Continuity and Evolution: The Case of NSO Group (2010-2026) as a Gateway for Israeli Technology into Europe

Authors: Cèlia Carbonell Cassanyes (Irídia – Center for the Defense of Human Rights)

Coordination: Alys Samson (NOVACT) i Maite Ramos (SUDS)

Communication: Lucrecia Baquero (Observatory on Human Rights and Business in the Mediterranean)

Layout: Carmela Márquez B. @edicionescaseras

Observatori de Drets Humans i Empreses
NOVACT
suds Internacionalisme Solidaritat Feminismes
Irídia
Al-Himaya
Defensa de l'espai cívic a l'euromediterrània

Index

The history of NSO Group,
from 2010 to the present. 3

NSO Group and the Israeli government:
a lucrative partnership. 5

Spying, criminalising and silencing:
Pegasus in Palestine. 7

Pegasus in the shadow of genocide. 8

NSO Group in Europe, with its
headquarters in Luxembourg 10

WhatsApp vs. NSO Group and
corporate responsibility. 13

Strategic reorientation towards
the 'Americanisation' of NSO Group. 14

The history of NSO Group, from 2010 to the present.

Despite the exponential growth of numerous technology companies in the wake of the cybersecurity sector's rapid expansion, the role of certain Israeli companies, such as the NSO Group[1] in completely transforming this industry cannot be overlooked. In 2010, this industry was still in its infancy. The NSO Group was the first company to develop spyware with capabilities that were previously unheard of, including the ability to access and control the contents of a mobile device remotely and without the owner's permission or knowledge. This gives them access to all the content on the phone, both past and future, as well as control over the camera and microphone.

Pegasus cannot be considered obsolete technology. Indeed, companies such as the NSO Group are continuing to refine and modify the capabilities of their products in order to achieve the original objective that led to the company's creation: 'to develop a tool capable of remotely and undetectably infiltrating a mobile device'. From the outset, Niv Carmi, Shalev Hulio and Omri Lavie[2] emphasised the importance of the technology they had developed by pointing to the need for European security: 'Police forces and intelligence agencies across Europe told us that we could help solve their problem with the technology we had developed'. [3] According to the information published on its corporate website, the company "develops the best surveillance technology to help government agencies detect and prevent terrorism and delinquency".[4] This was the starting point that led them to establish NSO Group Technologies Ltd. The company was founded on 25 January 2010.

Although NSO develops a wide range of products, its best-known product is 'Pegasus', a surveillance technology which the company claims is sold exclusively to governments and intelligence agencies worldwide. [5] Pegasus has evolved considerably in recent years, progressing from requiring user interaction for activation to incorporating zero-click exploitation mechanisms and features such as the creation, modification and insertion of information on the device.[6] This increasing sophistication has serious consequences, as it grants the software total and disproportionate access to, and control over, the content on mobile devices.

1 NSO Group (2010), https://www.nsogroup.com/

2 Forbidden Stories (2021). *The rise and fall of NSO Group.*

3 The New York Times (2022). *The Battle for the World's Most Powerful Cyberweapon.*

4 More information on the NSO Group website, available at: https://www.nsogroup.com/about-us/

5 NSO Group (2025). *Transparency and Responsibility Report 2024*. 4, https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf

6 EDRI (2025). *Spyware and state abuse: The case for an EU-wide ban*. 7—8, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/

Since 2010 up to the present day, and particularly since 2015 –when first the Mexican government, and shortly after the Spanish government,[7] were first documented as using this technology– the company has operated under ambiguous regulations that have allowed the disproportionate and systematic surveillance of tens of thousands of people worldwide.[8] Thus, it has become a tool that was created, tested and developed in the context of occupation and colonialism in Palestine, that is now being offered, advertised and marketed as a means repression and persecution.

Since the start of the genocide in the Gaza Strip, the NSO Group has been in the media spotlight as it attempts to clean up its image after years of scandals and public allegations. Around ten legal complaints have been filed in Spain since April 2022 over illegal spying using Pegasus. This followed a report by Citizen Lab[9] which confirmed the threat posed by a WhatsApp notification sent to 1,400 users,[10] including the former president of the Catalan parliament, Roger Torrent, and the former ERC MP, Ernest Maragall. Maragall filed a complaint against the CNI (Spanish National Intelligence Centre) and the NSO Group in 2020 regarding the use of Pegasus.[11]

A report by The Citizen Lab, confirmed by Amnesty International's forensic laboratory, identified at least 65 individuals associated with the Catalan independence and self-determination movements as targets of espionage using Pegasus and Candiru. Those targeted included lawyers, journalists, human rights defenders and political representatives in the Catalan and European Parliaments*. This is the first case in which a victim of Pegasus has filed a complaint, resulting in the indictment of three senior NSO Group executives, including two of its founders, in Israel and Luxembourg.[12] Shalev Hulio and Omri Lavie are currently under investigation in a criminal case before a court in Barcelona.

Since its foundation, the NSO Group has emphasised that its technology is derived directly from Israeli military experience. As the report "The gateways for genocide technology into Europe" shows, it is common for founders of companies in this sector to have served

7 El Diario.es (2025). *Artur Mas fue el primer espiado con Pegasus en España cuando era presidente en 2015,* según Citizen Lab, https://www.eldiario.es/catalunya/artur-primer-espiado-pegasus-espana-president-citizen-lab_1_12270015.html

8 Forbidden Stories (2021). *About the Pegasus Project,* https://forbiddenstories.org/about-the-pegasus-project/

9 The Citizen Lab (2022). *CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru,* https://citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

10 Tech Crunch (2019). *WhatsApp blames —and sues— mobile spyware maker NSO Group over its zero-day calling exploit,* https://techcrunch.com/2019/10/29/whatsapp-spyware-nso-group

11 El Diario.es (2020). *Torrent se querella contra el exdirector del CNI por "espionaje político" y pide al juez comprobar si el Gobierno contrató el programa Pegasus,* https://www.eldiario.es/catalunya/torrent-querella-exdirector-cni-espionaje-politico-pide-juez-comprobar-si-gobierno-contrato-programa-pegasus_1_6136003.html

12 Irídia — Centre per la defensa dels drets humans (2025). *Tres directius de NSO Group imputats per la seva responsabilitat en l'espionatge amb Pegasus,* https://iridia.cat/tres-directius-de-nso-group-imputats-per-la-seva-responsabilitat-en-lespionatge-amb-pegasus/

in Israeli military intelligence units such as Unit 8200, Unit 81, or the Mossad. In this case, Niv Carmi (the 'N' in NSO), the technical founder of the NSO Group, was an intelligence officer and security expert at the Mossad.[13] Another recent example from the same market sector is Paragon Solutions,[14] which was founded in Israel in 2019 by Ehud Barak, a former Israeli minister, and Ehud Schneorson, a former commander in Unit 8200. The company's flagship product, Graphite,[15] is a spyware program with technical capabilities[16] comparable to Pegasus, which was at the centre of the latest spyware scandal in Italy.[17]

As stipulated by Israeli law governing the export of 'defence products', the Defence Export Control Agency (DECA) is responsible for issuing export licences to companies such as the NSO Group.[18] Reporting to the Israeli Ministry of Defence, DECA is the sole body responsible for supervising and controlling the global commercialisation of this technology for profit. The company typically invokes this authorisation to justify the existence of an alleged external control mechanism. However, this also highlights the company's direct links with the Israeli government.

NSO Group and the Israeli government: a lucrative partnership.

After 15 years in business, numerous articles and studies show that NSO Group has become a symbol of Israel's offensive cyber industry. It is publicly promoted as a strategic export tool serving the government. Marketed under the banner of 'high-tech defence technology made in Israel', Pegasus has been presented as a vital tool in Israeli foreign policy, strengthening, expanding and consolidating diplomatic relations. This activity has been accompanied by a campaign to gain public legitimacy, centred on four key areas: securitisation, normalisation, ethics laundering and Zionist patriotism.[19] This campaign

13 Forbidden Stories (2021). *The rise and fall of NSO Group,* https://forbiddenstories.org/the-rise-and-fall-of-nso-group/

14 The Citizen Lab (2025). *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations,* https://citizenlab.ca/2025/03/a-first-look-at-paragons-proliferating-spyware-operations/

15 The Citizen Lab (2025). *Graphite Caught. First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted,* https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

16 Amnesty International (2025). *Italy: New case of journalist targeted with Graphite spyware confirms widespread use of unlawful surveillance,* https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/

17 The Guardian (2026). *Italian activists and journalist targeted by spyware in 2024, prosecutors confirm,* https://www.theguardian.com/world/2026/mar/06/italy-activists-and-journalist-targeted-by-spyware-in-2024-prosecutors-confirm/

18 NSO Group (2024), *Transparency and Responsibility Report 2024.* https://www.nsogroup.com/wp-content/uploads/2025/02/2024-Transparency-and-Responsibility-Report.pdf

19 Kotliar, D. M., & Carmi, E. (2023). *Keeping Pegasus on the wing: legitimizing cyber espionage. Information, Communication & Society*, 27(8), 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873

presents surveillance as the only viable response to security challenges. This argument is also used in the European process of deregulation and simplification to justify the use of these tools and normalise them as inevitable in the name of innovation.[20]

This dynamic has resulted in a clear exchange of benefits: economic advantages for the company and increased geopolitical influence for Israel. Several studies have demonstrated a direct correlation between visits or meetings involving heads of state and Israeli government representatives, and the granting of new Pegasus export licences. This pattern has been observed in diplomatic normalisation processes, as a bargaining chip to improve diplomatic relations with the government of Israel —such as those involving Hungary, Poland, Rwanda, Azerbaijan or India,[21] as well as in international political negotiations, including votes at the United Nations, such as the cases of Mexico and Panama.[22]

In the case of Panama, a joint investigation by the Organized Crime and Corruption Reporting Project (OCCRP), a partner of *Forbidden Stories*, together with *Código Morse* and *Shomrim*,[23] has brought to light a new element that reveals this relationship of dependence between the company and the Israeli government. According to the investigation, published on 16 July 2026, Shalev Hulio, one of the founders of NSO Group, allegedly used an Israeli diplomatic passport to enter Panama on 3 December 2013. Panamanian migration records reportedly show that Hulio entered the country as a "diplomat" on a visit he himself described as "recreational", and told immigration authorities that he would be staying at the Israeli embassy. A year earlier, in 2012, the Panamanian government had reportedly signed a contract with NSO in a process led by Hulio himself.

The former NSO executive has denied these claims, but several experts believe the investigation once again puts the spotlight on the possible relationship between the two parties. Israeli lawyer Eitay Mack, known for his long-standing work against the use of Pegasus, sums it up: "[Pegasus] is an important tool for Israel to build ties, especially with the intelligence units of foreign countries […]. It is one of its main tools for creating and maintaining foreign relations."[24]

20 Ibid. 1500–1501.

21 Haaretz (2021). *The Pegasus Project: Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales,* https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000

22 The New York Times (2022). *The Battle for the World's Most Powerful Cyberweapon, A Times investigation reveals how Israel reaped diplomatic gains around the world from NSO's Pegasus spyware — a tool America itself purchased but is now trying to ban,* https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

23 OCCRP (2026). Co-Founder of Controversial Spyware Firm Had Israeli Diplomatic Passport, https://www.occrp.org/en/project/the-pegasus-project/co-founder-of-controversial-spyware-firm-had-israeli-diplomatic-passport

24 Ibid.

In recent years, the export and marketing of the Pegasus spyware system has also played a significant part in normalising Israel's relations with several Gulf states.[25] The 2020 Abraham Accords[26] aim to secure diplomatic support for Israel from Arab nations. The Israeli government exerts such influence over the NSO Group, the company that developed Pegasus, that it was able to reinstate[27] Saudi Arabia's licence to use the spyware following a phone call between Crown Prince Mohammed bin Salman and Benjamin Netanyahu, even after the company had withdrawn it due to Saudi Arabia's alleged involvement in the murder of Washington Post columnist Jamal Khashoggi at the Saudi consulate in Istanbul in 2018.

The power of influence of Pegasus was also highlighted by a post by the acting Israeli ambassador on the social network X, in which he threatened Pedro Sánchez's government with using and publishing all information relating to the Pegasus case in the Spanish State.[28] Some media outlets documented the post to ensure that a record of it remained, despite it having been deleted. [29] This post was published just hours after the Spanish president recognised the Palestinian state.

Spying, criminalising and silencing: Pegasus in Palestine.

Pegasus is the best-known case, but it is just the tip of the iceberg when it comes to Israeli cyber-surveillance technology being exported to enable authoritarian control around the world. What is often overlooked is that these systems were designed and tested in the context of the Israeli occupation of Palestine, and that they have also been used to undermine and criminalise Palestinian human rights organisations. Shortly after six Pal-

25 Haaretz (2022). *NSO Played Key Role in Israel's Gulf Diplomacy, NYT Finds, Confirming Haaretz Reports,* https://www.haaretz.com/israel-news/2022-01-28/ty-article/.premium/netanyahu-gave-greenlight-to-saudi-arabia-to-use-nso-spyware-report-says/0000017f-dc3d-d3ff-a7ff-fdbd5a680000

26 The Abraham Accords are a series of bilateral agreements initiated by the United States during the first Trump administration. The aim of these agreements was to normalise diplomatic relations between Israel and several Arab countries. The first agreement was signed on 15 September 2020 by Israel, the United Arab Emirates, and Bahrain. Sudan (October 2020) and Morocco (December 2020) were subsequently added. These agreements represent the first formal normalisation of Arab-Israeli relations since the peace treaty between Israel and Jordan in 1994, and the agreement between Egypt and Israel in 1979.

27 The New York Times (2021), *Israeli Companies Aided Saudi Spying Despite Khashoggi Killing,* https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

28 The use of Pegasus in the Spanish State has been identified through two distinct cases. The first one is the one covered in this report, concerning the Catalan Gate; the second one involves political representatives of the current Spanish government, in which Morocco was identified as the alleged perpetrator of the espionage.

29 Diario Red (2025). El embajador de Israel en funciones amenaza al Gobierno de España con revelar información obtenida con 'Pegasus', https://www.diario-red.com/articulo/espana/embajador-israel-funciones-amenaza-gobierno-espana-revelar-informacion-obtenida-pegasus/20250529191025048336.html

estinian human rights organisations were labelled "terrorist" 30 by Israel in November 2021, it emerged that six of their employees had been spied on using Pegasus.[31]

Espionage perpetuates the cycle of criminalisation by seeking to silence organisations such as Al-Haq, Addameer and the Bisan Centre. These organisations have spent years documenting and denouncing the war crimes and crimes against humanity that Israel has committed against the Palestinian people. The consequences for affected Palestinians extend well beyond the declaration of their work as illegal. Human rights defender Salah Hamouri[32] was imprisoned and subsequently deported to France.[33] He is now banned from returning to Palestine or practising as a lawyer in Israeli military courts.

Pegasus in the shadow of genocide.

These links with certain Israeli military and intelligence units form part of a state strategy designed to project prestige and reinforce the perception of the technological quality of their products. Since the start of the genocide in the Gaza Strip, this communication strategy has become particularly pronounced. Technology companies linked to the Israeli military-industrial complex have reinforced the narrative that their expertise in 'national security' contexts renders their products effective and reliable. This has been NSO Group's main argument in its attempts to re-enter the US market since being added to the US Department of Commerce's[34] sanctions list on 3 November 2021, under the justification of "putting human rights at the centre of United States foreign policy".[35]

Since October 2023, the NSO Group and a long list of other Israeli cybersecurity firms have volunteered to help locate Israeli hostages.[36] In fact, the NSO Group has begun upgrading its military surveillance technology to meet this need. Despite the highly competitive nature of the market, these companies have reportedly been collaborating on an unprec-

30 United Nations Human Rights Office of the High Commissioner (OHCHR) (2021). *UN experts condemn Israel's designation of Palestinian human rights defenders as terrorist organisations,* https://www.ohchr.org/en/press-releases/2021/10/un-experts-condemn-israels-designation-palestinian-human-rights-defenders

31 Amnesty Internat (2021). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware,* https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

32 Addameer (2022). *Lawsuit filed against Israeli spyware company NSO,* https://addameer.ps/es/news/4743

33 Front Line Defenders (2022). *Detained human rights defender Salah Hammouri was forcibly deported to France,* https://www.frontlinedefenders.org/en/case/detained-human-rights-defender-salah-hammouri-was-forcibly-deported-france

34 The Intercept (2023). *Israeli Spyware Firm NSO Demands "Urgent" Meeting With Blinken Amid Gaza War Lobbying Effort,* https://theintercept.com/2023/11/10/nso-group-israel-gaza-blacklist/

35 Ibid.

36 Haaretz (2023). *NSO, Israeli Cyber Firms Help Track Missing Israelis and Hostages,* https://www.haaretz.com/israel-news/security-aviation/2023-10-19/ty-article/.premium/israeli-cyber-arms-and-intelligence-firms-like-nso-aiding-israeli-efforts/0000018b-4813-de3d-a58f-c87b7d950000?v=1698415601171

edented joint initiative since 7 October, presenting a united front in the field of digital 'intelligence' and promoting Israeli technology as unique worldwide. These moves have been described by international organisations such as Democracy for the Arab World Now (DAWN) as 'an attempt by the company to restore its image in the midst of a crisis'. [37]

As of October 2023, it is clear that the Israeli government is once again allowing NSO to play a significant and prominent role in an unprecedented military deployment. A 19 October 2023 podcast[38] by the Israeli media outlet Haaretz — a format which, according to several analysts, is subject to less censorship than print media in Israel — examines how NSO acts on behalf of the government, undertaking significant tasks for the Ministry of Defence. This development is far from exceptional or unprecedented; it highlights the ongoing nature of the long-standing collaboration between the company and the Israeli government. This was accompanied by the January 2024[39] announcement that the NSO Group was moving to larger offices as part of a corporate expansion plan.

At present, it is not known for certain to what extent or in what way Pegasus is being used in the Gaza Strip. However, what is clear is that the Israeli occupying forces are deploying their full technological arsenal, as confirmed by the present report. Investigative media outlets such as +972 Magazine[40] have sounded the alarm over a specific AI tool designed to compile lists of potential military 'targets'. This system quickly analyses and cross-references large volumes of data to identify thousands of people or places, such as homes, for bombing. In the case of Lavender —described as the artificial intelligence machine that directs Israel's bombings of the Gaza Strip—, [41] verification involves locating phones or voice recordings to determine the gender of the person in question. This is the only procedure that enables the system to confirm ownership of the device. Some international experts have pointed out that Pegasus's capabilities, which allow remote access to and control of a mobile device, including geolocation and microphone activation, have played a critical and fundamental role in gathering data from the Gaza Strip during the ongoing genocide.[42] This has been described as a 'mass murder factory'.[43]

---

37 The Intercept (2023). *Israeli Spyware Firm NSO Demands "Urgent" Meeting With Blinken Amid Gaza War Lobbying Effort.*

38 Haaretz (2023). *יאיר גולן: השיח של ההרתעה הוא פרימיטיבי. הפעילות מול חמאס תימשך שנים* https://www.haaretz.co.il/digital/podcast/weekly/2023-10-19/ty-article-podcast/0000018b-470f-df22-a5eb-4f7fb1be0000

39 Globes (2024). *Israeli spyware co NSO moving to bigger offices,* https://en.globes.co.il/en/article-israeli-spyware-co-nso-moving-to-bigger-offices-1001466834

40 +972 Magazine (2024). *'Lavender': The AI machine directing Israel's bombing spree in Gaza,* https://www.972mag.com/lavender-ai-israeli-army-gaza/

41 La Directa (2024). *Lavender: la màquina d'intel·ligència artificial que dirigeix el bombardeig d'Israel a Gaza,* https://directa.cat/lavender-la-maquina-dintelligencia-artificial-que-dirigeix-el-bombardeig-disrael-a-gaza/

42 Youtube (2024). *Roda de premsa Irídia vs. Pegasus. Minut 35:57*—38:30, https://www.youtube.com/watch?v=l3zqiwFJtyA&t=1s

43 +972 Magazine (2023). *'A mass assassination factory': Inside Israel's calculated bombing of Gaza,* https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/

NSO Group in Europe, with its headquarters in Luxembourg.

Although the company justifies its product on the grounds of 'national security', available data show that this technology has been used against hundreds of thousands of individuals from civil society[44] who posed no threat to the states involved. Such practices encourage the use of the concept of 'criminal potential', based on the idea of an unfounded threat. This is a common mechanism in the use of surveillance technologies. Numerous international organisations have therefore called for a ban on Pegasus.[45]

NSO Group Technologies Ltd. is a private company incorporated and registered in Israel, but the name 'NSO Group' is used as an umbrella brand for its associated operational and financial companies located around the world. The rapid expansion and proliferation of this sector is reflected in NSO's[46] corporate structure, highlighting a worrying reality of the present day.[47] The group operates through a deliberately opaque, dendritic structure comprising 13 holding companies and 12 subsidiaries across multiple jurisdictions. Companies often change their names and expand their activities into other jurisdictions to circumvent stricter regulations.[48] It is therefore important to analyse how the group operates in Europe as an example of the kind of practices and logic replicated within the surveillance market. This type of company is characterised by a lack of transparency and effective accountability mechanisms regarding its activities and exports. This hinders access to verifiable information, including legal proceedings brought by individuals who have been spied on using Pegasus.[49]

NSO has a particularly significant corporate network presence in Luxembourg. As a founding member of both the EU and the Eurozone, Luxembourg has established itself as a strategic hub for international businesses. This is due to its access to the European market, its flexible business environment, its advanced technological infrastructure, its economic stability and its specialisation in cybersecurity. Furthermore, Israel actively

44 Forbidden Stories (2021). *The Pegasus Project, Global Democracy under cyber attack,* https://forbiddenstories.org/about-the-pegasus-project/

45 EDRI (2025). *Spyware and state abuse: The case for an EU-wide ban.*

46 La marca comercial "NSO Group" es propiedad exclusiva de la empresa matriz israelí NSO Group Technologies Ltd.

47 EDRI (2025). *Spyware and state abuse: The case for an EU-wide ban.*

48 SMEX (2025). *Click, Load, Kill: A Look into the Cyberweapon industry in the WANA Region.* 28—45, https://smex.org/new-research-click-load-kill-a-look-into-the-cyberweapon-industry-in-the-wana-region/

49 El Diario.es (2025). *La exjefa del CNI vuelve a escudarse en que la ley le impide declarar por el espionaje a dos diputados de ERC,* https://www.eldiario.es/catalunya/exjefa-cni-vuelve-escudarse-ley-le-impide-declarar-espionaje-diputados-erc_1_12640307.html

promotes Luxembourg as a destination for business expansion.[50] At the time of writing this report, NSO had nineteen registered companies, eleven of which shared the same corporate purpose.[51] This corporate structure broadens the scope of these organisations' activities, giving them an instrumental role by expanding their area of operation without clearly defining their purpose. Furthermore, these companies share both their corporate purpose and their physical location. [52]

The final report by the European Parliament's PEGA Committee[53] concluded that NSO's continued existence depends to a large extent on the support of companies based in Luxembourg. The report identified these entities as the group's European business hub. This hub enables the group to operate under less stringent regulations within the EU and third countries. It also manages invoicing, contracts, and payments relating to spyware.[54] The EU's lenient stance on the commercial spyware market enables these companies to market their products legitimately from within Europe and operate within a relaxed regulatory framework.

Of the nineteen companies linked to the NSO Group and registered in Luxembourg, Osy Technologies Sàrl and Q Cyber Technologies Sàrl are particularly notable, both due to their connection to cyber technology and their importance within the group's structure. Osy Technologies, established in February 2014, was the first company of the group in the country, followed by Q Cyber Technologies, founded in January 2016 with Osy as the sole shareholder. Both are located in the group's original European headquarters, which consolidated rapidly through corporate expansion involving three acquisitions in 2017, four in 2018 and five in 2020. Osy and Q Cyber are closely linked to NSO Group Technologies; in fact, they shared a board of directors in the early years. Omri Lavie and Shalev Hulio, two of NSO's founders, play a key role.[55]

According to the Israeli courts, this structure also served a tax purpose. In August 2026, an Israeli court convicted NSO Group of fraud. According to the ruling, between 2014

50 Luxembourg Trade & Invest. Your gateway to Luxembourg and Israel, https://luxembourgtradeandinvest.com/our-international-network/ltio-tel-aviv

51 The corporate purpose of eleven of these companies is to be formally appointed by contract, articles of association, or a decision of a competent body to hold offices or perform functions in other companies. This includes acting as managing directors, acquiring shareholdings in Luxembourg or abroad, and being involved in management.

52 Fourteen of the nineteen NSO Group companies in Luxembourg have the same registered office, while the remaining five are located at different addresses.

53 He spent a year investigating cases of espionage involving Pegasus in the European Union, with a particular focus on Hungary, Poland, Greece and Spain. Más información en: https://www.europarl.europa.eu/regdata/etudes/brie/2024/761472/ipol_bri(2024)761472_EN.pdf

54 European Parliament (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.* 397—399, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

55 The fact that Lavie sits on the boards of nine Luxembourg companies and Hulio on six reinforces the idea of an interconnected, centrally managed structure.

and 2018 the group received 86 million dollars in profits through Osy without paying the corresponding taxes in Israel.[56] The court also concluded that NSO's ownership structure through Osy was created, at least in part, to reduce the taxes on its debt and financing operations.

Beyond the tax motive, the presence in Luxembourg has also helped the group build a new image. *It should be noted that when the management team and founders of NSO Group announced on 14 February 2019 that British private equity firm Novalpina Capital was taking (...)*

It should be noted that when the management team and founders of NSO Group announced on 14 February 2019 that British private equity firm Novalpina Capital was taking control, the group had already presented itself as a 'cyber technology company based in Luxembourg', formed through the 'merger of Israeli and European cyber technology companies'.[57] This rebranding was intended not only to make the group's corporate identity appear more European, but also to position the group institutionally and legitimise its activities within the European cybersecurity market. The rebranding also sought to distance the group from its direct links with Israel, particularly in light of the controversies surrounding the use of Pegasus. However, this more diffuse corporate identity, which has enabled the group to integrate more seamlessly into the global market, has come into conflict with its founding values, reaffirmed after October 2023, when the group unequivocally aligned itself with the Israeli government.

Following the Pegasus scandals of mid-2022, Shalev Hulio stepped down as CEO of the NSO Group, with Yaron Shohat taking over the role. In January 2023, Hulio founded Dream Security.[58] While serving as an Israeli reservist in the Gaza Strip on 7 November 2023, Hulio announced a funding round,[59] describing it as a "great message for the tech community and the people of Israel".[60] Despite his attempts to distance himself from the NSO Group, a dozen former senior executives and operatives have joined him at Dream Security. While most of the company's staff are based in Israel, Dream Security also has offices in Tel Aviv, Vienna, and Abu Dhabi. The company was founded amid controversy due to its

56 Lexology (2026). Q Cyber Technologies Ruling: District Court Holds That a Leveraged Acquisition Structure May Constitute an Artificial Transaction, https://www.lexology.com/library/detail.aspx?g=4c2105a1-094c-410e-a495-7d50ac920f64

57 Amnesty International, Privacy International & SOMO (2021). *Operating from the Shadows: Inside NSO Group's Corporate Structure.* 42—27, https://www.amnesty.org/es/documents/doc10/4182/2021/en/

58 Dream Security is a start-up specialising in defensive cybersecurity solutions for critical infrastructure, with the stated ambition of becoming the "world's best AI-based defensive cybersecurity platform". Further information is available at: https://dreamgroup.com/about/

59 The Intercept (2024). *In Video From Gaza, Former CEO of Pegasus Spyware Firm Announces Millions for New Venture,* https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/

60 El Salto Diario (2024). *Los señores israelíes de la ciberguerra,* https://www.elsaltodiario.com/espionaje/senores-israelies-ciberguerra-pegasus-predator

links with the Israeli and international right, particularly because of Sebastian Kurz's involvement as a co-founder[61] —the former Austrian chancellor. Like the NSO Group, Dream Security is expanding rapidly and maintaining a prominent presence in Europe.

WhatsApp vs. NSO Group and corporate responsibility.

The lawsuit filed by WhatsApp and Meta against the NSO Group in the United States[62] in 2019 was a pivotal moment in the company's reputational crisis. During the legal proceedings, the US Department of Commerce added the NSO Group to its sanctions list in 2021[63] on the grounds that its activities were contrary to national security interests. Since then, the NSO Group has been banned from operating in the US market, and its staff have been barred from entering the country.[64] Despite the economic and political impact of this sanction, the European Union has neither adopted equivalent measures nor established a common position on the Pegasus ban.

In December 2024, a Californian court found the NSO Group guilty of breaching federal and state computer fraud and abuse laws. The court ruled in favour of WhatsApp,[65] awarding damages totalling over 168 million dollars.[66] The proceedings once again highlighted the group's lack of transparency and demonstrated that the NSO Group carries out the initial stages of infecting and extracting data from targeted devices. This contradicts the narrative that the group has maintained until now,[67] and the ruling has been hailed internationally as a significant step forward in the fight against spyware abuse.[68]

61 Follow The Money (2025). *The Talented Mr. Kurz: How Austria's Ex-Leader Leader made it big in Israeli Cyber industry,* https://www.ftm.eu/articles/spyware-sebastian-kurz

62 The New York Times (2019). *WhatsApp Says Israeli Firm Used Its App in Spy Program,* https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html?auth=login-email&login=email

63 The Guardian (2021). *Israeli spyware company NSO Group placed on US blacklist,* https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

64 The Guardian (2024). *US announces new restrictions to curb global spyware industry,* https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions

65 Sentencia procedimiento WhatsApp v. NSO Group (2024). Para mayor información consulta: https://www.documentcloud.org/documents/25467209-gov/

66 The Record Media (2025). *Jury orders NSO Group to pay $168 million to WhatsApp for facilitating Pegasus hacks of its users,* https://therecord.media/jury-orders-nso-to-pay-meta-168-million-over-whatsapp-hack

67 The Guardian (2024). *NSO – not government clients – operates its spyware, legal documents reveal,* https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp

68 Access Now (2025). *Statement on the historic decision in the WhatsApp v NSO case,* https://www.accessnow.org/press-release/statement-on-whatsapp-v-nso-case-decision/

Strategic reorientation towards the 'Americanisation' of NSO Group.

Although the NSO Group's reputation crisis forced dozens of female employees to relocate, the company continued to operate under the leadership of one of its founders, Omri Lavie, until November 2025. After 25 years in business and with over 22 clients in Europe alone, including 12 of the 27 member states,[69] a significant change in management took place. This marked a turning point in the company's history, as it was the first time that the founders — some of whom had been involved since 2010 — no longer held any shares.

This new phase is being led by David Friedman,[70] an American lawyer. This development follows a group of US investors (some of whom are Israeli nationals) taking full control of the company, thereby highlighting its links with the Israeli government and far-right circles. The current chief executive was the US ambassador to Israel during the first Trump administration and participated in the negotiations for the Abraham Accords. He is also known for publicly defending illegal settlements in occupied Palestinian territory and for leading fundraising campaigns with this objective in mind. This change in management and ownership is indicative of a wider trend towards Americanisation within the NSO Group.

This change marks a new direction for the group: on paper it is now an American company, but it continues to operate effectively from Israel. The same is true of Paragon, which in December 2024 merged with REDLattice,[71] an American offensive cybersecurity company owned by the investment fund AE Industrial Partners. It is also the case of Candiru, which was acquired by the American investment firm Integrity Partners.[72] All three companies are now competing for contracts in the United States, despite the sanctions imposed on them.

In the current climate, a growing number of Israeli companies are choosing to establish or relocate subsidiaries in Europe. While this has been a common practice for years, it has now intensified. Companies are attracted by a more permissive legislative environment that facilitates growth in the European market for commercial spyware.[73]

---

69 Haaretz (2022), *Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone,* https://www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000

70 Haaretz (2025), *Ex-Trump Ambassador to Israel David Friedman Named NSO Chairman, as Spyware Firm Shifts to U.S. Ownership,* https://www.haaretz.com/israel-news/security-aviation/2025-11-09/ty-article/.premium/ex-trump-ambassador-to-israel-named-nso-chairman-as-spyware-firm-shifts-to-u-s-ownership/0000019a-68f4-da41-a9fe-79f7966f0000

71 Wired (2026). The Secrets of a US Spyware King, https://www.wired.com/story/the-secrets-of-the-us-spyware-king/

72 Ibid.

73 For further information, please refer to section IV.2 (page 37) on the regulatory framework in Europe.

At the same time, there have also been changes in management and ownership at three NSO Group companies registered in Luxembourg.[74] These companies are now led by Ohad Shazar and Shalem Schremer,[75] along with their team. Shazar, an Israeli lawyer, lives in the illegal settlement of Neve Daniel in the occupied Palestinian territory of Gush Etzion and sits on the board of a settlers' association. This new leadership reflects an agenda that aligns with far-right views in Israel and internationally, as well as colonial interests.

74 The three NSO Group companies in Luxembourg that changed their registered address are: North Pole Newco, Osy Technologies, and Q Cyber Technologies.

75 Ibid.