed 29 Aug. 2025].

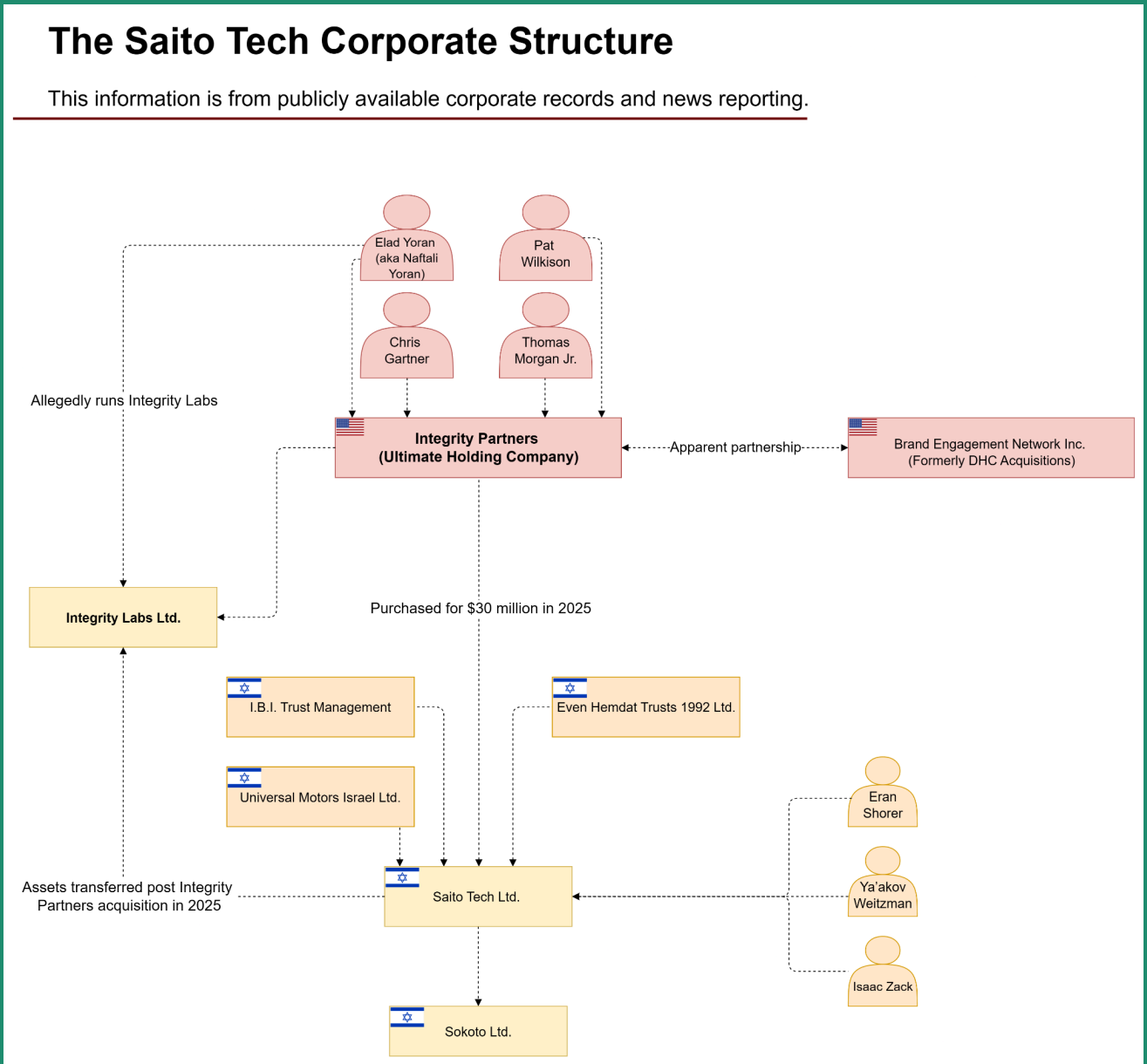


Image 30: Saito Tech's corporate structure in 2025.

Marketing: "The Techie"

Little is known about how Saito Tech markets its products, in part due to its stringent secrecy requirements and scant presence on social media and the internet. Leaked marketing materials, however, offer some insights into how it has marketed its products.

Haaretz posted a profile on Saito Tech (reported under its former name, Candiru) in 2020, featuring a commercial proposal originally leaked by The Marker.[495] In the leaked proposal, an unnamed sales vice president describes a product's capabilities as "untraceable": "Once deployed, the untraceable agents immediately identify and map networks the target is connected to," and the spyware "initiate[s] undetected data exfiltration tasks, throughout manipulation and control of device hardwar[e] and local programs."[496] The proposal notes that the spyware platform—which it brands as a "high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, [and] mobile handsets"—can target Windows devices, iPhones, and Android devices.[497] The proposal states customers can use its software anywhere across the world, except within China, Iran, Israel, Russia, and the United States.[498] [499] It appears to also boast about one-click capabilities, stating, "Proprietary [infiltration] agents are silently deployed into target[s] … with minimal requirements of target interaction." The vice president closes the introduction letter by noting the company aims to serve its customers with "the highest level of professional integrity."[500]

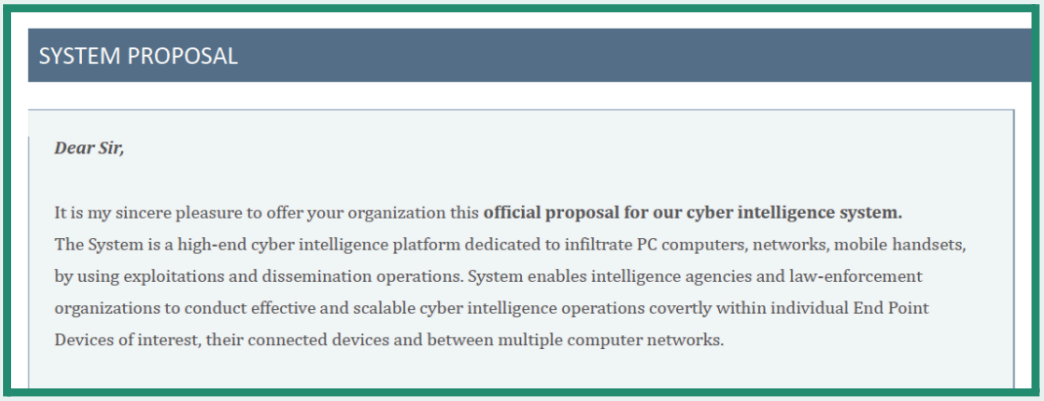
Saito Tech also appears to have occasionally participated in international surveillance trade fairs, despite its reclusive nature. Saito Tech presented a seminar at ISS World Europe in 2021, titled "Zero-Click Attacks: The Holy Grail," which suggests the company's interests.[501] [502]

While Saito Tech refers to its product as "the System" in the leaked proposal, Amnesty International notes that its "cyber infiltration system" is marketed as "Cyrus."[503] In the proposal, Saito Tech uses terms that identify its "System" as highly sophisticated and one-of-a-kind, such as "revolutionary," "unrivaled," "comprehensive," "proprietary," "advanced," and "robust."[504] Haaretz notes that a key part of Candiru's sales strategy lies in

---

[495] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.
[496] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[497] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[498] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[499] Microsoft reported it found Candiru victims in Iran in 2021, suggesting Saito Tech may not enforce these restrictions or that its technology was nevertheless somehow used in a blacklisted country.
[500] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[501] While SMEX found evidence of Candiru's presentation via the Internet Archive, public brochures for ISS Europe 2021 do not appear to list Candiru as a presenter.
[502] ISS World Training. (2021). *ISS WORLD Europe - Conference Agenda: 7-9 December 2021*. [online] Available at: https://web.archive.org/web/20211202132420/https://www.issworldtraining.com/ISS_EUROPE/ [Accessed 30 Aug. 2025].
[503] Amnesty International (2024). *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. p.17.
[504] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.

its reliance on "agents," or intermediaries, based in customer countries who assist in closing deals. They allegedly receive a 15% commission per transaction.[505]


SYSTEM PROPOSAL

Dear Sir,

It is my sincere pleasure to offer your organization this **official proposal for our cyber intelligence system.** The System is a high-end cyber intelligence platform dedicated to infiltrate PC computers, networks, mobile handsets, by using exploitations and dissemination operations. System enables intelligence agencies and law-enforcement organizations to conduct effective and scalable cyber intelligence operations covertly within individual End Point Devices of interest, their connected devices and between multiple computer networks.

Image 31: Leaked Candiru product proposal refers to its spyware as the "System."[506]

Unlike every other CSV mentioned in this report, Saito Tech does not appear to market itself as caring for human rights or only selling to countries that meet human rights standards. As mentioned earlier, it only declines to sell to China, Iran, Israel, Russia, and the United States. After Amnesty International reached out to Saito Tech in 2024 to check its human rights due diligence standards and to see if it conducted business with Heha PTE Ltd. to transfer spyware systems to Indonesia, Saito Tech responded that "the company operates under the regulation of Israeli Ministry of Defense Export Control Agency (DECA) – Export Control Law, 5766-2007." It is "legally prohibited," it argued, from divulging any information regarding its activities or licenses.[507] By maintaining a sense of legal plausible deniability, Saito Tech continues to operate in the shadows.

Premier Products and Capabilities

Saito Tech claims to offer an "untraceable," sophisticated spyware suite that targets iOS and Android mobile devices and Windows computers.[508] In its commercial proposal, Saito Tech referred to its spyware as the "System"; Amnesty International refers to it as "Cyrus"; and Microsoft tracks it as "DevilsTongue." According to Microsoft threat researchers, Saito Tech's spyware is a "complex modular multi-threaded piece of malware written in C and C++ with several novel capabilities."[509]

Saito Tech's proposal claims its spyware can successfully target the "latest versions" of Windows 10, 64-bit and Windows 7, 32- and 64-bit systems.[510] It also claims it can target the

[505] Ziv, A. (2020). *Cellphone Hacking and Millions in Gulf deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*.
[506] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[507] Amnesty International (2024). *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. p.22.
[508] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[509] Microsoft Threat Intelligence (2024). Private Sector Offensive Threat Actor Caramel Tsunami. *Security Insider*. Available at: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/caramel-tsunami#section-master-oc2985 [Accessed 29 Aug. 2025].
[510] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.

latest versions of three major browsers using remote code execution exploits; harvest data, including location, files, passwords, and browser history, from a variety of applications; and use a victim's webcam and microphone.[511] Saito Tech also boasts the ability to capture essentially all major types of data from Samsung Galaxy phones and the latest iOS versions on iPhones, including messaging apps and microphone/camera access.[512] The Windows spyware appears able to exfiltrate a variety of files, including messages from encrypted messaging apps like Signal.[513]

It offers a number of infection vectors to its customers, such as one-click malicious links and adversary-in-the-middle attacks.[514] Saito Tech is known to rely on sending malicious emails with links that download payloads.[515] It offers a 6 million euro add-on of the "Sherlock" infection vector, which Citizen Lab assesses may be a "browser-based zero-click vector."[516] A University of Strasbourg cybersecurity blog reported in 2024 that Sherlock is a separate spyware strain created by Israeli company Insanet (registration no: 516013364[517]). Sherlock can infect victims through Android, iOS, and Windows devices, relying on "programmatic advertising" to deliver infection payloads.[518] Insikt Group in 2025 reported Sherlock is used to help covertly install a spyware payload.[519]

Saito Tech appears to sell access to its suite of spyware tools based on the number of devices that can be targeted simultaneously. Unlike other CSV proposals discussed in this report, Saito Tech's suggests a customer can purchase an unlimited number of infection attempts for around 16 million euros, but with a limit of 10 devices targeted simultaneously. Saito Tech offers customers the ability to target an additional 15 devices for 1.5 million euros. An additional 5.5 million euros gets a customer the ability to target another 25 devices simultaneously and use devices within five additional countries. The ability to target specific apps such as Signal or Viber costs extra.

Citizen Lab highlights a particularly concerning element to its proposal: the option for a customer to purchase a remote shell capability add-on for 1.5 million euros, which allows customers to remotely execute code on a device.[520] This could enable them to download data onto a victim's device. For a total of 16.85 million euros, the company offered spyware

---

[511] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[512] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[513] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[514] Saito Tech (2020). *Leaked Saito Tech Spyware Proposal*.
[515] Scott-Railton, J., Campo, E., Marczak, B., Abdul Razzak, B., Anstis, S., Böcü, G., Solimano, S. and Deibert, R. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*. [online] *The Citizen Lab*. Available at: https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ [Accessed 12 Aug. 2025].
[516] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[517] CheckID (2025f). *Insanet Ltd - 516013364*. [online] CheckID. Available at: https://en.checkid.co.il/company/INSANET++LTD-w6e85Bd-516013364 [Accessed 28 Aug. 2025].
[518] Freiermuth, J. (2024). Sherlock, the Terrifying Israeli spyware, Surpassing Pegasus. *Blog Cyberjustice*. Available at: https://cyberjustice.blog/2024/01/22/sherlock-the-terrifying-israeli-spyware-surpassing-pegasus/ [Accessed 12 Aug. 2025].
[519] Insikt Group (2025). *Tracking Candiru's DevilsTongue Spyware in Multiple Countries*.
[520] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.

modules for Windows, iOS, and Android systems; data analysis capabilities; unlimited deployment attempts; up to 10 simultaneous infections; multiple infection vectors; the ability to target within one country; hardware; system delivery and relevant training; and a warranty. Saito Tech's spyware infrastructure is also known to use malicious links masquerading as being legitimately associated with advocacy groups, media companies, and civil society.[521]

Insikt Group released a report in August 2025 detailing new activity associated with Saito Tech and its Windows-based spyware.[522] Insikt Group tracked clusters of activity linked to Saito Tech in Saudi Arabia. The activity appears to have been active until as of June 26, 2025. Insikt Group found that Saito Tech uses highly varied infrastructural design across spyware operators, with some customers directly operating DevilsTongue victim infrastructure, others using "intermediary infrastructure layers," and some using Tor.

Major Attacks

On April 18, 2022, Citizen Lab released its second major report on Saito Tech, detailing an "extensive mercenary spyware operation" targeting Catalans with Pegasus and Candiru spyware.[523] After conducting its initial analysis of Candiru spyware, Citizen Lab's team identified an active victim in Catalonia, Joan Matamala. Matamala is a Girona-based political activist who runs a bookstore and foundation, both of which advance and teach the Catalan culture and language.[524] Matamala also founded the Nord Foundation, a nonprofit that encourages citizens to take part in open-source technologies in a social and ethical way. Citizen Lab researchers identified evidence of a live infection at a consortium of Catalan universities, and, with the help of local technicians, identified that Matamala owned the live infected device.

When Citizen Lab realized the infection was live, its researchers called Matamala's colleagues in an effort to move him away from his infected computer, in case it was actively surveilling him. He allowed researchers to access his computer, after which they identified that they had secured a live variant of Saito Tech's spyware. Citizen Lab worked with Microsoft to patch the vulnerabilities Saito Tech exploited, which led Microsoft to issue a patch to 1.4 billion devices across the globe.[525]

Matamala's story, it turns out, was a part of a much more extensive spyware operation, in which spyware operators targeted multiple Catalan politicians and civil society members, including Catalan members of the European Parliament and local politicians. At least three

[521] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[522] Insikt Group (2025). *Tracking Candiru's DevilsTongue Spyware in Multiple Countries*.
[523] Scott-Railton, J., Campo, E., Marczak, B., Abdul Razzak, B., Anstis, S., Böcü, G., Solimano, S. and Deibert, R. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*.
[524] Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B. and Deibert, R. (2021). *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*.
[525] The Citizen Lab (2017). *Would You click? — A a Story by the Citizen Lab*. [online] The Citizen Lab. Available at: https://catalonia.citizenlab.ca/ [Accessed 11 Aug. 2025].

other Catalonians were infected with Candiru's spyware via malicious emails. Upon further review, Matamala was also targeted with Pegasus at least 16 times from August 2019 to July 2020, and 65 individuals were targeted with spyware throughout this operation.[526]

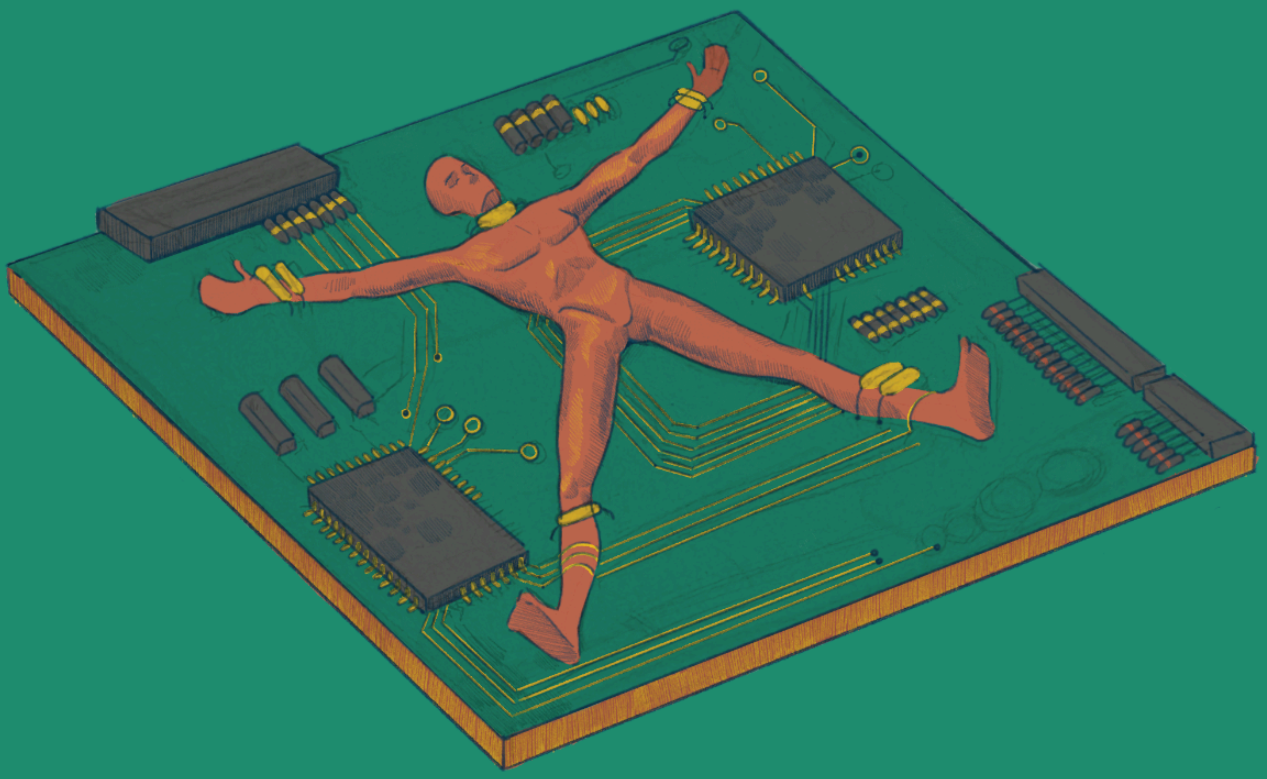
The variants of Saito Tech's spyware that targeted individuals in Catalonia were reportedly designed to gain "extensive access" to victim devices, including the ability to exfiltrate file and browser data as well as surveil and download encrypted messaging app messages.[527]

While it cannot be definitively proven, Citizen Lab suggests that the NSO Group and Saito Tech customer(s) could have been associated with the Spanish government, particularly given the political context between Spain and Catalonia.

[526] Scott-Railton, J., Campo, E., Marczak, B., Abdul Razzak, B., Anstis, S., Böcü, G., Solimano, S. and Deibert, R. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*.

[527] Scott-Railton, J., Campo, E., Marczak, B., Abdul Razzak, B., Anstis, S., Böcü, G., Solimano, S. and Deibert, R. (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru*.

Part 4: Zeroing In on Sypware's Impact on Human Rights: A SMEX CASE STUDY



interested in his activities is heavily rooted in the civil war that has gripped Yemen for over a decade.

Yemen's Civil War

Yemen's bloody civil war erupted in July 2014, in what the United Nations has termed "one of the world's worst humanitarian crises."[528] According to the United Nations, the war has led to over 377,000 Yemenis being killed, 10,000 of whom were children; over 4 million displaced; 54% of the population's livelihoods destroyed; and 15.6 million Yemenis forced into "extreme poverty."[529]

After former Yemeni President Abd Rabbuh Mansur Hadi reduced fuel subsidies in July 2014, major protests spread across Sanaa.[530] The Houthi movement, a militant Zaidi Shia group aligned with Iran, then took over several parts of the capital.[531] After failed negotiations, Houthi rebels stormed and took over the Presidential Palace in January 2015, and Hadi and his government resigned.[532] Soon thereafter, in March 2015, a Saudi Arabia-led coalition launched an air strike campaign against the Houthis, coupled with an economic isolation campaign.[533] Despite the campaigns, the Houthis took over Sanaa in December 2017. By the late 2010s, it became clear that Iran was militarily and strategically backing the Houthis, especially considering the Houthis' possession of advanced heavy weaponry likely made in Iran.[534] [535] The Houthis expanded their control, despite a major coalition offensive being launched in 2018 for Hodeidah. Fighting intensified in 2021 when the Houthis launched an offensive toward Marib, though a UN-led ceasefire was reached in 2022.

After Israel launched its genocidal campaign against Gaza, the Houthis began to launch attacks against Israel and Israel-affiliated trade shipments. This led the United States to initiate a bombing campaign against the Houthis, leading government and Saudi Arabia-aligned government forces reportedly to consider a new offensive against Houthi

[528] United Nations Yemen (2021). *UN Yemen Country Results Report: 2021*. [online] United Nations Yemen, p.6. Available at: https://yemen.un.org/sites/default/files/2022-04/Yemen_UNCT%20Annual%20Report%202021_.pdf [Accessed 27 Aug. 2025].
[529] United Nations Yemen (2021). *UN Yemen Country Results Report: 2021*.
[530] Zeidan, A. (2025). *Houthi Movement | Yemen, History, Leader, & Goals | Britannica*. [online] www.britannica.com. Available at: https://www.britannica.com/topic/Houthi-movement [Accessed 27 Jul. 2025].
[531] Zeidan, A. (2025). *Houthi Movement | Yemen, History, Leader, & Goals | Britannica*.
[532] Center for Preventive Action (2025). *Conflict in Yemen and the Red Sea*. [online] Global Conflict Tracker. Available at: https://www.cfr.org/global-conflict-tracker/conflict/war-yemen [Accessed 27 Aug. 2025].
[533] Zeidan, A. (2024). *Yemeni Civil War | [2015-present] | Britannica*. [online] www.britannica.com. Available at: https://www.britannica.com/event/Yemeni-Civil-War [Accessed 20 Aug. 2025].
[534] Zeidan, A. (2025). *Houthi Movement | Yemen, History, Leader, & Goals | Britannica*.
[535] Abo Alasrar, F. (2022). *The Houthis' War and Yemen's Future*. [online] Middle East Institute, p.5. Available at: https://www.mei.edu/sites/default/files/Alasrar%20-%20The%20Houthis'%20war%20and%20Yemen's%20future.pdf [Accessed 2 Aug. 2025].

strongholds.[536] [537] As of April 2025, the Houthis control a third of Yemen and where approximately 80% of its population lives.[538]

Since taking control of large swathes of Yemen, the Houthis have implemented a campaign of digital repression. In May 2025 France 24 reported this trend, noting the Houthis ban certain forms of online speech deemed to be a security threat and seek to control digital narratives.[539] The Houthis also appear capable of surveilling private communications across Yemen. The Counter Extremism Project reported in October 2023 that the Houthis are capable of monitoring communications based on SIM cards used to connect to local Yemeni cellular networks, as well as unique device identifiers, thanks to Houthi control of mobile network operators.[540] While not definitively using CSV products, reports suggest Houthis and Houthi-aligned groups have relied on intrusive malware to surveil political targets. Insikt Group in November 2018 found suspicious internet activity coming out of Yemen, suggesting potential adware and spyware use.[541] Insikt Group in May 2023 investigated a likely pro-Houthi cyber threat group, assessing it likely used remote access trojans—a form of surveillance malware that can secretly control devices remotely—against civil society and development sector targets.[542] The Houthis, as they have expanded their surveillance apparatus, have routinely arrested civil society members and journalists opposing official narratives.[543]

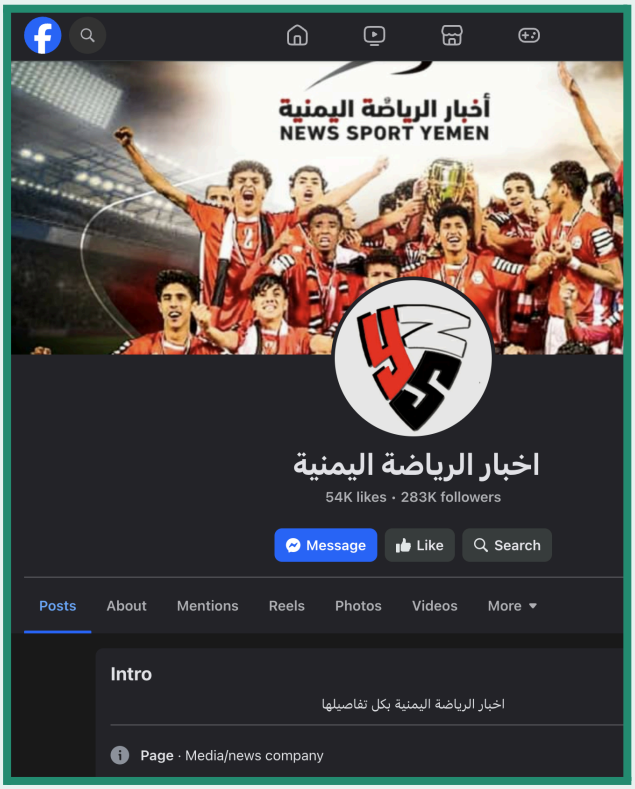
The Incident

On May 7, 2024, the journalist received a notification in his Gmail inbox that his phone number registered to his Yahoo account had been changed. He used Yahoo as a primary email address and Gmail as his backup account. His Yahoo phone number was subscribed to the Yemeni-Omani telecommunications company Yemeni Omani United (YOU), which is controlled by the Houthis. After taking control of his Yahoo email account, they immediately

[536] O'Connor, T. and Feng, J. (2025). *Houthis Warn Saudi Arabia and UAE Will Pay Price if They Back New Offensive*. [online] Newsweek. Available at: https://www.newsweek.com/houthis-warn-saudi-arabia-uae-will-pay-price-if-they-back-new-offensive-2060728 [Accessed 27 Aug. 2025].
[537] Iddon, P. (2025). Yemeni Militias May Be Planning a Ground Offensive against the Houthis. *Forbes*. [online] 3 May. Available at: https://www.forbes.com/sites/pauliddon/2025/05/03/yemeni-militias-may-be-planning-a-ground-offensive-against-the-houthis/ [Accessed 27 Aug. 2025].
[538] O'Connor, T. and Feng, J. (2025). *Houthis Warn Saudi Arabia and UAE Will Pay Price if They Back New Offensive*.
[539] Djamel Belayachi (2025). *How Yemen's Houthis Are Carrying out a Campaign of Digital Repression*. [online]
The Observers - France 24. Available at: https://observers.france24.com/en/middle-east/20250605-yemen-houthis-campaign-digital-repression-midri [Accessed 22 Aug. 2025].
[540] Counter Extremism Project (2023). *The Houthis' Use of Technology for Repression*. [online] pp.7–8. Available at:
https://www.counterextremism.com/sites/default/files/2023-09/The%20Houthis%20Use%20of%20Technology%20for%20Repression_Oct%202023.pdf [Accessed 25 Aug. 2025].
[541] Insikt Group (2018). *Underlying Dimensions of Yemen's Civil War: Control of the Internet*. [online] *Recordedfuture.com*. Available at: https://www.recordedfuture.com/research/yemen-internet-activity [Accessed 25 Aug. 2025].
[542] Insikt Group (2023). *OilAlpha: a Likely Pro-Houthi Group Targeting Entities across the Arabian Peninsula*. [online] p.2. Available at: https://assets.recordedfuture.com/insikt-report-pdfs/2023/cta-2023-0516.pdf [Accessed 25 Aug. 2025].
[543] Djamel Belayachi (2025). *How Yemen's Houthis Are Carrying out a Campaign of Digital Repression*.

reset the password, linked the account to another account, changed the backup email and added new emails, and changed the name and date of birth attached to his account.

First, they changed the journalist's account name to "Mohammed Abdulkarim" and then another name SMEX does not have access to. They then removed his Gmail backup account and added it to a separate Facebook account impersonating him. The imposter account was linked to a Yemeni sports news page with over 283,000 followers.



Images 32: The Facebook Yemeni Sports page linked to the imposter account.

At this point, he discovered he no longer had access to his phone number. His family members claimed they were not receiving his calls, and he noticed his SIM card was in "X" mode, suggesting some sort of error with connecting to YOU. In addition to gaining apparent access and control over his usernames and passwords, the threat actor(s) intercepted multifactor authentication codes, gained access to all of his social media accounts, and tried to delete them and all of their content.

The journalist reached out to YOU to get access back to his Yemeni number to stop this process to no avail. Over the next four months, YOU evaded the journalist and provided no substantive updates. He then reached out to another digital forensics lab, which contacted Facebook on his behalf and restored his account. Upon learning he regained access, the hackers tried to restore their access to the account by logging in from other devices he was logged in on, adding a spoofed email address similar to his to recover their password, and reaching out to Facebook claiming he was a fake person trying to steal their account. They sent his national ID card to Facebook, leading Facebook to require him to prove his identity. Even though he complied, Facebook continues to restrict his account today. Because of this,

he created a second Facebook account. With the help of the other digital forensics lab, his other accounts were later restored.

Based upon a forensic analysis of what SMEX could obtain after his phone was reset, DFL assesses with low confidence that he was likely targeted with an unidentified spyware strain to obtain his social media account credentials. SMEX cannot confirm this, but the journalist noted he did not click any malicious links, receive suspicious messages, or give his credentials to any untrusted individuals. SMEX assesses with low confidence that the threat actors obtained his credentials and multifactor authentication codes through the use of malware—such as keyloggers—and/or compromise tactics—such as adversary-in-the-middle attacks.[544]

The attack threatened to decimate years of work he had done building his profile on social media networks. When discussing how the attack impacted him and his work, he told SMEX:

"I felt as if I had lost everything I had built over many years of hard work and effort. Since 2009, I had been working continuously in [media], and all that effort vanished in an instant … Unfortunately … with this hack, I lost control over everything."

To the journalist, his presence on social media was everything he had built over his career. He wanted to fight back. However, when the threat actors took over the journalist's social media accounts, they said that unless he stopped talking about the incident, they would publicly release his personal information. Through the compromise, they also appeared to have stolen information on his journalistic sources, and threatened to release those too. This led the journalist to develop an incredible sense of panic and fear at every corner. Referring to being kidnapped by the Houthis, he told SMEX:

"As a former detainee, I was … living in constant anxiety … in Yemen, having been arrested twice … because of my journalis[m]. The second time … I was forced to sign a pledge not to continue any future journalistic activity, under the threat of execution … Even after my release, I continued to live in fear until I eventually left Yemen."

Everything in his life changed after he was targeted and digitally surveilled. He immediately left Yemen, moving to Egypt, Lebanon, and then ultimately France, where he remains today. He suspects he was targeted again shortly after leaving Yemen, and also experienced another cyberattack in Egypt. He felt an urgent need to radically update his digital hygiene along the way: he changed his passwords, replaced all his digital devices, and started using new email addresses in every country he traveled to. Yet in other ways, his work style is almost unimaginably different from what it once was. While he used to publicly rely on his socials to communicate his work, he has "become more reserved in communication and less visible on public platforms" for his personal safety, saying, "The attack left a clear psychological and professional impact [on me]."

[544] Keyloggers are malware that track what users type on a computer or mobile device, and can screenshot activity. Adversary-in-the-middle attacks are a compromise technique in which threat actors try to force a victim's device to communicate with malicious systems so that they can obtain information on the targeted user.

While SMEX DFL analysts are not able to state what CSV operated this likely spyware strain at this time, analysts assess with low confidence based on preliminary analysis that he was targeted with surveillance software. DFL hopes to gain additional insight into this case and release details at a later date. This targeting ruined his career in the short term and forced him to flee his home in the long term, destroying any sense of financial security and psychological safety he once knew. Spyware appears to have played an instrumental role in attacking the freedoms of the press and expression in Yemen, silencing a journalist and ruining his career along the way.

The journalist feels his life was turned completely upside down. Since the initial attack, he has never known peace. Yet after he was earlier kidnapped twice and threatened with execution, the attack was only another attempt to silence those willing to challenge those in power.

Concluding Thoughts

Watchdog organizations, international governing bodies, and independent researchers have made major strides in identifying spyware in the wild and calling on CSVs to halt the sale of spyware. The EU's PEGA Commission investigating Pegasus and other strains of spyware brought much-needed attention to the inner workings of NSO Group.[545] Amnesty International, Access Now, Citizen Lab and Human Rights Watch, among other groups, have made countless investigative contributions. Some of these efforts bore considerable fruit in the fight against spyware: Some major CSVs like FinFisher and QuaDream have shut down. Several major cybersecurity investors have pledged (voluntary) commitments not to invest in spyware or divested from CSVs, and investments in companies like NSO Group are now sometimes viewed as reputational anathema, especially given the US government's sanctions.[546] In a recent example, Norway's sovereign wealth fund, worth over a trillion US dollars, dropped all of its investments in Israeli CSV Cognyte in 2022 after accusing it of "extremely serious human rights violations."[547] Reputation costs also seemed to be on the rise for spyware makers. As noted in Section 3.1, NSO Group suffered major losses after the revelations of investigations into its spyware, and some investors seemed to believe it was at one point functionally worthless. The US Treasury Department has also sanctioned multiple spyware makers, including most of this report's subjects.

Yet despite these promising changes, it does not appear that spyware use is slowing. Despite the increasing condemnation of their actions, CSVs have not stopped selling spyware. Instead, evidence suggests they are doing the opposite: they hide their actions, change their names, obfuscate activity through multiple layers of corporate governance, market themselves as abiding by human rights standards, and continue to sell to governments that abuse their products and catalyze repression. As Feldstein and Kot noted in 2023, while

[545] Veld, S. in 't (2023). *REPORT of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware*.
[546] Franceschi-Bicchierai, L. (2024). *Investors' Pledge to Fight Spyware Undercut by past Investments in US Malware Maker*. [online] TechCrunch. Available at: https://techcrunch.com/2024/03/22/us-cyber-investors-pledge-spyware-is-off-limits-with-a-catch/ [Accessed 22 Mar. 2024].
[547] Shulman, S. (2022). *Cognyte Reeling after Being Dropped by Norway Sovereign Wealth Fund*. [online] CTech. Available at: https://www.calcalistech.com/ctechnews/article/r1yexabyi [Accessed 27 Aug. 2025].

some CSVs have shut down due to controversies, countless smaller spyware vendors fill market gaps and sell similar products.[548]

Moreover, as the Carnegie Endowment for International Peace stresses, democracies have not fully committed to banning the sale and use of spyware. While the EU has strict regulations on dual-use products like spyware, different European nations have less stringent standards for implementation, allowing CSVs to circumvent regulations and operate across Europe (and, more broadly, the world).[549] Another example is the US. Although the US government has sanctioned several notable CSVs, it actively has contracts with spyware vendors. This suggests that sanctions, laws banning spyware, and reports investigating the use of the technology are not enough to curb CSV activity, in and out of the WANA region. It is also not clear that sanctions have lasting impacts on CSVs' abilities to continue operations. For instance, on August 5, 2025, Insikt Group researchers published new research tracing Saito Tech's spyware actively being used in Saudi Arabia, despite sanctions associated with the group.[550] SMEX calls on human rights defenders, governments across the world, and investors to challenge and fight the proliferation of spyware—a technology that at its core violates human rights.

However, CSVs are likely not simply going to stop selling lucrative malware products when human rights defense organizations demand it. Consequently, SMEX strongly recommends that at-risk groups (e.g. human rights defenders, civil society members, etc.) in the WANA region employ cybersecurity best practices to best defend against spyware. As Amnesty International and the Electronic Frontier Foundation recommend, SMEX urges:[551] [552]

- Creating an online security plan;
- Keeping all mobile operating system, computer, and web browser software updated;
- Enabling higher-security modes on devices, like Apple's "Lockdown Mode";
- Avoiding clicking links or opening documents from strangers;
- Monitoring changes in device functionality. If your device starts acting up, it may have been infected by malware;
- Always using a virtual private network (VPN) from a well-known company;
- Changing social media account privacy settings to a higher level of security, and always evaluating new follow or friend requests closely;
- Encrypting your devices when possible;
- Enabling two-factor authentication;
- Using end-to-end encrypted messaging services like Signal;
- Using strong and unique passwords;
- Managing passwords via a password manager.

[548] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive?*
[549] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive?*
[550] Insikt Group (2025). *Tracking Candiru's DevilsTongue Spyware in Multiple Countries*.
[551] Amnesty International (2023). *What is spyware and what can you do to stay protected? - Amnesty International Security Lab*. [online] Amnesty International Security Lab. Available at: https://securitylab.amnesty.org/latest/2023/12/what-is-spyware-and-what-can-you-do-to-stay-protected/.
[552] Electronic Frontier Foundation (n.d.). *Surveillance Self-Defense Basics*. [online] Surveillance Self-Defense. Available at: https://ssd.eff.org/module-categories/basics [Accessed 11 Aug. 2025].

SMEX recommends continued research into CSVs operating in the WANA region, with a particular focus on smaller, boutique firms. Not much is publicly reported on their activity, and much is to be gained from updated knowledge on who, and what, is operating in the wild in the region. The fight against spyware is long and still underway—that doesn't mean it will always be that way.

APPENDIX

Data and Visualization of Spyware Incidents Occurring Over the Past 14 Years

SMEX created a table of spyware incidents occurring over the past 14 years, building on Feldstein and Kot's latest 2023 dataset. To view the visualization, visit Datawrapper at this link.

A Note on Memento Labs

Memento Labs presents a complex story. As noted in Section 2.4, Memento Labs technically appears second-most (as a tie) in this dataset. However, its last publicly reported incident happened a decade ago. Following this paper's methodology, if this report just looked at the last five years, Memento Labs would not appear at all in the analysis.

After its predecessor Hacking Team was notoriously hacked and consequently embroiled in scandal in 2015, major news outlets reported that Memento Labs was struggling to remake itself years later.[553] Once a hacking giant with contracts across the world, Memento Labs seemed to no longer be the major player it once was. Memento Labs does appear to still be active, though it does not appear to have been involved in any major spyware incidents over the past decade. The following are some pieces of evidence pointing to Memento Labs' continued activity in the WANA region:

- Hacking Team was a frequently used vendor in the WANA region, with contracts with at least eight regional governments before it was hacked in 2015.[554]
- Saudi Arabia purchased a 20% stake in Hacking Team to help it avoid complete insolvency in 2016 despite being hacked in 2015, raising questions about its interests in continuing to work with the company.[555]
- Security researchers at the Slovakian cybersecurity company ESET in 2018 reported they found new traces of Hacking Team's flagship product, Remote Control System, operating in the wild one year before the Swiss investor InTheCyber purchased Hacking Team and rebranded it to Memento Labs in 2019.[556]
- In 2023, the Swiss newspaper NZZ reported that InTheCyber has actively pursued selling its spyware products in the United Arab Emirates directly and via distributors in Dubai, also appearing twice on the 2023 ISS World conference presentation lineup in Dubai. As NZZ reports, Memento Labs as of 2023 had an active contract with the Dubai-based distribution company S.A.T. Trading LLC, which offers the "Tactical EXecutor" made by Memento Labs, a product that boasts the ability to unlock encrypted Windows systems.[557]

[553] Cox, J. and Franceschi-Bicchierai, L. (2020). *Memento Labs, the Reborn Hacking Team, Is Struggling*. [online] VICE. Available at: https://www.vice.com/en/article/memento-labs-the-reborn-hacking-team-is-struggling/ [Accessed 19 Jul. 2025].
[554] Feldstein, S. and Kot, B. (2023). *Why Does the Global Spyware Industry Continue to Thrive?*
[555] Franceschi-Bicchierai, L. (2018). *Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia*. [online] VICE. Available at: https://www.vice.com/en/article/hacking-team-investor-saudi-arabia/ [Accessed 15 Jul. 2025].
[556] Kafka, F. (2018). *New traces of Hacking Team in the wild*. [online] ESET. Available at: https://www.welivesecurity.com/2018/03/09/new-traces-hacking-team-wild/.
[557] Lukas Mäder (2023). *Swiss company sells spy software to Arab intelligence services*. [online] Neue Zürcher Zeitung. Available at: https://www.nzz.ch/english/a-swiss-company-is-selling-spy-software-to-arab-intelligence-services-the-federal-government-supports-them-ld.1739341 [Accessed 15 Jul. 2025].

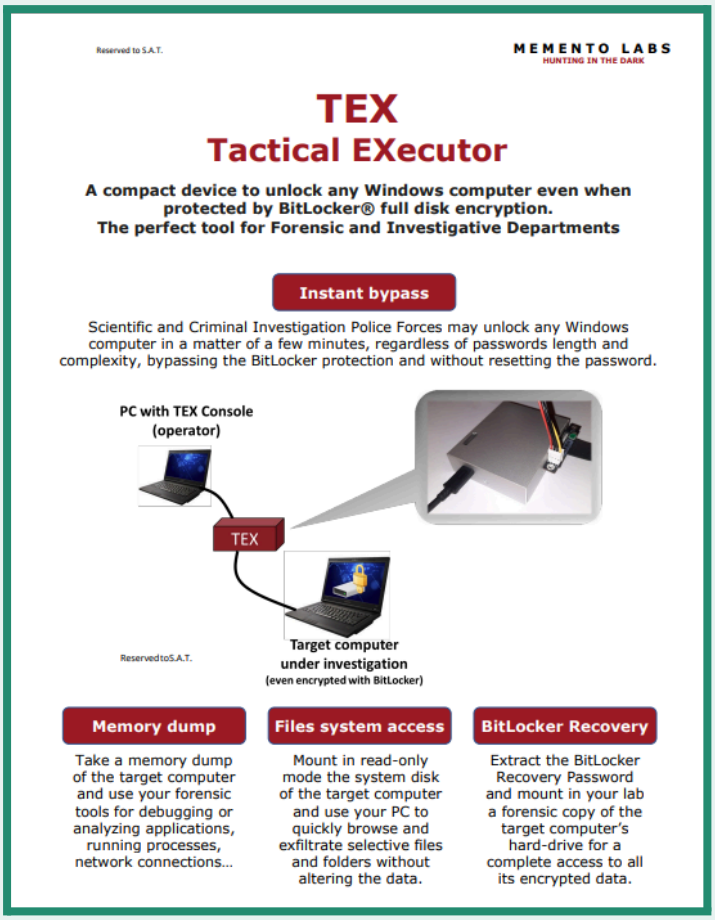


Image 33: A brochure from December 2022 offering insight into a new Memento Labs product, as reported by NZZ in 2023.

- Memento Labs actively participated in ISS World in 2025, marketing "Cutting Edge Offensive Cyber Capabilities for the Mobile World."[558] Together, these suggest that Memento Labs, though potentially not the success story its predecessor Hacking Team once was, nevertheless still has an active interest in procuring clients in the WANA region.

Image 34: Memento Labs' presentation at ISS World in 2025.

[558] ISS World (n.d.). *ISS World 2025 Middle East and Africa: Intelligence Support Systems for Electronic Surveillance, Social Media/DarkNet Monitoring, and Cyber Threat Detection* [brochure]. [online] Available at: https://www.issworldtraining.com/iss_mea/brochure01.pdf. n.p..

Interview Questions

SMEX interviewed several victims who believed they were attacked by sophisticated threat actors, including by potential spyware. The following are questions SMEX asked them after they reached out to SMEX's Digital Forensics Lab:

Basic background

1) Where are you from/where did you grow up?

The attack

2) What happened to you?
3) When did you first notice things were wrong? What did you notice? What did you do at that point?
4) Had you heard of computer hacking, spyware, or government surveillance before this attack?
5) Did you take any precautions online before this attack?

The impact

6) How did experiencing this cyberattack affect your life?
7) How did it impact your lifestyle?
8) Did you have to change how you lived in response to the attack?
9) How do you live now, having experienced the attack?