The European gateway for genocide technology

The traceability of the Israeli security technology sector in Europe

---

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

The European gateway for genocide technology

The traceability of the Israeli security technology sector in Europe

Authors: Observatory for Human Rights and Business in the Mediterranean (Felipe Daza, Carlos Díaz, Nora Miralles) and Irídia – Center for the Defense of Human Rights (Cèlia Carbonell Cassanyes and Laura Riba Singla)

Coordination: Maite Ramos i Alys Samson

Communication: Lucrecia Baquero Ramos

Legal assistance: Laia Serra Perelló

Layout: Carmela Márquez B @edicionescaseras

The authors would like to thank MigrESS, Who Profits, DIMSE, European Digital Rights (EDRi) and Access Now for their review and comments, which have helped to improve the quality of this reporte.

with the support of:

Agència Catalana de Cooperació al Desenvolupament

Generalitat de Catalunya

ICIP INTERNATIONAL CATALAN INSTITUTE FOR *PEACE*

Table of contents

LIST OF ACRONYMS **6**

Introduction **8**

I Contextualisation:
the genocide and impact of security
and military technologies. **11**

II The Gaza Strip as a laboratory
of genocide technologies
that are arriving in Europe **17**

III Main companies and key investors
in the development and funding of
the technology used for the genocide 2023 ..... **20**

1. The major companies of the military industry
and security, the great beneficiaries. 21
2. The drone sector, a pie shared
among many investors. 24
3. Spyware, robotics, facial
recognition and other sectors 26
4. Genocide as a financial product. 29

IV Structural factors of the Israeli
business penetration in Europe. **31**

1. Offshoring, specialists and Israeli
capital heading towards the continent 33
2. European Regulatory Framework 34
3. Control of a securitisation narrative. 35
4. Deregulation: neglecting rights
for the sake of 'competitiveness'. 36
5. European legal framework applicable
to intrusive surveillance technologies. 37

V Gateways for Israeli defence tech companies. **46**

1. European rearmament through NATO and the ReArm Europe Plan 47
2. The Ukraine war and penetration of Israeli companies via Eastern Europe 52
3. The epicentre of the Israeli military lobby: Germany. 54
4. Participation in technology and cybersecurity events as a mechanism to access the EU 57
5. From soft-landing in Cyprus to opaque corporate structures 60
6. Luxembourg as a launch pad. 62
7. Acquisition of European companies and r ebranding in order to operate in the EU 68
8. Access to the European Union through funding programmes. 72
9. Barcelona as a technology hub of cybersecurity companies 75

Conclusions and recommendations **80**

TERMINOLOGY CLARIFICATIONS:

According to international law, Israel is illegally occupying the Palestinian territories of the West Bank and East Jerusalem, as well as the Gaza Strip. Other authors consider that the whole of Historic Palestine (the colonised territory under the British protectorate between 1918 and 1948) is occupied, as the State of Israel was created after the destruction of over 500 Palestinian villages and the expulsion of a large number of the native population who lived there, the Palestinian people. When the United Nations Partition Plan for Palestine was voted, all neighbouring countries voted against it and the Palestinian people were not consulted.

In this report, when we mention the Occupied Palestinian Territory (OPT), we are referring to the Gaza Strip, East Jerusalem and the West Bank.

LIST OF ACRONYMS

ACCIÓ	Agency for Business Competitiveness (Government of Catalonia)
CAAT	Campaign Against Arms Trade
C4I	Command, Control, Communications, Computers, and Intelligence
UNHRC	United Nations Human Rights Council
CRA	Cyber Resilience Act
CSDD	Corporate Sustainability Due Diligence Directive
CTEM	Continuous Threat Exposure Management
DIANA	Defence Innovation Accelerator for the North Atlantic
DM	Digital Markets Act
DPAP	Defence Production Action Plan
DSA	Digital Services Act
EDF	European Defence Fund
EDRI	European Digital Rights Network
EIC	European Innovation Council
ELNET	European Leadership Network
EMFA	European Media Freedom Act
ESDI	Security and Defence Initiative
GCS	Ground Control Station
GII	Global Israel Initiative
GINSUM	German Israeli Network of Startups & Mittelstand
IA	Artificial Intelligence

IAI	Israel Aerospace Industries
DFI	Direct Foreign Investment
IDSF	Israel Defence and Security Forum
INCIBE	Spanish National Cybersecurity Institute [Institut Nacional de Ciberseguretat d'Espanya]
MFF	Multiannual Financial Framework
NSPA	NATO Support and Procurement Agency
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
UN	United Nations
NATO	North Atlantic Treaty Organization
PEGA	European Parliament's Pegasus Inquiry Committee
PURL	NATO Prioritised Ukraine Requirements List
R+D	Research and Development
GDPR	General Data Protection Regulation
RPAS	Remote Piloted Aircraft Systems
UAV	Unmanned Aerial Vehicle
EU	European Union
UNOSAT	United Nations Satellite Centre

Introduction

The genocide perpetrated by Israel in the Gaza Strip has been used by the global military-industrial complex to develop new technologies and military strategies that have proven to be extremely beneficial to economic and political elites. This phenomenon is reflected in the **emergence of the tech defence sector, characterised by the symbiotic relationship between military and security technology companies**. Standing out among their applications are the innovation and development of cybersecurity technologies, artificial intelligence (AI), biometric recognition and state-of-the-art drones, among other applications. In many cases, these companies produce civil-military dual-use technologies and therefore offer their services to institutions of the military industry, security agencies and other public actors, in order to increase the control and surveillance of the population, including migratory control.

This study analyses **the Israeli defence tech[1] companies that have emerged or been strengthened as a result of the genocide in the Gaza Strip** and the occupation of Palestinian territory. And, more specifically, the manner in which they are transferring the knowledge they have acquired and the developed products to Europe. The Occupied Palestinian Territory has been used by Israel as a 'laboratory' of Israeli defence and military technologies. The uncontrolled major offensive against Palestinian territory in the Gaza Strip has not only continued with this logic, but has amplified it to an extreme. A key point of this trend is that **over a third of Israeli startups of the defence industry has been created since 7 October 2023.[2]**

According to Sherrington Hoffman, director of Global Partnership at the Israeli agency Startup Nation Central, 'We're seeing a change in what defence tech has become as a sector. Defence spending is skyrocketing worldwide, coupled with, obviously, local and geopolitical concerns that Israel is facing but have really fast-tracked some of the inventions, created this situation where there is **battle-tested innovation, that is being validated so quickly** at a speed and rate that we have not seen for a while'.[3] According to Startup Nation Central, in 2025 the Israeli defence ecosystem was made up of over 300 startups in operation (compared to 160 in 2024). This unstoppable growth includes new projects focused on unmanned vehicles and drones; C4I systems (Command, Control,

1 This refers to the set of technologies, systems and innovations developed for military use or security. It includes both the development of weapons and other technology tools used by armies, governments or companies linked to defence.

2 Harris, L. (2024, 25 August). Your Taxes: Israel's R&D edge over other OECD countries. *The Jerusalem Post*. https://www.jpost.com/business-and-innovation/article-868577

3 Spiro, J. (2025, 25 February). AI, drones, and the explosive growth of Israel's dual-use defensetech industry. *CTech*. https://www.calcalistech.com/ctechnews/article/b16ehzo5kg

Communications, Computers, and Intelligence); electronic systems; missile defence system and other dual-use technologies.[4]

At the same time, with the European rearmament and subsequent increase of the defence expenditure of NATO members, **the region has been consolidated as a pole of attraction for numerous Israeli defence tech companies that have taken part in the genocide and occupation of Palestine**. These companies use diverse strategies to penetrate the European continent and access contracts in the defence and security sectors. However, there is no systematic scrutiny of how these companies and their dual-use technologies manage to penetrate Europe.[5] In this regard, the specific objectives of this report are:

- Put the spotlight on who benefits and who funds the genocide as regards companies and type of technology, as well as the financial funds that enable them to operate and collect dividends.
- Explore the traceability of companies in the defence tech and technological security sector, paying special attention to the countries, mechanisms and actors that facilitate their penetration.
- Study the legal and bureaucratic conditions that enable defence tech companies to establish themselves in the European Union (EU) without any trouble.
- Investigate the records and activity of cybersecurity and surveillance companies created in Europe, with Israeli or international links that operate as national companies, potentially avoiding scrutiny (map of affiliate companies, innovation and production centres, etc.).

4 Startup Nation Central. (2025, 3 April). *Startup Nation Central's 2025 Israel Defense Tech Companies Sees Surge in Companies in the Sector*. PR Newswire. https://www.prnewswire.com/news-releases/startup-nation-centrals-2025-israel-defense-tech-companies-sees-surge-in-companies-in-the-sector-302419767.html

5 Dual-use technologies may be used for both civilian and military applications. In other words, they are technologies, equipment, software or knowledge that have been developed with an apparently civilian purpose (for example, scientific, industrial or commercial purposes), but they may also be used for defence, surveillance or repression purposes.

The purchase of these technologies by government and companies in the European continent takes place within a framework of increased technological surveillance, legal suppression and growing police violence against activism,[6] where there is a plausible risk that technologies of some of the companies mentioned in this report are being used.

Therefore, the analysis of the gateways used to enter these technologies into Europe do not only constitute a business traceability exercise, but is also an interrogation of the structural responsibilities of European states in the reproduction of a global colonial order, where security is considered more important than human rights and technology innovation is legitimate, even when it has been created and used in contexts of extreme violence.

6 United Nations. (2025, 16 October). *UN experts urge Germany to halt criminalisation and police violence against Palestinian solidarity activism*. OHCHR. https://www.ohchr.org/en/press-releases/2025/10/un-experts-urge-germany-halt-criminalisation-and-police-violence-against
See also: AFP. (2025, 16 October). Dozens charged under anti-terror laws in UK court over Palestine Action support. The Times of Israel. https://www.timesofisrael.com/dozens-charged-under-anti-terror-laws-in-uk-court-over-palestine-action-support/

Contextualisation: the genocide and impact of security and military technologies.

In September 2025, the Independent International Commission of Inquiry on the Occupied Palestinian Territory, a commission set up by the UN Human Rights Council, decided that Israel has committed genocide against Palestinians in the Gaza Strip.[7] This independent authority reached this conclusion after Israel had maintained a blockage in the Gaza Strip by land,[8] sea and air for 18 years and, since, in October 2023, the Israeli army initiated a new invasion and attack on the same territory.[9]

Genocide, understood as a deliberate attempt to completely or partially destroy a national, ethnical, racial or religious group, constitutes one of the most serious human rights violations. Traditionally, the analysis of genocides has always focused on their political, ideological and military dimension, although in recent decades it has become evident that control technologies, cybersecurity, surveillance and AI play a growing role in their preparation, execution and even their justification. According to Jalal Abukhater, Policy Manager at 7amleh, an organisation to defend Palestinians' rights, 'The AI systems refined during the war, whether for predictive analytics, biometric monitoring, automated targeting, or mass data extraction will entrench and expand the occupation and apartheid regime. **These tools don't disappear after conflict – they become part of everyday governance'.**[10]

In a racialised global order, territories subjected to colonial domination operate as laboratories, where control, surveillance and violence techniques are tested. After they have been stabilised, they are normalised and are reexported as security 'solutions'. Within this framework, the decades-long occupation of Palestine has resulted in the consolidation of a technopolitical ecosystem in which innovation is validated on racialised bodies that have been dispossessed of their rights, **converting permanent exceptionality into infrastructure and a model**. As Ruha Benjamin warns, far from eliminating racism, contemporary technologies tend to reproduce and automate it, hiding it under narratives of neutrality, efficiency and progress.[11]

Based on this analysis, the genocide in Gaza would be an especially crude expression of this general regime of power, in which technology intertwines with historical schools of

7 United Nations. (2025, 16 September). *Israel has committed genocide against Palestinians in the Gaza Strip*. UN News. https://news.un.org/es/story/2025/09/1540443

8 In June 2007, after Hamas came to power in Gaza, Israeli authorities significantly intensified existing movement restrictions, virtually isolating the Gaza Strip from the rest of the occupied Palestinian territory, and the world.

9 United Nations Office for the Coordination of Humanitarian Affairs. (2022, 30 June). *Gaza Strip | The humanitarian impact of 15 years of the blockade – June 2022*. https://www.ochaopt.org/content/gaza-strip-humanitarian-impact-15-years-blockade-june-2022

10 Lessware, J. (2025, 27 November). How Israel's use of AI in Gaza has transformed warfare and the 'automation of apartheid'. *Arab News*. https://www.arabnews.com/node/2624225/middle-east

11 Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity Press.

thought on colonial and racial domination.[12] From this perspective, **genocide is not understood as an anomaly or temporary alteration of market performance, but a circumstance that enables new ways of business accumulation and expansion**. The report by the UN Special Rapporteur, Francesca Albanese,[13] reinforces this interpretation by pointing out that numerous companies directly or indirectly benefit from occupation, apartheid and genocide, providing infrastructure, including technological infrastructure, without which violence and mass surveillance could not be deployed with the same effectiveness. **Subcontracting military and intelligence functions to private companies thus contributes towards privatising violence, diluting political responsibility** among contracts, affiliates and transnational supply chains. From an antiracist approach, this corporate economy of war strengthens a world order in which the destruction of racialised populations turns into a business opportunity, normalising business impunity at the same time.

There is some literature that is not so hegemonic and more critical – literature written from a decolonial and antiracist perspective – that focuses on its insertion in material structures of domination and particularly **in racial capitalism**: a concept developed by Cedric J. Robinson to describe an economic system that depends structurally on racial hierarchy and the unequal exploitation of populations considered dispensable.[14]

The events that occurred in the Gaza Strip qualify as genocide, since they fit the definition established by the 1948 Convention on the Prevention and Punishment of the Crime of Genocide,[15] which defines genocide as crimes committed 'with intent to destroy, in whole or in part, a national, ethnical, racial or religious group'.[16]

This definition does not strictly limit genocide to a specific military operation or a closed temporary period, but perceives it as a pattern of acts guided by a particular intentionality, the total or partial destruction of a group. In this regard, genocide does not necessarily end by signing a ceasefire or political agreement if there is still behaviour directed towards making the affected group's physical or social survival impossible.

12 Along these lines, Achille Mbembe has pointed out that in contemporary order, sovereignty is exercised through the capacity to decide who may live and who must be exposed to death or lethal conditions of existence, a logic that is conceptualised as necropolitics.

13 United Nations Human Rights Council. (2025, 2 July). *From economy of occupation to economy of genocide: Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967* (A/HRC/59/23). https://docs.un.org/en/A/HRC/59/23

14 Robinson, C. J. (2020). *Black Marxism: The making of the Black radical tradition*. University of North Carolina Press.

15 United Nations. (2025, 16 September). *Israel has committed genocide in the Gaza Strip, UN Commission finds*. OHCHR. https://www.ohchr.org/en/press-releases/2025/09/israel-has-committed-genocide-gaza-strip-un-commission-finds

16 International Association of Genocide Scholars. (2025, 6 September). Resolution of the IAGS on the situation in Gaza. *Viento Sur*. https://vientosur.info/resolucion-de-la-iags-sobre-la-situacion-en-gaza/

In the current context in the Gaza Strip, the systematic deprivation of food, access to drinking water, healthcare, shelter, hygiene and items that are essential for survival, as well as the forced and repeated displacement of the civil population cannot be analysed as isolated events or mere collateral consequences, but as elements of a continuous pattern that could constitute a prolongation of the crime of genocide. Therefore, speaking of genocide as regards the Gaza Strip does not only imply performing a retrospective reading of the events that commenced in October 2023, but also carrying out a present-day analysis of behaviours that, due to their nature and intentionality, can still be classified as the crime of genocide, in accordance with international law in force.

However, Israel's colonial project is not limited to the genocide offensive in the Gaza Strip. **Since October 2023, in the West Bank both the Israeli army and armed settlers have intensified the control, mass surveillance and the attacks on the Palestinian population.**[17]

In this regard, different international bodies have documented a very significant increase of violence, perpetrated by Israeli settlers, security forces and the Israeli army in the West Bank. According to the UN Human Rights Office in the Occupied Palestinian Territory and the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), which monitor the incidents and attacks associated to settlers,[18] between 7 October 2023 and mid-October 2025, more than 1,000 Palestinians were assassinated in the occupied West Bank and East Jerusalem.[19]

The report from the United Nations special committee to investigate Israeli practices states that, as an occupying power, the State of Israel is obliged to protect civilians and prevent settlers from scaling the violence, which not only does it ignore, but Israeli security forces (police and army) often work in collusion with armed settlers.[20]

New control, cybersecurity, surveillance and artificial intelligence technologies do not only widen the lethal capacity of government and companies, **they also transform the way in which mass violence is planned, managed and legitimised.**

---

17 Palestinian Return Centre. (2025, 23 September). *PRC to UNHRC: Settlers violence in the West Bank is a systematic 'colonial project,' not a response to October 7.* https://prc.org.uk/en/post/5041/prc-to-unhrc-settlers-violence-in-the-west-bank-is-a-systematic-colonial-project-not-a-response-to-october-7

18 Office of the United Nations High Commissioner for Human Rights. (2025, 17 October). *UN Human Rights in Occupied Palestinian Territory: 1001 Palestinians killed in West Bank since 7 October 2023 — one in five are children* [Press release]. United Nations. https://www.un.org/unispal/document/ohchr-press-release-17oct25/

19 United Nations Office for the Coordination of Humanitarian Affairs – occupied Palestinian territory. (n.d.). *Settler-related violence*. https://www.ochaopt.org/page/settler-related-violence

20 Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories. (2025, 5 September). *Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories* (A/80/365). United Nations. https://www.un.org/unispal/document/special-committee-israeli-practices-report-05sep25/

This phenomenon intensifies when these technologies are developed and tested within a context of conflict and/or occupation. In this regard, the Gaza Strip genocide fits the expression coined by Mbembe, 'death worlds', where power is not limited to killing but it organises the exposure to death and confines populations to degraded living conditions, as if life were no more than a piece of waste.[21] However, this regime does not only operate through death, it also functions by causing harm. Jasbir K. Puar broadens the analysis when she points out that colonial power can govern keeping populations in a permanent state of injury and precarity. The 'right to maim' describes **a system that manages damaged life as a control strategy.**[22] Amputations, irreversible injuries and psychosocial trauma documented in the Gaza Strip can be construed from this perspective: as part of a government technology that not only kills, it also controls wounded life.

The incorporation of AI systems and mass surveillance boost this process and convert genocide into a technopolitically managed device: the lethal decision moves towards opaque algorithmic infrastructures and the principles of responsibility and democratic control are eroded. Within this framework, biometric surveillance and automated targeting make it easier to exercise violence faster and at a greater distance, with a higher degree of impunity.

The conflict's technification has multiple effects. On the one hand, it **increases destruction capacity and accelerates execution**: automation means attacks can be made at an unprecedented scale and speed, with direct impacts on the civilian population. On the other, digitalising the war **weakens accountability**: when decisions with immediate consequences for human rights depend on opaque algorithms, frequently of a closed-source nature and, therefore, difficult to audit, the civil society is unable to monitor either the biases or functional logic, thus diluting human responsibility. This makes it difficult to subsequently investigate crimes and identify the responsible parties.[23] At the same time, purchase agreements for these technologies do not include licence revocation in the event that they are used for purposes that constitute a violation of human rights.

In parallel, the military-technology complex has been consolidated as a structural element in the exercise of power and often operates with dual-use technologies. According to a report published in 2024 by the Global Centre for the Responsibility to Protect, 'How these technologies are utilized, and by whom, greatly impacts their capacity to strengthen or degrade societal resilience to atrocities'.[24] **The same digital infrastructure that can**

21 Mbembe, A. (2019). *Necropolitics*. Duke University Press.

22 Puar, J. K. (2017). *The right to maim: Debility, capacity, disability*. Duke University Press.

23 International Committee of the Red Cross. (2019, June). *Artificial intelligence and machine learning in armed conflict: A human-centred approach*. https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach

24 Global Centre for the Responsibility to Protect. (2024, March). *The relationship between digital technologies and atrocity prevention* (Policy brief). https://www.globalr2p.org/wp-content/uploads/2024/03/2024-March-Digital-Technologies-Policy-Brief.pdf

be used to document war crimes may also enable mass surveillance and the automated selection of civilian objects, as made evident in the Gaza Strip.[25]

Furthermore, algorithms and AI have error rates in target identification and classification. A report by Al Haq, published in December 2025, on the impact of the genocide and occupation on women and children, exposes the direct relationship between the generalised use of AI in the genocide and the extreme rate of civilian deaths, among which is an exponential increase of the assassination of women and children. The Gospel software[26] has doubled the number of daily military targets, normalising fire against entire residential buildings. In fact, nine out of ten women and children were inside residential buildings when they were killed, and 95% of women were executed together with their children.[27]

The data provided by United Nations agencies are clear; at the end of October 2025, it was estimated that around 70,000 people had been killed and 170,000 injured in the Gaza Strip, with displacement of approximately 90% of the population.[28] Diverse studies state that the number of assassinated people could be much higher.[29] The satellite imagery analysis by the United Nations Satellite Centre (UNOSAT) indicates that nearly 83% of infrastructure (hospitals, schools, roads, water tanks) in the Gaza Strip have been damaged or destroyed.[30]

In addition, according to data from the OCHA, since the beginning of October 2023, Palestinian infrastructure has been systematically demolished in the West Bank and East Jerusalem; a total of over 4,800 Palestinian structures have been demolished, meaning that more than 9,000 people have been displaced from their homes.[31]

25 Access Now. (2024, 10 October). *Big Tech and the risk of genocide in Gaza: What are companies doing?* https://www.accessnow.org/gaza-genocide-big-tech/

26 An artificial intelligence system used by the Israeli army to identify and prioritise large-scale targets, especially in systematic attacks on the Gaza Strip.

27 Al-Haq. (2025, 9 December). *Al-Haq comments on CEDAW Addendum regarding women in conflict*. https://www.alhaq.org/cached_uploads/download/2025/12/13/ah-comments-on-addendum-re-women-in-conflict-9-december-2025-1765658931.pdf

28 United Nations Office for the Coordination of Humanitarian Affairs – occupied Palestinian territory. (2025, 30 October). *Humanitarian Situation Update #336 | Gaza Strip*. https://www.ochaopt.org/content/humanitarian-situation-update-336-gaza-strip

29 Prost, A., Burgess, R., & Tariq, S. (2025). Gaza and the collapse of public health: A call for action. The Lancet, 406(10509), 1215–1216. https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(25)01690-3/fulltext

30 UNITAR-UNOSAT. (2025, 22 October). *Gaza Strip – Comprehensive Damage Assessment (Product 4205)* [Satellite imagery analysis]. https://unosat.org/products/4205

31 United Nations Office for the Coordination of Humanitarian Affairs – occupied Palestinian territory (OCHA oPt), *"Data on demolition and displacement in the West Bank"* https://www.ochaopt.org/data/demolition

II

The Gaza Strip as a laboratory of genocide technologies that are arriving in Europe.

The genocide against the Gaza Strip has shocked the world. The impunity with which the Palestinian population is being exterminated every day in this territory and the lack of perspectives for addressing responsibilities for these acts, has caused a global undermining of international institutions. However, this shock has not only been felt from an emotional, regulatory and humanitarian perspective, according to authors like Naomi Klein, it is also an economic shock.[32] For Klein, **severe crises create the condition to make fear and disorder 'economically profitable', privatising public services or expanding the security market.**[33] In this case, the assassination of tens of thousands is economically profitable, due to more contracts, exports and a demand for military and surveillance technologies.

Thus, behind this new colonial and extractivist phase that perpetrates a genocide without any consequences, we discover a structure of economic and political interests, not only made up of Israeli, European and North American defence tech and security companies, but also of investment funds and sub-funds that hold the shares of these companies. The activity of these companies takes place within a context of apartheid, genocide, colonialism and military occupation,[34] where big technology companies do not play a neutral role. Quite the opposite in fact, as they would be contributing towards **perpetuating an ecosystem that takes advantage of a mass violation of Palestinian's rights in order to obtain financial benefit.**

The lack of transparency in the data does not provide a clear and accurate image of the economic and financial volume generated by the Gaza genocide. However, some analyses point out that the **genocide has converted a 'surplus and unproductive' population, as a result of the Israeli occupation, into a market product**,[35] where the main attraction of the gain was the loyalty and effectiveness of the weapons used. That is, death, mass mutilation of the Palestinian population in the Gaza Strip, the destruction of its territory and subsequent reconstruction has become a new showcase for Israeli military and technological 'products', which for decades have been advertised as 'tested in combat' on the Palestinian population.

Although there are cases of companies that have lost contracts because they were publicly linked to the genocide and occupation, what is really happening is that this loss of benefit is residual with respect to the economic growth they experience.

Indeed, many companies have found new markets, fruit of the standardisation of the export and funding of the technology used in the genocide, meaning that there are still nu-

32 The shock doctrine explains how crises are used to impose neoliberal reforms, reducing social resistance through fear and uncertainty.

33 Klein, N. (2012). *La doctrina del shock*. Booket.

34 Apoorva, P. G. (2023, 24 November). *Ver el mundo como una palestina*. Transnational Institute. https://www.tni.org/es/art%C3%ADculo/ver-el-mundo-como-una-palestina

35 Kaminer, M. (2025, 1 October). Gaza and the economy of genocide. *Jacobin*. https://jacobin.com/2025/10/gaza-economy-genocide-capitalism-surplus

merous gateways to the European continent, plus the addition of even more new entry paths linked to the present context, such as the European rearmament, the enhanced relationship between Israel and Ukraine or an increase in the number of Israeli companies and their specialist staff that come to Europe.

This journey of military know-how from the State of Israel to Europe means that military and security innovation learnt in the last two years can be applied to European technology. This transfer is mainly carried out **through the creation of affiliates and subsidiaries, purchase of pre-existing European companies, supranational organisations such as NATO, research institutions and funds from Europe, states and countries with bilateral agreements with Israel or a lax regulatory framework**, from where operations can commence. In some cases, these companies have been obliged to sophisticate the process for two reasons: the extension of European Union regulations that regulate the use of these technologies and the feeling of rejection caused by their origin. Rejection that is not only territorial, but is also linked to the purpose for which the technologies were created and their use in the systematic violation of human rights.

Lastly, it is worth noting that the transfer of technology and knowledge to Europe occurs within a context of increased control, growing police violence and legal persecution against activism in support of Palestine and against the genocide in the Gaza Strip.[36] The majority of police forces in the countries where these protest actions take place operate with information extraction tools,[37] facial recognition and interception of communications developed by Israeli companies or linked to Israel,[38] such as Cellebrite, Corsight and Excem.[39] It is also the case of law enforcement agencies in Spain, as the Catalan police force [*Mossos d'Esquadra*] and the Spanish Civil Guards.[40]

Qualitatively speaking, it is worth highlighting that this technology is transforming the nation-state espionage paradigm by deploying transnational cyber espionage and repression techniques, which allow mobile device intervention, regardless of the geographical location.

---

36 Office of the United Nations High Commissioner for Human Rights. (2025). *UN experts urge Germany to halt criminalisation and police violence against Palestinian solidarity activism*. https://www.ohchr.org/en/press-releases/2025/10/un-experts-urge-germany-halt-criminalisation-and-police-violence-against

37 Borak, M. (2024, 15 January). London police deploy facial recognition during Palestine and Israel protests. *Biometric Update*. https://www.biometricupdate.com/202401/london-police-deploy-facial-recognition-during-palestine-and-israel-protests

38 Agence France-Presse. (2025, 16 October). Dozens charged under anti-terror laws in UK court over Palestine action support. *The Times of Israel*. https://www.timesofisrael.com/dozens-charged-under-anti-terror-laws-in-uk-court-over-palestine-action-support/

39 Observatori de Drets Humans i Empreses, European Network of Corporate Observatories, & Shoal Collective. (2021). *Vigilància massiva i control de la dissidència europea*. https://mass-surveillance.odhe.cat/es/

40 Latorre, E. (2025, 3 November. Monopoli israelià en l'espionatge digital dels Mossos i la Guàrdia Civil. *Directa*. https://directa.cat/monopoli-israelia-en-lespionatge-digital-dels-mossos-i-la-guardia-civil/

III

Main companies and key investors in the development and funding of the technology used for the genocide 2023.

In June 2025, the office of the United Nations Special Rapporteur on the situation of human rights in the Occupied Palestinian Territory, Francesca Albanese, published an extremely relevant report, titled 'From economy of occupation to economy of genocide', which contains a list of the main entities that have profited from the Gaza genocide and the occupation of Palestine.[41] Included in this list are public or private companies, multinational corporations, for-profit and not-for-profit entities that 'have profited from the Israeli economy of illegal occupation, apartheid and now genocide"[42] against the Occupied Palestinian Territory. The entities include US Big Tech companies, such as Microsoft, Google, IBM and Palantir Technologies, which have played a key role in the automation of the genocide. These companies have placed their technology at the service of some of the most controversial target localisation systems used to exterminate tens of thousands of people in the Gaza Strip. Appearing in the list are also companies that were identified many years ago or are included in the recently updated database that was originally published by the supranational body in 2020, as well as some of Israel's or the world's biggest armament companies, with presence in Europe through affiliates, subsidiaries and joint ventures.

However, there are many other startups and defence tech companies, or security and technological surveillance companies that either originated in Israel or were created with Israeli capital. They have benefited from contracts with the Israeli Ministry of Defence in the last two years and have provided the necessary technology for executing the genocide. In some cases, these companies had already been mentioned in reports by organisations such as Amnesty International, Who Profits, for the international Boycott, Divestment, and Sanctions (BDS) campaign in Israel, the American Friends Service Committee (AFSC) and the Observatory for Human Rights and Business in the Mediterranean (ODHE). Companies that are mentioned due to either their contribution to the manufacture of the arms, drones or software used in the Gaza Strip or because they continue to provide digital colonialism, by way of mass surveillance and control of the lives of Palestinian people in occupied territory.

1. The major companies of the military industry and security, the great beneficiaries.

The three beneficiaries of the major contracts directly related to the genocide underway in the Gaza Strip are also three of the world's largest companies in the military, defence

41 Albanese, F. (2025, July). *From economy of occupation to economy of genocide* (A/HRC/59/23). Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

42 bid.

and security industries: Elbit Systems LTD, Israel Aerospace Industries (IAI) and Rafael.[43]

Elbit Systems

Elbit Systems is an Israeli company with affiliates around Europe and is the Israeli army's largest drone supplier.[44] At the closure of 2024, the company reported profits of $6 billion and a backlog of orders for $22.6 billion, an increase of 14% compared to the previous year.[45] While until the second quarter of 2025, Elbit reported a profit of $2 billion and a backlog of orders for $23.8 billion.[46] Some of these contracts are for the MPR-500 bombs, which are capable of penetrating several layers of concrete[47], which the Israeli army is dropping on the Gaza Strip.[48]

Furthermore, in 2024, the profits from its Aerospace division grew by 9% year-over-year, largely as a result of the sales of Unmanned Aerial Vehicles (UAVs). The cyber security sector saw an increase of 11%, while the land systems grew by 29% due to ammunition and munition sales to the Israeli army.[49]

Israel Aerospace Industries (IAI)

IAI is a company owned by the State of Israel. It specialises in military avionics but has divisions in cybersecurity and critical infrastructure solutions, and police. At the beginning of 2025, IAI reported total sales of $6.1 billion in 2024 and record profits of $493 million, a year-over-year growth of 55%, plus a backlog of orders for $25 billion.[50] Internal sales to the Israeli government accounted for 34% of the profit, which grew from $1.5 billion in 2023 to $2 billion in 2024. Its participation in the genocide is linked to the sales of UAVs such as the Heron killer drones.[51,52] IAI also supplies the Israeli army with the Zibar tactical utility vehicle.

---

43 Elmas, D. S. (2025, 1 December). Israel's top 3 defense firms rise in global rankings. *Globes*. https://en.globes.co.il/en/article-israels-top-3-defense-firms-rise-in-global-rankings-1001528042

44 Hoffman, M. (2025, 17 March). War to Wall Street: IAI prepares for IPO fueled by global weapons demand. *Ynetnews*. https://www.ynetnews.com/business/article/rkw7dz831g

45 Elbit Systems. (2025, 25 March). *Elbit Systems reports fourth quarter and full year 2024 results*. https://www.elbitsystems.com/news/elbit-systems-reports-fourth-quarter-and-full-year-2024-results

46 Elbit Systems. (2025, 12 August). *Elbit Systems reports second quarter 2025 results*. https://www.elbitsystems.com/news/elbit-systems-reports-second-quarter-2025-results

47 Elbit Systems. (n.d.). *MPR 500*. https://www.elbitsystems.com/air-space/air-surface-munitions/bombs/mpr-500

48 Who Profits Research Center. (2023, 17 December). *The companies supplying weapons to Israel's attack on Gaza*. https://www.whoprofits.org/writable/uploads/publications/1704198844_be4b3465011bcea6c0a0.pdf

49 Ynet News, citation 34

50 Israel Aerospace Industries. (2025, 3 January). *IAI publishes its annual financial statements for 2024*. https://www.iai.co.il/press/iai-publishes-its-annual-financial-statements-for-2024/

51 Ynet News, citation 34

52 Israel Aerospace Industries. (2025, 18 November). *Heron Family's crucial impact on the Iron Swords War*. https://www.iai.co.il/news/iai-unmanned-aerial-dominance/

IAI is preparing for issuing bonds to investors to inject cash into Israel's economy, which is seriously affected by the offensive against the Gaza Strip, after two years of soaring public expenditure in the military industry.[53]

The company has received €2.7 million from the European Commission through eight projects,[54] in some cases awarded by a Greek company owned by them, Intracom Defense, which is currently participating in 15 European Defence Fund (EDF) projects, of which seven were awarded after this company had been sold to IAI and the genocide had started in the Gaza Strip, in October 2023. Even though Intracom Defense is registered and headquartered in Greece (and also has Greek presence on its board of directors), its financial records for 2024 show that 94.5% of the shares are owned by IAI, which, according to the Israeli company's latest records, possess 100% of the voting rights in Intracom.[55]

Rafael Advanced Defense Systems

Rafael is one of the world leaders in weapons production and is owned by the State of Israel. The Israeli army has used systems, such as the Spike missiles, manufactured by Rafael to attack people inside buildings in Gaza,[56] and different sources point out that they would have also used Matador rockets, manufactured by the German affiliate, Rafael Dynamit Nobel Defence.[57] These rockets are a short-range anti-armour weapon, highly effective against vehicle armour and brick walls.

On 1 April 2024, a Hermes 450 drone manufactured by Elbit Systems, which, according to the British newspaper, The Times, was armed with Rafael's Spike missiles,[58] attacked a three-car convoy belonging to the humanitarian organisation, World Central Kitchen, near Deir al-Balah, in the centre of the Gaza Strip, killing seven humanitarian workers. Likewise, the Orbiter 4 killer drones developed by Aeronautics, affiliate of Rafael, which would have

53 Azulay, Y. (2025). *Iron Dome developer Rafael pushes for IPO as rival IAI targets $30 billion market debut*. Calcalist. https://www.calcalistech.com/ctechnews/article/hkmgb0r00lg

54 Marsi, F. (2024, 18 December). EU research funds flow to Israel despite outrage over Gaza war. *Al Jazeera*. https://www.aljazeera.com/news/2024/12/18/eu-horizon-funding-israel

55 Investigate Europe. (2025, 11 June). *European Defence Fund millions benefiting Israeli state-owned drone manufacturer*. https://www.investigate-europe.eu/posts/european-defence-fund-millions-benefiting-israeli-state-owned-drone-manufacturer

56 American Friends Service Committee. (2023, 1 December). *Companies profiting from the Gaza genocide*. https://afsc.org/gaza-genocide-companies

57 Tielke, N. (2023, 31 October). Würgendorf: Rüstungsfirma Dynamit Nobel Defense liefert Panzerfäuste nach Israel. *Siegener Zeitung*. https://www.siegener-zeitung.de/lokales/siegerland/burbach/wuergendorf-ruenstungsfirma-dynamit-nobel-defense-liefert-panzerfaeuste-nach-israel-UXMIKBQTKZAS3E6YRLH4ZULRRE.html

58 Grylls, G. and Weiniger, G. (2024, 3 April). How Israel's 'super-accurate' Spike missiles may have killed British aid workers in Gaza. *The Times*. https://www.thetimes.com/uk/article/israel-accurate-spike-missile-killed-aid-workers-gaza-idf-rdcsmr3kx

been used in the Gaza Strip for the first time, on 8 November 2023.[59] Furthermore, Rafael collaborated with the Israeli army in the development of Spark, a new unmanned aerial system used to carry out intelligence missions, escort ground forces and direct strikes.[60] Organisations such as Campaign Against Arms Trade (CAAT) state that the Spark would have been used in the offensive against the Gaza Strip.[61]

In 2024, the company's sales reached $4.8 billion – a year-over-year growth of 27% – with a net profit of $257 million. The company's CEO fully acknowledged that the genocide in the Gaza Strip had boosted sales and orders, half of which were to provide Israel with weapons.[62]

2. The drone sector, a pie shared among many investors.

Israel is a world power in the drone industry, a pioneer in its military development since the 1960s and a leader in innovation, with numerous startups at the forefront of the civilian market. In recent years, a large number of them, mostly founded by former soldiers, have provided their technology to the Ministry of Defence, which is the case of **SpearUAV**, the manufacturer of the Viper 'suicide drone', which locates, tracks, crashes into and detonates on targets, before self-destructing. The company has acknowledged that the Gaza genocide has accelerated its development,[63] so as to meet the requirements of the Israeli army.[64]

In the same field we find **NextVision**, responsible for the development of the cameras used by the Elbit Systems drones. They were tested in the Gaza Strip during the genocide and, as a result, in August 2025, the startup lost the funding from KLP, Norway's largest

59 Walla! News. (2023, 9 November). *הזעב לועפל ולחה מישדרה מימ"מטכה :ויעידומ מיפסואו מילבחמ מיפשוה* [Exposing terrorists and collecting intelligence: new UAVs (drones) have started operating in Gaza]. https://news.walla.co.il/item/3621520

60 Breaking Defense. (2023, 12 September). *Israel's air force officially receives new, secretive Spark UAV, 'gateway' to 5th gen drones*. https://breakingdefense.com/2023/09/israels-air-force-officially-receives-new-secretive-spark-uav-gateway-to-5th-gen-drones/

61 Campaign Against Arms Trade. (2025, 7 September). *Rafael*. https://caat.org.uk/data/companies/rafael/

62 Rafael Advanced Defense Systems. (2025, 26 March). *RAFAEL reports record FY2024 results with 27% growth in sales*. https://www.rafael.co.il/news/rafael-reports-record-fy2024-results-with-27-growth-in-sales/

63 Cohen, S. (2024, 3 January). Shark tanks: With Gaza as testing ground, Israeli defense startups flourish. *Haaretz*. https://www.haaretz.com/israel-news/2024-01-03/ty-article-magazine/.premium/suicide-drones-and-ai-with-gaza-as-testing-ground-israeli-defense-startups-flourish/0000018c-cf39-ddba-abad-cfb9a3ee0000

64 Mönch Publishing Group. (2025, 24 March). *SpearUAV announces completion of a significant funding round led by Deep Insight venture fund*. https://www.spslandforces.com/news/?id=676&h=SpearUAV-Announces-Completion-of-a-Significant-Funding-Round-Led-by-Deep-Insight-Venture-Fund

pension.[65] On 10 December 2025, NextVision Stabilized Systems announced it had a market value of more than $5 billion, as well as profits of €150 million.[66]

DRS RADA Technologies, owned by Leonardo DRS, a subsidiary of the Italian defence macro-conglomerate, Leonardo, produces and delivers the radar that support the Israeli army's air surveillance and early warning capabilities.[67] This year, the company has obtained a net profit of €265 million.

Furthermore, Ben Levinson, the founder of the Israeli manufacturer of hydrogen-powered drones, **Heven Aerotech**, a subsidiary of the Indian company, Paras Defence & Space,[68] recently assured that 'A lot of companies have been working on defence stuff since October 7, but we had a facility that can produce 100 drones a month when the war broke out, which helped us become a supplier for the Israeli army'.[69]

These declarations illustrate how a company perceives the potential use of its technology in the genocide, besides reflecting the good relationship between Israel and countries such as India or the United Arab Emirates. Heven could penetrate Europe via the channels that Paras Defense already has with Germany and, in addition, it is one of the best-positioned companies to profit from the European ReArm Plan.[70]

Lastly, in this sector we find the case of **XTEND Defense**, which manufactures remotely controlled drones that can travel up to 9,000 km, which use artificial intelligence to perform precision strikes with minimum human intervention. The Israeli Ministry of Defence has recently awarded XTEND a contract worth $5.5 million to supply 5,000 first-person view drones[71] for the Israeli army.[72] The company has been named by media as the man-

65 KLP. (2025, 11 August). *KLP excludes new Israeli company*. https://www.klp.no/en/press-room/klp-excludes-new-israeli-company

66 CompaniesMarketCap. (n.d.). *Revenue for NextVision Stabilized Systems*. https://companiesmarketcap.com/nextvision-stabilized-systems/revenue/

67 Egozi, A. (2023, 6 June). DRS RADA Technologies mobile radars selected for IDF. *Defence Industry Europe*. https://defence-industry.eu/drs-rada-technologies-mobile-radars-selected-for-idf/

68 Adhikary, D. (2025, 23 May). Paras Defence shares rise 1% after firm forms JV with Israel's Heven Drones to make cargo drones in India. *Moneycontrol*. https://www.moneycontrol.com/news/business/markets/paras-defence-shares-rise-1-after-firm-forms-jv-with-israel-s-heven-drones-to-make-cargo-drones-in-india-13043513.html

69 Wrobel, S. (n.d.). Israel's Heven Drones says its hydrogen-fueled flying robots are a military game-changer. *The Times of Israel*. https://www.timesofisrael.com/israels-heven-drones-says-its-hydrogen-fueled-flying-robots-are-a-military-game-changer/

70 Vaishnav, A. (2025, 6 March). Paras Defence, BEL, HAL and more: 9 Indian companies that could benefit from Europe ramping up defence budgets. *CNBCTV18*. https://www.cnbctv18.com/market/defence-stocks-paras-defence-hal-bel-bharat-dynamics-data-patterns-solar-industries-european-union-spending-plan-19569885.htm

71 XTEND. (n.d.). *Warfare has changed forever* [Video]. https://vimeo.com/1100413074

72 SOFX. (2025, 22 August). *Israel orders 5,000 XTEND FPV drones for IDF ground forces*. https://www.sofx.com/israel-orders-5000-XTEND-fpv-drones-for-idf-ground-forces/

ufacturer of the drone that tracked and filmed the operation that killed Hamas leader, Yahya Sinwar.[73] The company was created in 2018 by Aviv Shapira, Matteo Shapira and Rubi Liana. According to its CEO 'it can recognise and follow a target with lethal precision'.[74] In August 2025, the Israeli Ministry of Defence announced that XTEND had won a tender, worth millions of dollars, to supply its technology to the Israeli army's ground forces.[75] In an article published in the New York Times, they acknowledged their use in the Gaza Strip.76 In 2025, the company doubled its revenue of 2024, achieving an annual turnover of tens of millions of dollars.[77]

3. Spyware, robotics, facial recognition and other sectors.

The most important spyware company, mentioned frequently in this report, is **NSO Group**, the manufacturer of the well-known Pegasus spyware. It was the first company capable of developing espionage technology with unprecedented properties, such as remote access and total control over the content of a mobile device, without the owner's knowledge or permission; technology that the company has stressed that it directly originated from Israeli military experience.

From 2010 until the present day, the company has operated under an ambiguous regulation that has enabled it to carry out a disproportionate and systematic surveillance of tens of thousands of people around the world.[78] **NSO has appeared in numerous independent reports and investigations[79] due to having provided surveillance technology to governments and intelligence agencies that has subsequently been used to spy on journalists, lawyers, dissidents and human rights activists.** In Spain up to a dozen criminal

73 Noticias de Israel. (2025, 31 January). *Startups israelíes se expanden globalmente tras su rol en Gaza*. https://israelnoticias.com/economia/startups-israelies-se-expanden-globalmente-tras-su-rol-en-gaza/

74 The New York Times. (2025, 25 April). Israel's A.I. experiments in Gaza war raise ethical concerns. *The New York Times*. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html

75 Israel Ministry of Defence [Israel MOD]. (2025). *Israel MOD to procure thousands of drones from XTEND worth millions of dollars* [LinkedIn publication]. LinkedIn. https://www.linkedin.com/posts/israel-mod-to-procure-thousands-of-drones-share-7363873945214693377-nQt9/

76 The New York Times. (2025, 25 April). Israel's A.I. experiments in Gaza war raise ethical concerns. *The New York Times*. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html

77 Shahaf, T. (2025, 11 December). Israeli firm XTEND, whose drones reportedly killed Sinwar, wins major US defense deal. *Ynetnews*. https://www.ynetnews.com/business/article/bkcdsowgzl

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

79 Amnesty International. (2021, 18 July). *Forensic methodology report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

complaints have been filed for illegal espionage with Pegasus; one of which has become the first complaint by a victim who has succeeded in triggering the legal investigation of three senior managers of NSO Group in Israel and Luxembourg.[80]

After 25 years, the company has grown and established itself as a symbol of Israel's offensive cyber industry. Pegasus, its spyware, is marketed as a defence technology 'made in Israel' and has been promoted as a foreign policy tool to strengthen diplomatic relations.[81] Investigations show a direct correlation between the visits from heads of state to Israel and the authorisation of new licences to export Pegasus, a pattern observed in both diplomatic normalisation processes and international negotiations, including voting at the United Nations.[82]

Since October 2023, NSO Group has volunteered to collaborate with its technology in the mission to locate Israeli hostages.[83] Indeed, **NSO Group initiated a process to update its military surveillance technology so it could be used during the current genocide against the Gaza Strip.**

Following its trail, one of the latest incorporations into the market that has appeared as a result of the genocide is **Dream Security**, founded in November 2023 by one of the original owners of NSO Group, Shalev Hulio, together with Sebastian Kurz, ex-chancellor of Austria, and Gil Dolev, former leader of Wayout Group.[84] Dream has developed an AI-based platform to anticipate cyberattacks and prevent security breaches, which Hulio, dressed as a soldier, announced to the public from the Gaza Strip.[85]

Corsight AI is the developer of the facial recognition technology installed in the cameras with which the Israeli army permanently surveils and scans the faces of the Palestinian population in the Gaza Strip,[86] especially at the checkpoints set up along the routes used by civilian Palestine people to escape from bombings. The company, with

80 Irídia — Center for the defense of human rights (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/

81 The New York Times Magazine. (2022, 28 January). The battle for the world's most powerful cyberweapon. *The New York Times*. https://www.nytimes.com/2022/01/28/world/middleeast/israel-pegasus-spyware.html

82 Haaretz. (2022, 28 January). *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

83 Haaretz. (2023, 19 October). *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

84 Aleph. (n.d.). *Shalev Hulio & Sebastian Kurz* (No. 50) [Audio podcast]. https://www.aleph.vc/content/shalev-hulio-sebastian-kurz

85 Gee, G. (2024, 18 January). In video from Gaza, former CEO of Pegasus spyware firm announces millions for new venture. *The Intercept*. https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/

86 Who Profits. (n.d.). *Corsight AI*. https://www.whoprofits.org/companies/company/7383?corsight-ai

offices in the United States and the United Kingdom, possesses subsidiary companies in Israel. In Europe it has presence in Portugal and supplies technology to Switzerland. Corsight is owned by the Israeli company, Cortica, and the Canadian venture capital firm, Awz Ventures.[87]

In the tactical equipment sector, **Agilite** is an Israeli company founded by former soldiers from Israel and the US, which manufactures tactical gear and bulletproof vests used by the Israeli army. Since October 7, 2023, Agilite has repeatedly advertised the use of its equipment by the Israeli military in its ground invasion of Gaza.[88] One of the slogans on its products is 'As Israelis, we've always had to innovate to survive, in order to protect our families and our homeland. Our gear has always had to stay one step ahead of our enemies.'[89]

We must not leave out **Cellebrite DI Ltd**, a software developer based in Israel, specialised in information extraction tools.[90] Its star product is the Universal Forensic Extraction Device (UFED), which unlocks mobiles and other devices, bypassing the devices' encryption and passwords. According to the American Friends Service Committee (AFSC) – citing an article by the Haaretz – during the attacks in the Gaza Strip Israel has used Cellebrite tools to collect data from the telephones of thousands of Palestinians who were captured and kidnapped from Gaza.[91] I would also appear that Cellebrite received funding from a Pentagon innovation unit to develop a product to map underground tunnels in the Gaza Strip.[92] At the same time, this technology has recently been used to obtain data from phones owned by pro-Palestinian activists in countries like Jordan.[93]

In July 2025, the Spanish Ministry of the Interior renewed its collaboration with this company, which supplies technology to different Spanish law enforcement agencies.[94]

87 Awz Ventures. "Our portfolio" https://www.awzventures.com/our-portfolio

88 Agilite. (2024, 11 October). *Underground warfare: Inside Gaza terror tunnels* [Video]. YouTube. https://www.youtube.com/watch?v=kliRb2Mh500

89 Agilite Europe. (n.d.). *About us*. https://agiliteinternational.com/pages/about-us

90 Cellebrite. (n.d.). UFED. https://cellebrite.com/en/products/physical-analyzer/

91 American Friends Service Committee. (n.d.). *Cellebrite DI Ltd*. Investigate. https://investigate.afsc.org/company/cellebrite-di

92 Shulman, S. (2024, 15 August). The biggest global VCs are secretly battling over Israeli defense-tech startups. *CTech*. https://www.calcalist.co.il/ctechnews/article/nphse8l7g

93 OCCRP. (2026, 22 January). *Jordan used Israeli tech to crack phones of Gaza war protesters: Report*. https://www.occrp.org/en/news/jordan-used-israeli-tech-to-crack-phones-of-gaza-war-protestors-report

94 Frías, C. (2025, 23 April). Interior compra un programa policial de Israel en plena polémica por la munición de la Guardia Civil. *El Independiente*. https://www.elindependiente.com/espana/2025/04/24/interior-compra-un-programa-policial-de-israel-en-plena-polemica-por-la-municion-de-la-guardia-civil/

4.Genocide as a financial product.

The companies that produce the technology used in the genocide and exported to Europe are not the only actors to benefit from this situation of extreme violation of international law. **The genocide in the Gaza Strip has turned into a profitable business opportunity for financial capitalism**. International investment funds and companies, as well as risk capital initiatives, invest in the Israeli startup and tech company ecosystem, providing capital in exchange for company shares, with the hope of maximising return on investment if the business is successful. Whether as shareholders of Israel's main defence and security technology companies or financing the Israeli investment funds that feed on the capital of these companies, there is a global financial structure ready to distribute the potential financial profits created by the shock and war economy in which Israel is immersed. However, as suggested by an article published in El Salto, 'an in-depth study was still required of the financial networks that were operating as capital investors or managers[95] of the profits obtained from the genocide.

One of the most illustrative cases is Elbit Systems. In 2024, it distributed **$89 million in dividends among its main shareholders**,[96] which included Israeli investment funds such as **Clal Insurance Enterprises** and **Altshuler Shaham**, and the **American The Vanguard Group** (the world's largest investment firm), 1**832 Asset Management L.P.**, **Morgan Stanley and Goldman Sachs.**[97] The Vanguard Group is also a shareholder of Clal Insurance, as well as other international financial funds, such as the British **Phoenix Group.**[98] This means that Vanguard Group not only obtains profits directly from Elbit as one of its shareholders, but also indirectly, by investing in the Israeli financial funds that enable Israeli defence tech companies to continue operating.

Another representative case is Cellebrite, whose shareholders include Morgan Stanley and BlackRock, the world's largest asset manager, as well as the funds from **Sun Corporation** in Japan, and **True Wind Capital Management** and **Axon Enterprise** in the United States.[99]

As regards startup funding, two representative cases are Corsight and Dream Security.

---

95 Fernández, L. T. and Anred. (2025, 16 August). El lucro del genocidio: los países de la UE ponen la logística, Estados Unidos las armas. *El Salto Diario*. https://www.elsaltodiario.com/analisis/empresas-norte-global-genocidio-gaza

96 Elbit Systems. (2025, 25 March). *Elbit Systems reports fourth quarter and full year 2024 results*. https://www.elbitsystems.com/news/elbit-systems-reports-fourth-quarter-and-full-year-2024-results

97 MarketScreener. (n.d.). *Elbit Systems Ltd. (ESLT)*. https://www.marketscreener.com/quote/stock/ELBIT-SYSTEMS-LTD-6497555/company/

98 Investing.com. (n.d.). *Clal Insurance Enterprises Holdings Ltd (CLIS)*. https://www.investing.com/equities/clal-insurance-ownership

99 MarketScreener. (2025, 20 December). *Cellebrite DI Ltd.: Shareholders board members managers and company profile*. https://www.marketscreener.com/quote/stock/CELLEBRITE-DI-LTD-126371088/company/

In the case of Corsight, its largest investor is **Awz Ventures**, a Canadian venture capital firm that has an agreement with the Israeli Ministry of Defence to fund the development of AI-based technologies in the country's security industry.

XTEND Defense is financed by Israeli **Protego Ventures** and **ClalTech**, the investing arm of Clal Industries and Technologies which, at the same time, is owner of the United States global investment firm, **Access Industries**.[100] In July 2025, the company initiated a new funding round to raise $30 million. Among the companies participating were U**nion Tech Ventures** – the investment arm of Union Group, an Israeli holding company – **Chartered Group** – a Singapore-based investment firm – and the American **Aliya Capital Partners**, based in Miami, and **Enkore International**.[101] **XTEND's main investor, Protego Ventures, created by the Israeli reservist soldiers, Lital Leshem and Lee Moser**, brags about being 'Israel's only venture capital fund, led by women, to focus exclusively on investing in military equipment and software after the attacks on 7 October'.[102] Since then, **they have secured $100 million for defence tech companies.**

In the case owned by the State of Israel, such as IAI and Rafael, financial intervention has been via the so-called 'Israel bonds', direct loans to the state that have increased significantly since October 2023. They were specifically issued to cover the costs of its war economy, and were advertised as opportunities to support 'Israel at war'.[103] In January 2025, Israel issued these bonds for a value of $19.4 million. Research by Profundo, BankTrack and Pax has revealed that **since 7 October 2023, Goldman Sachs has underwritten over $7 billion in Israeli 'war bonds'. The other financial institutions identified in this research as bond underwriters are the Bank of America, Deutsche Bank, BNP Paribas, Citi, Barclays and JPMorgan Chase.**[104] These loans by international financial institutions will have played a crucial role in the offensive against the Gaza Strip'.[105]

100 ClalTech. (n.d.). *About us*. https://claltech.com/about/

101 PitchBook. (n.d.). *XTEND Defense*. https://pitchbook.com/profiles/company/266230-09#signals

102 Shulman, S. (2024, 10 December). Defense tech VC Protego raises $70M in just two weeks, sets sights on $200M. *Calcalist Tech*. https://www.calcalistech.com/ctechnews/article/bymundbn1x

103 Israel Bonds. (n.d.). *Israel at war*.

104 BankTrack, PAX i Profundo. (2025, 14 February). *Seven underwriters of 'war bonds' instrumental in enabling Israel's assault on Gaza, new research finds*. https://www.banktrack.org/news/seven_underwriters_of_war_bonds_instrumental_in_enabling_israel_s_assault_on_gaza_new_research_finds

105 Follow the Money. (2025, 6 October). *This is how Western banks and insurers finance Israel's war on Gaza*. https://www.ftm.eu/articles/israel-gaza-war-funding-western-banks-insurers

IV

Structural factors of the Israeli business penetration in Europe.

In recent years, numerous **Israeli companies of the defence, cybersecurity and dual-use technology industries have directed their expansion towards the European market**. This strategy responds to a combination of economic, technological, political and regulatory factors. Their implementation in the continent enables them to access new markets, funding sources and talent, while boosting their business reputation and 'hiding' their involvement in the genocide against Palestine.

By establishing themselves in Europe, these companies are offered a direct proximity to strategic institutional customers: government, armed forces, security agencies and EU and NATO institutions. The continent's rearmament with plans like ReArm Europe, which rapidly increase public and private funds for security and the defence industry, represent a potential market of great interest for forthcoming years. This political initiative is reflected in the Multiannual Financial Framework (MFF) — a seven-year framework that sets the EU's spending limits — with a fivefold increase of the budget for defence between 2021–2027 and 2028–2034.[106]

In this regard, territorial presence within the European Union facilitates participation in public tenders, access to research and development (R&D) projects or technology cooperation initiatives that would be much more difficult to obtain from Israel. Even more important is that **having a registered office in a Member State enables them to freely operate within the European single market, without internal barriers or administrative restrictions.** In these cases, companies may directly present themselves as startups or 'European' suppliers of advanced technology, thus diluting the image associated to the origin or military use of their products. A similar mechanism is the participation of research centres and Israeli companies in European research and innovation programmes, on occasions under new brands or through the purchase of directly European companies, as we will see in the case of Intracom Defense and IAI.

As an example, the record achieved in 2024 by Israel's defence exports, which reached a value of approximately $14.7 billion, is heavily linked to the decision to access the European market with greater strength.[107] **Fifty-four percent of the contracts signed in 2024, which helped achieve this record, were with European countries.**[108] Europe is consolidated as Israel's main export market in the defence industry, not just due to the volume of

106 European Union. (2000, 21 June). *Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the State of Israel, of the other part*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/06a73675-d5d4-11f0-8da2-01aa75ed71a1

107 Frantzman, S. J. (2025, 4 June). Israeli defense exports hit record $14.7 billion, despite regional conflicts. *Breaking Defense*. https://breakingdefense.com/2025/06/israeli-defense-exports-hit-record-14-7-billion-despite-regional-conflicts/

108 Ibid.

contracts, but also its strategic relevance, to the point it may be considered a key actor in the sustainability and expansion of the Israeli defence industrial ecosystem.[109]

Using intermediaries is another common tactic. Instead of directly operating under the Israeli brand, **companies turn to local consultants or technology integrators that market services and products under another business identity**. Not only do these mechanisms make it difficult to trace back to the parent company, they also make it easier to access contracts from public-sector bodies that, otherwise, could reject the collaboration due to their link to the genocide of the Palestinian population. At geostrategic scale, by opening affiliates in Europe the State of Israel can reduce its traditional dependence on the North American market and position itself within a more diversified regulatory environment.

In a nutshell, for Israeli defence and cybersecurity companies the different European countries make up an attractive environment for expansion, since they provide direct access to institutional customers, R&D funding and qualified human capital. These Israeli companies are also provided with the opportunity to improve their international reputation, while taking advantage of the links to insert themselves into European innovation projects and present themselves as pioneer cybersecurity startups, thus diluting their background and track record as regards the use of their technologies in the systematic violation of human rights.

1. Offshoring, specialists and Israeli capital heading towards the continent.

The conflict escalation in the region, including the strikes initiated by Israel and the United States on Iran, have caused a gradual exodus of Israeli citizens to other parts of the world. According to official sources, i**n 2024, 82,700 people originally from the State of Israel abandoned the country.**[110] **Europe is one of the main destinations of this migration and, within Europe, Germany** is the country that has received the highest number of Israelis in recent years. [111]

These human movements also involve the transfer of capital and Israeli companies to Europe. One of the main industries that is moving its operations and investment is the technology sector, a factor aligned with the fact that Israel is one of the countries with the

109 Campaign Against Arms Trade. (2025, 7 December). *Israel's arms industry & its links with the UK*. https://caat.org.uk/data/countries/israel/israels-arms-industry-its-links-with-the-uk/

110 The Jerusalem Post. (2025, 30 January). *Multi-front war caused emigration from Israel, Knesset report says*. https://www.jpost.com/israel-news/article-840501

111 OECD. (2024, 14 November). *International migration outlook 2024: Israel*. OECD Publishing. https://www.oecd.org/en/publications/international-migration-outlook-2024_50b0353e-en/full-report/israel_846cf927.html

most startups and innovation projects in the world. According to records, back in 2021, 912 Israeli tech companies moved to Europe, mostly from the IT (information technology) and software sector, with Germany, Netherlands, France, United Kingdom and Spain as the most popular destinations.[112] Some sources also indicated Cyprus, especially the coast of Limassol, as one of the preferred destinations for the Israeli business migration.[113] A recent report from the Israel Innovation Authority, reveals that **one in five Israeli tech firms has moved its operations abroad since the start of the genocide**.[114] The report also identifies that 50% of Israeli startups could run out of funds in six months, due to the difficulty to obtain capital from Israel. The cancellation of flights, disruptions of industrial operations, mobilisation of reservists and the unwillingness to invest foreign capital in Israel are some of the reasons that force Israeli companies to move abroad, so they may continue their activities and obtain funds.[115]

This situation is also leading to a 'brain drain'; that is, the emigration of experts in the Israeli tech sector.[116] **The Israeli Innovation Authority discovered that 8,300 specialist workers in the high tech sector left the country between October 2023 and July 2024**.[117] Many of these professionals come from large technology companies like Google or Intel and are relocated to these companies international offices. At the same time, European technology hubs act as a pole of attraction to access new career opportunities. Of notable importance are the hubs of Paris, London, Munich, Tallinn, Stockholm, Amsterdam, Vilnius and Barcelona, among others.

2. European Regulatory Framework.

The reason Israeli cybersecurity companies are attracted to Europe is partly due to the characteristics of the EU's legal and regulatory framework. On the one hand, it is characterised by the **growing deregulation, lack of accountability and inconsistencies between**

112 EIT Health. (2021, April). *Israeli tech companies in Europe: Map & report*. https://eithealth.eu/wp-content/uploads/2021/04/Israeli-Tech-Companies-in-Europe-Map-Report.pdf

113 Burke, S. (2024, 27 November). Israeli tech entrepreneurs and engineers from Google, Microsoft are seeking refuge in Europe. *Fortune*. https://fortune.com/europe/2024/11/27/israeli-tech-entrepreneurs-engineers-google-microsoft-are-seeking-refuge-in-europe

114 Wrobel, S. (2025, January). *One in five Israeli tech firms moved some operations and staff abroad during war*. The Times of Israel. https://www.timesofisrael.com/one-in-five-israeli-tech-firms-moved-some-operations-and-staff-abroad-during-war/

115 Ibid

116 Burke, J. (2025, 17 March). *Israelis moving to live in Europe 'rejuvenating' Jewish communities*. The Guardian. https://www.theguardian.com/world/2025/mar/17/israelis-moving-live-europe-rejuvenating-jewish-communities

117 Israel Innovation Authority. (2025, 7 April). *2025 High-tech employment status report*. https://innovationisrael.org.il/en/press_release/2025-high-tech-employment-status-report/

different jurisdictions. On the other, the EU offers legal security and lax regulatory guidelines that protect the companies' interests and profits. All together under a rhetorical claim to defend rights and protect consumers.

Although the EU assures that it is establishing business relationships of equality with countries in the Global South and is working to achieve sustainable development, it is actually applying a policy of double standards: while the **European regulatory framework prohibits technology systems that are used in disregard of human rights within the EU**, this same legal framework allows European companies to benefit from the sales outside the EU of products considered to pose an unacceptable risk, according the European regulations.[118]

The EU is also legally obliged to guarantee that its policies, including industrial and business policies, do not contribute towards human rights violation outside its territory. However, **allowing the export of surveillance technology that is banned within the EU infringes this obligation and consolidates a structural inconsistency of policies that are contrary to its own human rights commitments**.[119]

3. Control of a securitisation narrative.

Despite the high risk of abuse and serious threats that intrusive surveillance technologies represent for fundamental rights, as well as the long track record of complaints and public scrutiny that accompany them, when it is verified that **there is still no adequate and solid legal framework regulating their use, neither international nor national, it is quite worrying**. Regardless of the advocacy of civilians to effectively guarantee fundamental rights and freedoms, a high number of regulatory instruments – as will be mentioned in specific cases below – are non-binding proposals or are insufficient, characterised by notable exclusions in their articles.

At a time when the surveillance market is proliferating,[120] a consistent regulatory framework is more necessary than ever, to set the limits and apply sufficient accountability and control mechanisms. The existing lack of protection allows the private sector to operate within an ambiguous legal space, marked by the lack of transparency and recurring alliances with the military field (like the case of Israel, with companies such as NSO Group

118 Amnesty International and European Digital Rights. (2023). *Toxic double standards: How Europe sells products deemed too dangerous for Europeans to the rest of the world* (Joint briefing 13). https://www.amnesty.eu/news/toxic-double-standards-how-europe-sells-products-deemed-too-dangerous-for-europeans-to-the-rest-of-the-world-joint-briefing/

119 Loreti, V. (2020). *Human rights at the borders of Europe* [Master's dissertation, LUISS Guido Carli / Université de Liège]. LUISS Thesis Repository. https://tesi.luiss.it/34893/1/644822_LORETI_VALERIO.pdf

120 European Digital Rights. (2025, June). *Spyware and state abuse: The case for an EU-wide ban* (Position paper). https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf

and Paragon). A close connection is thus identified between security policy logic, and the creation and maintenance of a regulatory framework where, in practice, human rights and their protection are subordinated to the interests of business profit.

The rise in securitisation narratives in the EU is based on building the idea of a 'lack of security' and the existence of a 'foreign danger' from which we need to be protected. This tale has crystallised in legislative instruments like the EU Artificial Intelligence Act, in which securitisation also implies legal exceptions. In this way, the areas of police and border guards (and, therefore, their operating authorities) are exempt from the main control, transparency and supervision mechanisms established by law.[121] **This regime of exceptionality helps to consolidate an institutional culture of surveillance and criminalisation, in which the notion of 'national security' prevails over the protection of fundamental rights.**

4. Deregulation: neglecting rights for the sake of 'competitiveness'.

In recent years, there has been a growing deregulation trend in the EU that seeks to dismantle the rules for companies that operate in its territory. In the technology field, to supposedly 'simplify procedures' and 'boost the European block's competitiveness', this agenda seeks to release the private sector from obligations and progressively erode the systems that protect civilians from the risks of technology systems, including intrusive surveillance protection.[122]

The defence tech industry's penetration into EU countries in general, but also including Israel, benefits from a **regulatory double standard that combines, on the one hand, advanced discourses on fundamental rights and, on the other, security, rearmament and interoperability policies that prioritise military and police effectiveness.** This imbalance has been widely documented in the critical analysis of European securitisation, which clearly shows how security turns into the main guiding principle capable of suspending legal and ethical guarantees.[123]

121 European Center for Not-for-Profit Law. (2024, August). *AI Act: Enforcement – A civil society perspective*. https://europeanaifund.org/wp-content/uploads/2024/09/240827_FINAL_AI_ACT_Enforcement.pdf

122 European Digital Rights. (2025, November). The EU must uphold hard-won protections for digital human rights. https://edri.org/wp-content/uploads/2025/11/The-EU-must-uphold-hard-won-protections-for-digital-human-rights.pdf

123 Bigo, D. (2014). The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts. *Security Dialogue*, *45*(3), 209–225. https://doi.org/10.1177/0967010614530459

On 19 November 2025, the European Commission presented the D**igital Omnibus Regulation Proposal** that,[124] if approved, would provide the possibility to reopen and amend the General Data Protection Regulation, ePrivacy Directive, AI Act, Digital Services Act (DSA), Digital Markets Act (DMA) or Corporate Sustainability Due Diligence Directive (CSDDD). At the time of writing this report, the process was still at an initial negotiation stage due to its controversial content.

In the same way as over 470 civil society organisations around the world have reported,125 this wave of unprecedented deregulation is being negotiated without the pertinent assessment measures, excluding the civil society and giving in to business actors that seek to lower the standards of social, environmental, employment and human rights for their own benefit.

Both the security drift and the legislative deregulation clearly show the willingness to strengthen the private sector and endow it with public resources, with direct consequences for the democratic quality of the EU and its Member States. This trend does not only affect regulations in force, it also subjects any new legislative proposal to a 'competitiveness' check.[126]

5. European legal framework applicable to intrusive surveillance technologies.

In the EU, the application of digital technology with an impact on fundamental rights fits within a set of legal instruments that seek to establish the basic principles of human rights protection, privacy and democratic guarantees. This architecture is based on the **European Convention on Human Rights and the Charter of Fundamental Rights of the European Union** and, on paper, it establishes principles such as human dignity, personal data protection, necessity and proportionality, equality and non-discrimination, and the right to an effective remedy. In recent years, this architecture has expanded with the adoption of new sectoral instruments applicable in specific areas.

However, it is important to point out that this regulatory framework coexists with contracting and cooperation practices that make it easier to incorporate technology devel-

124 European Commission. (2025). *Proposal for a Regulation of the European Parliament and of the Council on the digital omnibus regulation*.
https://digital-strategy.ec.europa.eu/es/library/digital-omnibus-regulation-proposal

125 European Digital Rights. (2025). *The EU must uphold hard-won protections for digital human rights*.
https://edri.org/wp-content/uploads/2025/11/The-EU-must-uphold-hard-won-protections-for-digital-human-rights.pdf

126 European Commission. (2024). *Competitiveness*.
https://commission.europa.eu/priorities-2024-2029/competitiveness_en

oped in contexts of occupation, apartheid and genocide, often under the 'dual-use' category. From an antiracist perspective, this process implies the risk of transferring colonial logics of surveillance and control to European policies on borders, public order and protest management, and social unrest. As David Lyon warns, contemporary surveillance is not neutral; people and populations tend to be classified and governed differently, reinforcing exclusion and stigmatisation processes.[127]

By way of illustration, below are some of the main legislative instruments that regulate the use of intrusive surveillance technologies: [128]

- **Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021[129] setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.** Since its first formulation in 1994, this Regulation has aimed to control the transfer of goods and technologies that can be used for both civil and military applications. The 2021 update included significant advances, among which is the noteworthy incorporation of a catch-all mechanism used to control certain exports that do not figure expressly on the lists of products regulated in the annexes of the Regulation, when there is a clear risk that these items could contribute towards seriously violating human rights or international humanitarian law. However, there are still numerous limitations, such as:
    - Definitions with grey areas that give rise to discretional interpretations.
    - Excessive dependency on the good faith of exporters and their internal programmes in regard to the rules.
    - Member States have unequal capacity for the supervision of this Regulation, depending on the political will, internal rules, international weight.
    - Different levels of applicability, which generate substantial differences within the European market.

  In view of the increased marketing of surveillance technologies, in 2024 the European Commission published specific guidelines on the application of Regulation (EU) 2021/821[130] on the export of cyber-surveillance items. This document formally inter-

127 Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

128 In Europe, the following definitions apply: Regulations are binding legislative acts instruments that must be applied in their entirety in all Member States, without the need for a national act (or transposition. They apply to both the Member States and individuals (companies, public authorities, citizens). Directives are binding as regards the established goals, although they are not applied directly; each Member State is obliged to transpose them into their own legal systems.

129 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. (2021). *Official Journal of the European Union*, L 206/1. http://data.europa.eu/eli/reg/2021/821/oj

130 European Commission. (2024, 16 October). *Commission publishes guidelines for cyber-surveillance exporters*.

prets that the list of dual-use items also applies to categories like intrusion software, forensic tools or communication monitoring programmes, including commercial spyware. Notwithstanding this, the same guidelines acknowledges its incapacity to address the growing proliferation of commercial software, given the lack of an effective inspection system, the lack of transparency in exports and the persistence of legal loopholes that mean they can be produced and distributed from the EU, which has already become one of the market's most important global hubs.[131]

- **As regards export controls for conventional arms and other dual-use goods, the European regulation is partly based on international instruments, such as the 1999 Wassenaar Arrangement[132] and Council of Europe Convention No. 108 on data protection.**[133] The Wassenaar Arrangement establishes control lists for the transfer of conventional arms and dual-use goods that make up the basis of the European regulatory framework. However, its non-binding nature and the absence of coercive mechanisms have seriously limited its effectiveness. After remaining unchanged for decades, it is now considered to be an obsolete and ineffective instrument to approach today's technological reality.[134] While Council of Europe Convention No. 108 on data protection is the first internationally binding data protection tool. The rule sets forth that any transfer of personal data to third-party countries shall incorporate appropriate safeguards to protect human rights. However, the lack of strong coercive mechanisms (Member States that fail to comply are not sanctioned), the lack of technical standards for highly intrusive technologies, as well as a State's dependency on the application, mean that the tool is insufficient for regulating the current risks of surveillance technologies.

- **The General Data Protection Regulation (GDPR)[135] is a global standard as regards data protection** and establishes legal principles and barriers for the collection and processing of personal information. It considers biometric data (facial features, iris, fingerprints, voice characteristics, patterns of blood vessels, among others) to be especially sensitive and consequently prohibits public and private actors to collect and use them, with some exceptions.[136] Along these lines, since 2018 it has been manda-

131 Commission Recommendation (EU) 2024/214, of 15 January 2024, on the application of Regulation (EU) 2021/821 as regards Cyber-surveillance items. (2024). Official Journal of the European Union, L 2024/214. http://data.europa.eu/eli/reco/2024/214/oj

132 The Wassenaar Arrangement. (2026). *The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies*. https://www.wassenaar.org/

133 European Council. (1981, 28 January). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (European Treaty Series - No. 108). https://rm.coe.int/1680078b37

134 The Intercept. (2023, 10 November). *Israel put NSO Group on a blacklist – Then used its spyware in Gaza*. https://theintercept.com/2023/11/10/nso-group-israel-gaza-blacklist/

135 European Commission. (2022, 28 October). Personal data protection (applicable since 2018). https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

136 European Digital Rights. (2020). *Ban biometric mass surveillance* (Position paper). https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

tory to assess the impact on data protection, as well as establish mitigation and protection measures in cases that could represent a risk for rights and freedoms, such as in the application of profiling or mass monitoring in public or private spaces (like facial recognition systems).[137]

All companies that operate in the European market, even if they are based outside the EU, must guarantee strict compliance with its requirements. This requires robust technology systems to ensure privacy, access control, traceability and response against security gaps. Consequently, the GDPR has fostered an extensive market for advanced technological solutions, especially as regards encryption, data management and preventive cybersecurity.

Even though it is one of the most robust regulatory frameworks for surveillance technology protection, the digital rights organisation, **EDRi, warns that its implementation has not been uniform or effective in all Member States; that State data protection agencies do not have sufficient resources to meet the Regulation's requirements** and that, in practice, the application provides a limited guarantee at State level.[138]

Apart from finding ourselves under the aforementioned risk and pression of the EU's legislative 'simplification', which could weaken some of the few legal mechanisms that allow the civil society to challenge abuse from governments and companies,[139] the GDPR was not designed to regulate AI-based surveillance systems. For this reason, it does not include specific rules in this field and leaves data protection gaps that should be covered by the AI Act.

- **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data used by police and criminal justice authorities**[140] entered into effect together with and supplementing the GDPR, and follows the same data protection principles as a fundamental right. Fully applicable since 2018, the Directive establishes the personal data protection rules to be followed by

137 Lafede.cat, IA Ciudadana, and Algorace. (2024). *Automatización del control y vigilancia biométrica en el espacio público: Un análisis desde los derechos y las resistencias*. https://www.lafede.cat/wp-content/uploads/2026/01/CAST-Automatizacion-del-control-y-vigilancia-biometrica-en-el-espacio-publico.-Un-analisis-desde-los-derechos-y-las-resistencias.-1.pdf

138 European Digital Rights. (2020). *Ban biometric mass surveillance* (Position paper). https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

139 European Digital Rights. (2025, November). *The EU must uphold hard-won protections for digital human rights*. https://edri.org/wp-content/uploads/2025/11/The-EU-must-uphold-hard-won-protections-for-digital-human-rights.pdf

140 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (2016). *Official Journal of the European Union*, L 119/89. http://data.europa.eu/eli/dir/2016/680/oj

authorities responsible for obeying the law in criminal proceedings carried out for law enforcement purposes (prevention, detection or prosecution of crimes).[141] Therefore, this is a special regime for police authorities that, unlike the GDPR, is not based on consent but likewise stipulates that data must be processed in accordance with criteria of strict necessity. Like in the GDPR, there is a long list of safeguards and guarantees for especially sensitive data (including biometric data) and mass, indiscriminate processing of civilians' data is prohibited.[142]

As the EDRi warns, although the Directive stipulates that the processing of police data requires very solid justification, in practice the guarantees are not effectively met and there is a serious lack of transparency and control mechanisms. At the same time, the Directive is not applied harmoniously in all Member States, and overlapping between the GDPR and the Directive on the protection of personal data used by police and criminal justice authorities means that there are ambiguities and grey areas that enable the use of legal loopholes to justify the application of surveillance technologies.[143]

- **The European AI Act[144] is the EU's first binding and specific artificial intelligence instrument and is linked to the GDPR as regards personal data treatment and processing**. In force since August 2024, it is being gradually deployed until reaching the end of the implementation period in August 2026, when it must be fully applied (albeit growing pressure from the same European institutions to suspend or delay its implementation, and as part of the deregulation agenda).

  The Act classifies AI systems into four risk categories: unacceptable, high, limited and minimum; according to which, specific obligations are set for providers and developers, respectively.[145] **Although intrusive surveillance technologies are classified as an unacceptable or very high risk, the Act allows the EU to develop and export AI systems that are prohibited due to their incompatibility with human rights**, as documented in the sale of facial recognition technologies to Israel.[146] In the EU, the regulation prohibits systems classified as unacceptable risk, which prevents their

141 European Digital Rights. (2020, May). *Ban biometric mass surveillance* (Position paper). https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

142 Ibid.

143 Ibid.

144 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). (2024). *Official Journal of the European Union*, L 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

145 European Center for Not-for-Profit Law. (2024). Towards an AI Act that serves people and society: Strategic actions for philanthropy and civil society on the enforcement of the EU AI Act. European AI & Society Fund. https://ecnl.org/sites/default/files/2024-09/AIFUND_ECNL_AI_ACT_Enforcement_2024.pdf

146 Amnesty International and European Digital Rights. (2023). *Toxic double standards: How the EU's exports of surveillance technology are damaging human rights abroad*. https://www.amnesty.eu/news/toxic-double-standards-how-europe-sells-products-deemed-too-dangerous-for-europeans-to-the-rest-of-the-world-joint-briefing/

development and sale within the EU. These systems include, for example: social scoring, citizen manipulation or emotion recognition systems in the fields of education or employment, among others.[147]

However, as warned by the coalition of organisations IA Ciudadana, the numerous exceptions and gaps in the prohibitions (especially in the criminal, police and migration fields) enable the application of mass and discriminatory surveillance technologies that pose a serious risk for human rights, such as:

- Real-time facial recognition in public spaces (such as facial recognition cameras). These systems are not completely prohibited and may be used in the following cases: searches for missing people, prevention of terrorism and the identification of people suspected of committing a serious offence.
- Biometric recognition in public spaces. Law enforcement agents are permitted to use biometric recognition when they have legal or only administrative authorisation.[148]
- Emotion recognition. These emotion inference systems, which have no scientific base, may be applied, provided they are not used in education or employment environments.
- Assessment and profiling in border checks: such as predictive analysis systems to prevent migration or AI-based lie detection systems.[149]

Technologies considered high risk are subject to a series of special obligations (risk management, data governance, technical documentation, transparency, etc.), except when used by law enforcement agencies. As a result, the lobby strategy of the technology industry, as well as the European Council and Parliament, included a path followed by the same providers that decide whether or not their products are high risk.[150]

In an interrelated manner, the AI Act all AI systems created and developed for 'the purpose of national security' are exempt from transparency and accountability obligations, eliminating any measures to safeguard rights under this generic case.[151]

147 European Center for Not-for-Profit Law. (2024). *The AI Act: Enforcement and the role of civil society*. https://ecnl.org/sites/default/files/2024-03/ECNL_AI_Act_Enforcement_Briefing.pdf

148 Ex post biometric recognition is a process carried out after the events have taken place.

149 IA Ciudadana. (2024, 18 June). *IA Ciudadana considera que el Reglamento de Inteligencia Artificial no ha logrado un estándar adecuado de protección de los derechos humanos*. https://iaciudadana.org/2024/06/18/ia-ciudadana-considera-que-el-reglamento-de-inteligencia-artificial-no-ha-logrado-un-estandar-adecuado-de-proteccion-de-los-derechos-humanos/

150 Ibid.

151 European Digital Rights. (2024, 15 March). The EU AI Act fails to set a gold standard for human rights. https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/

As warned by organisations for human rights defence, the gaps in prohibitions and obligations to control AI systems are highly dangerous for human rights, as well as the structural deficiencies of the Act in key aspects like risk classification, as they dangerously open the door to the use of intrusive surveillance technologies within the EU.[152]

Other legislative instruments with an impact on the use of surveillance technologies are:

- **The *European Media Freedom Act* (EMFA).**[153] This legislation, adopted in 2024 and applicable since August 2025, has the purpose of establishing a common framework to protect media pluralism and independence in the EU. However, the final text of the EMFA includes a series of exceptions that **allows the use of spyware against journalists and journalistic sources** under certain circumstances, such as 'public security' or 'investigations of serious offences'. The set of articles, particularly Article 4, reproduces an air of permissiveness that directly threatens media freedom, since it opens the door to surveillance practices on figures especially protected by the rule of law. Thus, according to applicable European legislation, spyware could possibly be used against journalists.

  During the legislative process, different organisations for digital rights and civil liberties, such as Access Now, EDRi and Reporters Without Borders,[154] warned about the risks of this approach and they demanded a total ban on the use of spyware against journalists. Nevertheless, in the end, their proposal was rejected and the adopted text continues to include the exceptions that mean it can be used, with an ambiguous language that fails to clearly explain when it is admissible. The text does not only contradict the protective spirit of the regulation, but it creates a dangerous precedent in Europe-related matters: the standardisation of digital surveillance tools against essential actors for the working of democracy, as are independent journalists and media.

- **The *Pall Mall Process*** is a voluntary code of practice, addressed to States, aimed towards addressing 'proliferation and irresponsible use of commercial cyber intrusion capabilities'.[155] Launched by the United Kingdom and France in a process that started

152 IA Ciudadana. (2025, March). *Cómo lograr una transparencia real con los registros de algoritmos*. Brussels: IA Ciudadana. https://iaciudadana.org/wp-content/uploads/2025/03/Informe_ES.pdf

153 European Commission. (n.d.). *European Media Freedom Act*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en

154 European Centre for Press and Media Freedom. (2023, 22 June). *Civil society and journalists associations urge the Council to protect journalists against spyware and surveillance in the EMFA*. https://www.ecpmf.eu/civil-society-and-journalists-associations-urge-the-council-to-protect-journalists-against-spyware-and-surveillance-in-the-emfa/

155 UK Government. (2025). *The Pall Mall Process: Code of Practice for states*. GOV.UK. https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states

in February 2024,[156] which gathered representatives from States, companies and civil society organisations. The process entered into force in April 2025 with the signing of the Declaration. On the date of this report, two documents have been drawn up: a declaration and a code of practice for States, which has been signed by 27 countries, 19 of which belong to the European Union. Spain is not included.

Although both documents are based on the constructive will to address 'how the use of commercial spyware can weaken national security, human rights, international peace and the stability of cyberspace', its voluntary nature generates significant doubts about their real effectiveness as instruments to stop the abuse associated to these technologies or promote substantial changes in the policies and practices of the signatory States. In addition, since its beginning, **human rights organisations, like EDRi, have warned that these documents could help legitimise the use of certain types of spyware**. Nevertheless, since its approval and the adhesion of over 21 countries, the process is still being monitored in order to identify interferences.[157]

At present, the process is at risk of failing to achieve its goals and despite being non-binding, to be reduced to an excessively general and diplomatic framework that is neither effectively applicable nor reflects the sector's growing reality, nor the risks and damages documented relating to the use of spyware. It is important to mention that, due to its voluntary and broad nature, cases of interferences in its use or abuse aimed towards sabotaging or instrumentalising it have already been documented. On 7 January 2026, NSO Group mentioned in its Annual Transparency Report that it had participated in the Pall Mall Process to prove its human rights compliance, an affirmation that was immediately denied by the French and British government, which confirmed that the Israeli company had not formed part of any conversation.[158] Once again, it is made evident that despite several years have passed and the problem has become more serious, there is still no mandatory regulatory framework capable of addressing these situations.

- **NIS2 Directive**. Applicable since January 2023, it substantially reinforces cybersecurity obligations in critical sectors (such as energy, transport, health, telecommunications and digital structures).[159] Within this framework, thousands of European

156 Ministry for Europe and Foreign Affairs. (2024, 6 February). *The Pall Mall Process: Tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of

157 European Digital Rights. (2025, June). *Spyware and state abuse: The case for an EU-wide ban* (Position paper). https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf

158 The Record. (2026, 2 February). *Spyware maker is hijacking diplomatic efforts to limit commercial hacking, civil society warns*. https://therecord.media/spyware-maker-pall-mall-process-reputation

159 European Commission. (n.d.). *NIS2 Directive: securing network and information systems. A Directive on measures to achieve a common high level of cybersecurity across the Union (Directive SRI 2)*. EU International Digital Strategy. https://digital-strategy.ec.europa.eu/es/policies/nis2-directive

countries are obliged to adopt advanced protection, incident response and risk management measures. This regulatory framework is promoting a growing demand for cyberdefence services and technologies, creating opportunities for specialist providers, including foreigners with a high innovation capacity.

- **The Cyber Resilience Act – CRA)**.[160] The Act entered into force at the end of 2024 and stipulates that digital items (both hardware and software) must incorporate security from the design phase and maintain protection updates throughout its entire life cycle. It also requires certification systems to verify that these items comply with high security standards.[161] This regulation boosts the demand for companies with the capacity to offer digital defence solutions, security audits, monitoring tools and ongoing updating services. One of the main risks is that in order to meet new security demands, manufacturers could incorporate remote control or permanent monitoring mechanisms inside the digital products. Although these functionalities are justified protection reasons, they could turn into constant surveillance systems without sufficient democratic guarantees. The Electronic Frontier Foundation points out a possible indirect impact on the freedom of expression, as connected devices could restrict access to certain functionalities or content under the guise of security.[162] This legal framework would increase technical — and, eventually, political — capacity to intervene in the right to communicate and receive information in the digital environment.

Together it configures an **insufficient and fragmented regulatory system, currently unable to adequately respond to the risks to fundamental rights caused by intrusive surveillance technologies**. There are still important legal loopholes, broad exceptions for the sake of national security, weak supervision mechanisms and a lack of resources for the authorities responsible for complying with existing guarantees. In parallel, civil society participation mechanisms are practically non-existent and it can also be ascertained that there is a contradiction between the EU's fundamental rights commitments and the permissiveness with surveillance technology exports, which are not admitted within its own territory. Added to these restrictions, is the ongoing deregulation agenda that threatens to erode the current standards of the European digital framework.

160 European Commission. (n.d.). *Cyber Resilience Act*. EU International Digital Strategy. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

161 European Digital Rights. (2022, 12 December). *The Cyber Resilience Act: How to make Europe more digitally resilient*. https://edri.org/our-work/the-cyber-resilience-act-how-to-make-europe-more-digitally-resilient/

162 Electronic Frontier Foundation. (2023, 16 May). *EU's proposed Cyber Resilience Act raises concerns for open source and cybersecurity*. https://www.eff.org/deeplinks/2023/05/eus-proposed-cyber-resilience-act-raises-concerns-open-source-and-cybersecurity

V

Gateways for Israeli defence tech companies.

1. European rearmament through NATO and the ReArm Europe Plan.

As the result of NATO's new defence expenditure plan, member countries made a commitment to investing 5% of Gross Domestic Product (GDP) annually on defence-related spending by 2035. A very significant part of this expenditure will be used to develop defence and security technology.[163] In parallel, the ReArm Europe Plan, presented by the European Commission in March 2025, proposes enabling an additional €800,000 on EU Member States' defence expenditure.[164] The Plan, which aims to reinforce European strategic autonomy in weapon-related matters with respect to member countries and external competitors, establishes that 65% of the components of the new defence equipment must be manufactured in the EU or associated countries. The purpose of the 35% margin for collaborating with non-Member States is to compensate the current lack of certain technologies in the European defence industry, which could lead to greater cooperation with Israeli companies and technology providers. As mentioned earlier, this political initiative is reflected, for example, in the Commission's proposal to increase the defence budget in the European Competitiveness Fund by €131 billion between 2028 and 2034.[165]

As regards NATO, in January 2025, the Secretary General of NATO, Mark Rutte, declared, 'On the battlefields of Ukraine, $400 drones used the right way are taking out $2 million Russian tanks. Speed is essential, not perfection, to incorporate these new technologies'.[166] These political declarations have been translated in documents of the transatlantic organisation such as Foster and Protect: NATO's Coherent Implementation *Strategy on Emerging and Disruptive Technologies* (2021), which gives priority to new technological areas: AI, autonomous systems, quantum technologies, biotechnology and human enhancement technologies, space, hypersonic systems, novel materials and manufacturing, energy and propulsion autonomous systems, quantum technology, biotechnology and human improvement technologies, space technologies, hypersonic systems, new materials and advanced manufacturing, energy and propulsion, as well as next-generation communications networks.[167]

---

163 Unidos por Israel. (2024, 11 September). *La innovación en tiempos de guerra impulsa el crecimiento de la tecnología de defensa israelí, atrayendo el interés mundial*.
https://www.unidosxisrael.org/noticias/la-innovacion-en-tiempos-de-guerra-impulsa-el-crecimiento-de-la-tecnologia-de-defensa-israeli-atrayendo-el-interes-mundial/

164 European Commission. (n.d.). *Future of European defence*.
https://commission.europa.eu/topics/defence/future-european-defence_en

165 European Commission. (2024). *EU defence cooperation: Towards a European defence union*. Publications Office of the European Union.
https://op.europa.eu/en/publication-detail/-/publication/7e0c92fe-8e4d-11e9-9369-01aa75ed71a1

166 Rutte, M. (2025, 10 June). *Building a Better NATO* [Speech]. Chatham House, Londres. NATO official transcript.
https://www.nato.int/en/news-and-events/events/transcripts/2025/06/10/building-a-better-nato

167 OTAN. (s. d.). *Emerging and disruptive technologies*.
https://www.nato.int/cps/en/natohq/topics_184303.htm

To implement this technological transformation, NATO has created diverse instruments, among which the following stand out: the Defence Innovation Accelerator for the North Atlantic (DIANA), *NATO Innovation Fund and NATO-Ukraine Innovation Cooperation Roadmap*. In turn, these new instruments are facilitating the increase of military production in European Member States and an unprecedented attraction of defence tech and technology security companies towards Europe, many of which are Israeli.

Interoperability: the path towards procurement and mass production

NATO centres the contracts for weapons and other defence and logistics products through the *NATO Support and Procurement Agency (NSPA)*. This system establishes military and operational requirements to meet the organisation's standards, as well as EU export control regulations.[168] At the same time, the 2023 Defence Production Action Plan (DPAP) defines the operations for the mass production of munitions and weapons in cooperation with the European defence industry.[169] Within this framework, the interoperability of technologies with the transatlantic organisation's new armament is a fundamental requirement for subsequent contracts.

One way of achieving this interoperability is if a NATO member country previously adds this technology and armaments to its military architecture. For example, in 2023, Germany purchased the Arrow-3 system from IAI for its missile interceptor system; this integration implied including this technology in the European Sky Shield Initiative (ESSI), a system for air defence capabilities development and missile interception led by Germany in a group of different EU countries.[170] Two years later, NATO purchased the Arrow-3 system.[171]

In a similar manner, **Elbit Systems and Rafael Advanced Defense Systems**, have been transferring their technology and armament to NATO. On occasions, these companies are accessed through European companies, as in the case of the joint venture created between IAI and Airbus to deploy the Heron TP drone from NATO.[172] These contracts boost

168 White & Case. (2024, 25 January). *Navigating NATO procurement: Legal and regulatory considerations for companies in Finland*.
https://www.whitecase.com/insight-alert/navigating-nato-procurement-legal-and-regulatory-considerations-companies-finland

169 OTAN. (2025, 13 February). *Updated Defence Production Action Plan*.
https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/updated-defence-production-action-plan

170 German-Israeli Chamber of Industry & Commerce (AHK Israel). (2023, 28 September). *Germany signs nearly $4 billion deal for Israel's Arrow 3 missile defense system*.
https://israel.ahk.de/en/news/germany-signs-nearly-4-billion-deal-for-israel-s-arrow-3-missile-defense-system

171 Arvizo, A. (2025, 22 August). *Israel's growing military tech savvy gives it leverage abroad*. Defense Opinion.
https://defenseopinion.com/israels-growing-military-tech-savvy-gives-it-leverage-abroad/999/

172 Stenglin, W. (2025, 23 July). *Armaments cooperation: How Israeli start-ups aim to penetrate the German market*. Table. Briefings.
https://table.media/en/security/feature/armaments-cooperation-how-israeli-start-ups-want-to-penetrate-the-german-market

the installation of military production in European territory. In 2004, Elbit Systems created a subsidiary in the United Kingdom, named Elbit Systems UK Limited, to set up production plants in Brighton, South Wales, Leicester, among other places. Even since then, this Israeli company has been awarded numerous contracts to supply drones and other services. El 2025, a potential contract award for an armed forces training contract worth £2 billion (approx. €2.27 billion) generated considerable political debate.[173] In the end, the contract was awarded to the US defence company, Raytheon.[174]

The armament of Israel's main military companies incorporates other technologies developed by smaller growth-stage companies. For example, the Israeli startup **NextVision**, specialised in high-precision cameras for drones manufactured by companies like IAI, Rafael or Elbit Systems,[175] is certified by Blue UAS and included in the Blue UAS Framework, an interoperability mechanism for drone components, which facilitates access to US government and NATO contracts. [176] NextVision has benefitted from the Gaza Strip genocide and is currently at expansion stage in Europe,[177] as shown by the fact that 55% of the profit obtained during 2025 came from the European market, and NATO is a clear commercial goal, as made evident in its presentations of results.[178]

Case study: Defence Innovation Accelerator for the North Atlantic (DIANA)

In 2023, NATO created DIANA, a decentralised defence innovation accelerator with centres in London, Halifax and Tallinn. Through the network, dual-use technologies can be developed before they are purchased by the Atlantic Alliance. Every year, DIANA selects startups and SMEs in the fields of energy resilience, surveillance, critical infrastructure, secure information systems and health. For a year, the companies receive funding, access to test centres, connection with actors from the defence industry and security, and mentoring so they may adapt their solutions to NATO's requirements.

To date, there have only been two editions of the acceleration programme, and in both editions links to Israeli companies have been observed. In 2024, the US company **Zepher**

173 UK Parliament. (2025, 23 June). Armed forces training contract and Elbit Systems (Early Day Motion 64212). https://edm.parliament.uk/early-day-motion/64212/armed-forces-training-contract-and-elbit-systems

174 Glenton, J. (2026, 14 January). *Elbit Systems loses £2bn UK army contract to rival arms firm Raytheon*. The Canary. https://www.thecanary.co/uk/analysis/2026/01/14/elbit-systems-loses/

175 American Friends Service Committee. (n.d.). *NextVision*. Investigate. https://investigate.afsc.org/company/nextvision

176 NextVision. (2025). *Financial statements for the period ended June 30, 2025* (Q2 2025 Report). https://investor-relations.nextvision-sys.com/wp-content/uploads/2025/03/%D7%A8%D7%91%D7%A2%D7%95%D7%9F2-2025FS_300625_isa.pdf

177 NextVision. (2025). *Financial statements as of June 30, 2025* [Informe trimestral Q2]. https://investor-relations.nextvision-sys.com/wp-content/uploads/2025/03/%D7%A8%D7%91%D7%A2%D7%95%D7%9F2-2025FS_300625_isa.pdf

178 NextVision. (2025, August). *NextVision 1H-2025 Results Presentation*. https://investor-relations.nextvision-sys.com/wp-content/uploads/2025/08/NextVision1H-2025-Results-Presentation_Agu2025_En-%D7%A8%D7%91%D7%A2%D7%95%D7%9F2-%D7%97%D7%93%D7%A9.pdf

Flight Labs, specialised in drone design and production, benefitted from the DIANA programme.[179] A year later, the company was purchased by the Israeli startup, Heven Drones, specialised in the development of hydrogen-powered drones for the defence sector.[180] On its corporate website, the company indicates that the Israeli army is a strategic partner.[181] The 2025 edition saw the participation of the British affiliate of SB Technologies,[182] SB Tech UK Ltd,[183] which will work with its strategic partner, the Israeli company, XM Cyber, to develop and market CTEM (Continuous Threat Exposure Management) cybersecurity technology. XM Cyber is a company founded by the former Mossad chief, Tamir Pardo. Since 2021, XM Cyber forms part of the Israeli Operational Technologies Cyber consortium, led by Rafael Advanced Defense Systems. The purpose of the consortium is to provide technology solutions to protect Israeli critical infrastructures through the Cyber Emergency Response agreement, signed with the Israeli government.[184] At present, XM Cyber is owned by Schwarz Group, based in Germany. [185]

At the same time, DIANA cooperates with 20 innovation ecosystems[186] and 180 test centres (laboratories, test sites, cybersecurity centres, etc.) located in NATO member countries.[187] One of these is the Spanish National Cybersecurity Institute (INCIBE) that, since the start of the genocide in the Gaza Strip in 2023, has participated in cybersecurity events in Israel (*CyberTech Global 2025*); throughout 2024, it organised meetings with Israeli companies,[188] including a meeting between INCIBE and Dream Security, a company

179 NATO DIANA. (2024). 2024 cohort of companies. Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/about-diana/2024-cohort-of-companies.html

180 Heven. (2025, 25 April). *Heven announces acquisition of Zepher Flight Labs, expanding capabilities in advanced drone technology*. PR Newswire. https://www.prnewswire.com/news-releases/heven-announces-acquisition-of-zepher-flight-labs-expanding-capabilities-in-advanced-drone-technology-302437947.html

181 HevenDrones. (n.d.). *Hydrogen-powered drones for defense and commercial use*. https://hevendrones.com/

182 NATO DIANA. (2025). *2025 cohort of companies*. Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/about-diana/2025-cohort-of-companies.html

183 Companies House. (n.d.). *Heven Drones UK Ltd: Officers*. Gov.uk. https://find-and-update.company-information.service.gov.uk/company/13916820/officers

184 XM Cyber. (2021, 23 June). *Rafael sets up first-of-its-kind Israeli cyber consortium with leading cyber solution partners* [Press release]. https://xmcyber.com/press-release/rafael-sets-up-first-of-its-kind-israeli-cyber-consortium-with-leading-cyber-solution-partners

185 Ben-David, R. (2021, 22 November). *German firm acquires ex-Mossad chief's cybersecurity startup for $700m*. The Times of Israel. https://www.timesofisrael.com/german-firm-acquires-ex-mossad-chiefs-cybersecurity-startup-for-700m/

186 NATO DIANA. (n.d.). *Accelerator sites and test centres*. Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/accelerator-programme.html#accsites

187 NATO DIANA. (n.d.). *About DIANA*. Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/about-diana.html

188 INCIBE. (2018, 11 May). *Más de 40 empresas israelíes y españolas se reúnen para impulsar la innovación en ciberseguridad*. https://www.incibe.es/incibe/sala-de-prensa/mas-de-40-empresas-israelies-y-espanolas-se-reunen-para-impulsar-la

created by Shalev Hulio, the founder of NSO Group, during which INCIBE offered to buy the Israeli company's technology.[189]

Another strategic space for NATO is the coordination and technology development hub in Tallin.[190] Estonia is aiming to become a pole of excellence for disruptive technologies; that is, technology that changes markets, companies and consumption patterns, and attracts companies from around the world, creating an e-Residency system through which groups or individuals may register a company in a matter of minutes. Furthermore, the government of Estonia and the Estonian Centre for Defence Investment are creating a military technology and munitions production test centre at the Ämari military base, the Defence Industry Park.[191] Within this context, in November 2025, the Israeli government opened a new embassy to strengthen political and economic ties between both countries.[192] The event was accompanied by the organisation of a Estonia-Israel business forum, which was visited by over 50 companies from the Israeli cybersecurity and defence sector.[193]

These conditions position **Estonia as a European gateway for defence tech companies**. Added to the presence and relationships of large Israeli defence companies with the government of Estonia, such as IAI,[194] is the landing of security technology companies. An example is the cybersecurity company Cyberbit, involved in the mass surveillance of Palestinians and activists around the world,[195] and which in 2025 purchased the Estonian company Rangeforce, thus reinforcing its presence in the country.[196]

189 El Confidencial Digital. (2025, 11 September). *El INCIBE se reunió con la empresa israelí de un creador de Pegasus tras la invasión de Gaza*. https://www.elconfidencialdigital.com/articulo/seguridad/incibe-reunio-empresa-israeli-creador-pegasus-invasion-gaza/20250910171218979303.html

190 NATO DIANA. (n.d.). *Defence Innovation Accelerator for the North Atlantic*. https://www.diana.nato.int/index.html

191 Trade with Estonia. (2024, 15 May). *Estonia is creating a defence industry park*. https://tradewithestonia.com/estonia-is-creating-a-defence-industry-park/

192 Estonian World. (2025, 12 March). *Israel opens embassy in Tallinn, deepening ties with Estonia*. https://estonianworld.com/security/israel-opens-embassy-in-tallinn-deepening-ties-with-estonia/

193 Veksler, A. (2025, 16 November). *From Tallinn to Taipei, Israel Binds Small Democracies Into a Global Front*. The Media Line. https://themedialine.org/news/opinion/from-tallinn-to-taipei-israel-binds-small-democracies-into-a-global-front/

194 Israel Aerospace Industries [@ILAerospaceIAI]. (2021, 6 October). *IAI and South Korea's KAI signed a Memorandum of Understanding (MOU) to collaborate on Loitering Munitions programs* [Post]. X. https://x.com/ILAerospaceIAI/status/1445738484841336840

195 Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., and Deibert, R. (2017, 6 December). *Champing at the Cyberbit: Ethiopian dissidents targeted with new commercial spyware*. Citizen Lab. https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

196 Cyberbit. (2024, 6 May). *Cyberbit acquires RangeForce: Creating the world's leading cyber defense skills and readiness platform* [Press release]. https://www.cyberbit.com/news/cyberbit-acquires-rangeforce/

2. The Ukraine war and penetration of Israeli companies via Eastern Europe.

An important part of the increase in European defence budgets is spent on buying arms and military technology for Ukraine. The NATO Prioritised Ukraine Requirements List (PURL) is an instrument that coordinates Ukraine's military and technology requirements with European and US inventories. According to Alexus Grynkewich, NATO's Supreme Allied Commander, 'The Ukrainians will let us know what their requirements are. We then bring that into a combined U.S. European Command and NATO working group that elevates those requirements.'[197] Consequently, the international defence tech companies that operate in Europe test their technologies in combat and enter into contact with members of the Ukrainian army have greater opportunities to access NATO contracts.[198]

The presence of Israeli companies in Ukraine has expanded through different channels. On the one hand, by way of direct agreements with the Ukrainian government, as in the case of the Ministry of Defence and Elbit Systems. On the other, international companies participate in military innovation platforms like Brave1, as in the case of the Israeli company, R2.[199] In parallel, direct partnerships are formed between Israeli and Ukrainian companies – for example, Dronex Israel – which also collaborates with the Israeli army through MAFAT Directorate of Defense, Research and Development.[200]

XTEND, the hidden agenda of the drone industry's emergency

XTEND's drone technology, as mentioned in the previous section, has been massively used by the Israeli army in the Gaza Strip genocide.[201] The formalisation of contracts worth millions with the Israeli government[202] has strengthened the company's positioning and boosted its global outreach.[203] In parallel, it plans to scale up production for Ukraine to 4.5

197 Tucker, P. (2025, 28 August). *Test your arms and gear in Ukraine, NATO's military chief urges companies*. Defense One. https://www.defenseone.com/business/2025/08/test-your-arms-and-gear-ukraine-natos-military-chief-urges-companies/407779/

198 Ibid

199 Czerny, M. (2024, 19 November). *Better late than never: Israeli companies finally reach out to Ukraine to help fight Iranian drones*. The Kyiv Independent. https://kyivindependent.com/better-late-than-never-israeli-companies-finally-reach-out-to-ukraine-to-help-fight-iranian-drones/

200 Ibid

201 AFSC. (n.d.). *XTEND*. Investigate. Recovered on 3 October 2025, from https://investigate.afsc.org/company/XTEND

202 SOFX. (2024, 5 June). *Israel orders 5,000 XTEND FPV drones for IDF ground forces*. https://www.sofx.com/israel-orders-5000-xtend-fpv-drones-for-idf-ground-forces/

203 Rose, E. (2025, 31 January). *Israeli startups make global plans after key role in war*. Reuters. https://www.reuters.com/world/middle-east/israeli-startups-make-global-plans-after-key-role-war-2025-01-31/

million units.[204] Recently, the company's managing director also announced their interest in accessing NATO's market,[205] with the aim of extending sales to the fields of security and police.[206]

To achieve these goals, XTEND has developed a business structure in the United States and Europe; in the US, the company has set up its drone mass-production facility.[207] While in Europe its structure is based on a framework of commercial offices and product distribution networks in the United Kingdom, the Netherlands, Germany and Eastern Europe.[208] XTEND's penetration in the European continent has combined CORDIS research projects,[209] participation in military exhibitions — such as the LANDEURO conference held in Wiesbaden (Germany) in July 2025 — and showcases and simulations around Europe. In 2020, a demonstration of the Skylord Hunter was held in Spain with the participation of the Ministries of Internal Affairs and Defence.[210] Lastly, in the United Kingdon, exclusive tests have been conducted with the British army and the country's military industry.[211]

Transfer of Ukrainian technology to Israel: the Zvook case

The disruptive technologies used in Ukraine are also creating growing interest in Israel. An example is Zvook, a Ukrainian startup that develops AI-powered acoustic sensors for detecting drones, missiles and other aerial threats that, according to the director, Maryan Sulym, are able to detect Iranian-made Shahed drones within a range of 3 to 5 km and cruise missiles within a range of 5 to 7 km. According to Sulym, three Israeli defence tech companies have contacted Zvook to study possible collaborations.[212]

---

204 Avigad, D. (2025, 4 September). *Drone-maker Aviv Shapira dreams of a Wall Street IPO*. Globes. https://en.globes.co.il/en/article-drone-maker-aviv-shapira-dreams-of-a-wall-street-ipo-1001520867

205 Nir, G. (2025, 7 August). *Pioneering AI, autonomous technologies to support NATO's global evolving operational needs*. The Jerusalem Post. https://www.jpost.com/defense-and-tech/article-863579

206 Avigad, D. (2025, 4 September). *Drone-maker Aviv Shapira dreams of a Wall Street IPO*. Globes. https://en.globes.co.il/en/article-drone-maker-aviv-shapira-dreams-of-a-wall-street-ipo-1001520867

207 TechTime. (2025, 4 July). *XTEND accelerates its global expansion and product development*. https://techtime.news/2025/07/04/XTEND-4

208 Dronivo. (n. d.). *XTEND: Human-centric autonomous systems*. https://www.dronivo.de/XTEND_1

209 European Commission. (n. d.). *SKYLORD: A new generation of aerial robotic systems for first responders* (Project ID 887959). CORDIS. https://cordis.europa.eu/project/id/887959

210 UAS Weekly. (2020, 5 October). *XTEND showcases HUNTER platform at Europe's largest evaluation of counter drone systems*. https://uasweekly.com/2020/10/05/XTEND-showcases-hunter-platform-at-europes-largest-evaluation-of-counter-drone-systems/

211 Curtis, M. (2024, 20 June). *Battle-tested in Gaza: Britain's next drones?* Declassified UK. https://www.declassifieduk.org/battle-tested-in-gaza-britains-next-drones/

212 Czerny, M. (2024, 19 November). *Better late than never: Israeli companies finally reach out to Ukraine to help fight Iranian drones*. The Kyiv Independent. https://kyivindependent.com/better-late-than-never-israeli-companies-finally-reach-out-to-ukraine-to-help-fight-iranian-drones/

Ukrainian organisations like Global Israel Initiative (GII)[213] promote relationships between the defence tech sectors of both countries to exchange technology, alliances and joint research. Figuring in GII's portfolio of partners is the Ukrainian company, SIGMA Software, which offers cybersecurity services for the defence industry. NATO is one of the company's customers and it has offices in Israel.[214]

This situation means that an increasing number of Israeli companies are landing in Eastern Europe to manufacture and market products, led by large military companies like Elbit Systems. This company created three subsidiaries and four production plants in Romania. Through its subsidiary company, Uzina Automecanica Moreni S.A. (UAM), it has been awarded contracts with the government to produce artillery, promoting agreements with national companies, such as CN ROMARM S.A.[215] More recently, in 2022, the likewise Israeli company, Agilite, specialised in tactical gear, [216] and mentioned in the previous section for its participation in the genocide against the Gaza Strip, registered a subsidiary in Slovakia, under the name Agilite Systems Europe S.R.O.[217]

3. The epicentre of the Israeli military lobby: Germany.

Germany is Israel's second-largest arms supplier after the United States. Between 2018 and 2022, its export licences reached €879.8 billion. In 2023, exports from the heart of the European Union to Israel grew from €32.3 million to €326.5 million. The majority of these export licences were granted after the start of the genocide.[218] Around these economic interests a large lobby structure has developed, which is not a new phenomenon, but since the start of the genocide in the Gaza Strip, new trends can be identified.

The Israel Defence and Security Forum (IDSF), made up of 35,000 military reservists and led by the retired military officer of the Israeli army, Amir Avivi, started a lobby campaign in European institutions to prevent sanctions in Israel and influence people with its policy

213 Global Investigations Initiative [GII]. (s. d.). XTEND Ltd. - Defense Export and Supply Chain Data. The Global Israeli Initiative corporate website was active between 2018 and early 2026, with significant content activity throughout 2024. See the archived version retrieved via the Wayback Machine: https://web.archive.org/web/20240322094050/https://gii.global/

214 Sigma Software. (n. d.). *Custom software development for the defense industry*. https://sigma.software/industries/custom-software-for-defense

215 Elbit Systems. (n.d.). *Modernizing the eastern flank*. Elbit Systems blog post. https://www.elbitsystems.com/blog/modernizing-the-eastern-flank

216 Agilite. (n.d.). *Premium Israeli tactical gear and equipment*. https://agilite.co.il/en

217 EMIS. (n.d.). *Agilite Systems Europe S.R.O. (Slovakia) company profile*. EMIS Benchmark & Company Intelligence. https://www.emis.com/php/company-profile/SK/Agilite_Systems_Europe_SRO_en_17406060.html

218 Ibid

on the Gaza genocide, as well as reduce European support for ceasefire initiatives and the case of South Africa that was brought before the International Court of Justice.[219] According to its own public activity, since 2023, the organisation has travelled repeatedly to Brussels and attended meetings with at least 19 Members of the European Parliament, among whom were European Commissioner for Defence and Space, Andrius Kubilius, and the vice-president of the European Parliament, Pina Picierno.[220]

Along similar lines, the European Leadership Network (ELNET), based in Paris with branches in different European capitals (Berlin, Rome, London and Belgium), acts like a pro-Israel lobby structure. One of its main goals is to improve Israel's image in Europe. For this reason, it sends out messages to make France and other European countries adopt more favourable stances as regards Israel, like recognise Jerusalem as the capital of the State. It also works to **coordinate narratives and influence the media, think-tanks and strategic research centres, promoting agendas aligned with Israeli interests**, including the idea that Europe can benefit from Israeli technology and support in security, innovation and intelligence.[221] One of ELNET's characteristic features is the use of strategies for economic diplomacy o promote Israel as an innovation actor and strategic European ally, while minimising and concealing the implications of the policies that contribute towards the occupation and apartheid against the Palestinian population.[222]

ELNET's lobby strategies are especially evident in Germany, where it has announced a new partnership, the Security and Defence Initiative (ESDI), focused on promoting the adoption of Israeli military and security technology; it has also created a defence academy. Some of the German companies involved are DND Digital, Code Blue by Dussmann, Elbit Systems, IAI, Lufthansa Technik, Renk, Rohde & Schwarz and Werter.[223]

In parallel, ELNET has also promoted the Cyber and Security Pact between the government of Germany and Israel. In January 2026, the Federal Minister of the Interior, Alexander Dobrindt, and the Prime Minister of Israel, Benjamin Netanyahu, signed the expansion of the cybersecurity cooperation agreement between both countries.[224] It also contemplates promoting the creation of a joint cyber research centre between both countries, take advantage of Israeli technology to protect itself from possible strikes and significantly extend intelligence cooperation, especially between the Federal Intelligence Ser-

219 Dillenbourg, N. (2025, 6 March). *Exposed: The opaque lobby of high-ranking Israeli officers in Brussels*. Follow the Money (FTM) / The EU Files. https://www.ftm.eu/articles/israels-opaque-lobby-european-parliament

220 Ibid

221 IELNET. (n.d.). *European Leadership Network: Strengthening relations between Europe and Israel*.

222 Stern, J. (2021, 26 January). *Elnet. Visit Israel, its settlements, its surveillance technologies...* Orient XXI. https://orientxxi.info/elnet-visit-israel-its-settlements-its-surveillance-technologies,4467

223 ELNET Deutschland. (2024, 21 February). *ELNET begründet neue Security & Defense Initiative*. https://elnet-deutschland.de/themen/politik/elnet-begruendet-neue-security-defense-initiative/

224 Federal Ministry of the Interior and Community. (2026, January). *Cybersecurity cooperation with Israel expanded*. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2026/01/israel-dobrindt-en.html

vice and the Mossad.[225] Dobrindt also announced the creation of a German-Israeli cyber research centre.[226] An initiative that would strengthen even more the implementation of Israeli companies in the German technology ecosystem.

From an economic lobby to cooperation between technology ecosystems

Another initiative driven by ELNET is the establishment of the German Israeli Network of Startups & Mittelstand (GINSUM) with the support of the German Federal Ministry for Economic Affairs and Climate Action, to link the German Mittelstand, small and medium enterprises and municipal actors with Israel's ecosystem of emerging companies.[227]

The GINSUM affirms that cooperation between the German Mittelstand and Israeli start-ups offers important competitive advantages. Startups, which are more agile and customer-oriented, provide external innovation that helps medium companies adapt to new technologies, especially in fields such as cybersecurity, and prevent these companies from getting left behind from national and multinational competitors already active in Israel.[228]

According to a study by the German foundation Bertelsmann, **German and Israeli start-ups use different interaction and cooperation mechanisms: they either distribute their own products to Israel or purchase Israeli technology for internal use**. In the first case, collaboration usually starts with sales and, once local contacts have been established, innovation and R&D options are explored. In the second case, the integration of Israeli products – especially in the fields of cybersecurity and data analysis – reveals Israel's technology ecosystem and its capacity. Other mechanisms are scouting – the identification of technological opportunities and local startups, through specialists in the field – and creating accelerators or incubators, either proprietary or in collaboration with local actors, which make it possible to keep close to new innovations and monitor them at different degrees, depending on the chosen model. Furthermore, joint R&D activities can be set up with Israeli companies or own centres can be created. Finally, strategic invest-

225 Monroy, M. (2025, 24 July). *Israel and US companies are using Gaza as a tech test lab for AI, Germany may soon benefit in a new "pact"*. Dissecting Security Architectures. https://digit.site36.net/2025/07/24/israel-and-us-companies-are-using-gaza-as-a-tech-test-lab-for-ai-germany-may-soon-benefit/

226 Reuters. (2025, 29 June). *Germany seeks Israeli partnership on cyberdefence, plans 'Cyber Dome'*. https://www.reuters.com/business/aerospace-defense/germany-seeks-israeli-partnership-cyberdefence-plans-cyber-dome-2025-06-29/

227 Sommer, C. (2021, March 11). What can Israeli start-ups offer German mid-sized companies? GINSUM (German Israeli Network of Startups & Mittelstand). The article was published in 2021 and removed from the GINSUM website in early 2026. See the archived version retrieved via the Wayback Machine: https://web.archive.org/web/20210619145458/https://www.ginsum.eu/what-can-israeli-start-ups-offer-german-mid-sized-companies/

228 Ibid

ments or acquisitions of Israeli startups often lead to their transformation into local R&D centres.[229]

A specific examples is **C2A Security**, an Israeli startup specialised in cybersecurity for industrial and critical infrastructures.[230] In 2024, the company opened a subsidiary in Germany, C2A Security GmbH, with the purpose of positioning itself in the European security tech market, especially the German market,[231] to thus adapt to EU cybersecurity regulations.[232] In parallel, C2A Security is developing part of its technology through the Israeli incubator, Labs/02 — a technology project support and funding programme —[233] funded by international actors that include OurCrowd, Motorola Solutions, Reliance Industries and Yissum, the technology transfer company of the Hebrew University of Jerusalem.[234] Within this context, it is worth noting that Motorola Solutions and its subsidiary in Israel appear in the NATO database of companies linked to activities in illegal Israeli settlements in the Occupied Palestinian Territory.[235]

4. Participation in technology and cybersecurity events as a mechanism to access the EU.

In recent years, European cybersecurity fairs and congresses such as Cybersec Europe (Brussels), Barcelona Cybersecurity Congress, Cyber Intelligence Europe (Madrid), Cyberwise Con (Vilna), Infosecurity Europe (London) and IT-SA (Nuremberg) have become key platforms used by Israeli companies to access the European market. Under the umbrel-

229 Kandel, E., Harel, S., Alon, I., Elman, O., & Gick, M. (2017). *The German Mittelstand and the Israeli startup ecosystem: Tapping Israel's innovative potential*. Bertelsmann Stiftung. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Innov_Israel_final.pdf

230 C2A Security. (n.d.). *Securing solar infrastructure: Managing cybersecurity risks in renewable energy*. https://c2a-sec.com/securing-solar-infrastructure-managing-cybersecurity-risks-in-renewable-energy/

231 C2A Security. (2024, 16 May). *C2A Security expands in Europe, opens a German subsidiary*. https://c2a-sec.com/c2a-security-expands-in-europe-opens-a-german-subsidiary/

232 C2A Security. (2025, 4 August). *Navigating NIS2: Essential OT security for EU manufacturers*. https://c2a-sec.com/navigating-nis2-essential-ot-security-for-eu-manufacturers/

233 Labs/02. (n.d.). *Portfolio*. https://labs02.com/portfolio/

234 OurCrowd. (2018, 31 January). *OurCrowd's Labs/02 to invest in up to 100 early stage companies over the next 10 years with Israel Innovation Authority support*. MarketScreener. https://www.marketscreener.com/quote/stock/MOTOROLA-SOLUTIONS-INC-7130472/news/OurCrowd-s-Labs-02-to-Invest-in-up-to-100-Early-Stage-Companies-Over-the-Next-10-Years-with-Isra-25901691/

235 Office of the United Nations High Commissioner for Human Rights. (2025, 26 September). *Database of all business enterprises involved in the activities detailed in paragraph 96 of the report of the independent international fact-finding mission to investigate the implications of the Israeli settlements on the civil, political, economic, social and cultural rights of the Palestinian people throughout the Occupied Palestinian Territory, including East Jerusalem* (A/HRC/60/19, advanced edited version). United Nations. https://docs.un.org/en/A/HRC/60/19

la of technology innovation, Israeli companies promote surveillance and artificial intelligence solutions that often come from the military sector.

Israel's participation in these events is neither casual nor improvised, it forms part of a **sustained diplomatic and economic strategy, driven by Israeli internationalisation institutions, which organise national exhibitions and commercial missions to present the country as a 'global cybersecurity hub'**. This presence is reinforced by partnership agreements with the European Union that enable these companies to convey an image of legitimate actors within the European technology ecosystem, despite that fact that they were originally linked to a context of genocide, conflict and military occupation.

Thus, fairs like the ones held in Barcelona, Brussels or Nuremberg are rather like spaces used to legitimise and 'sanitise' businesses, where companies linked to the Israeli cybersecurity and military industry ecosystem may redefine themselves as digital innovation civil startups. This phenomenon raises the question of whether European institutions have the capacity to distinguish between civil and dual-use technology, and brings to light the fragility of ethical and political, and commercial and consumer-protection controls against commercial and geostrategic interests.

The IT-SA Fair in Nuremberg, held at the end of October 2025, is also a space where relationships with Israeli companies is encouraged.[236] Indeed, there was an Israel National Pavilion with eight Israeli cybersecurity companies that presented their products.[237]

At Fira de Barcelona, for example, the Israeli company owned by Sergio Vinitzly,[238] ViSerCo, figures as Fira de Barcelona's international office in Israel. This company is a delegate of Fira de Barcelona since 2007 and has represented Israel until the present day.[239] The company's CEO is also one of the co-founders of the Israel Smartcity Institute.[240]

According to its corporate website, ViSerCo is an Israeli business consultancy that specialises in supporting other companies, particularly Israeli companies, to position themselves in international markets through business strategies, establishing contacts and presence in trade fairs or sectoral events. The company highlights its knowledge and experience in the digital industry and new technologies, a sector that includes cybersecurity and technological innovation.

---

236 it-sa Expo&Congress. (n.d.). it-sa Expo&Congress — Europe's leading trade fair for IT security. https://www.itsa365.de/en/it-sa-expo-congress

237 Israel Trade & Economic Mission to Germany. (2025). Israeli National Pavilion at it-sa 2025, 7–9 October [Event]. Messe Nürnberg, Germany. https://itrade.gov.il/germany/event/israeli-national-pavilion-at-it-sa-2025-7-9-october/

238 Vinitsky, S. (n.d.). Sergio Vinitsky's LinkedIn profile. LinkedIn. https://www.linkedin.com/in/sergio-vinitsky-6b3a07

239 ViSerCo. (n.d.). *Soluciones tecnológicas de seguridad y defensa*. https://viserco.biz/

240 Israel Smart Cities Institute. (s. f.). *Board*. https://www.israelsmartcities.org/the-board/

The guidance provided by ViSerCo turns it into a true facilitator for helping Israeli technology and cybersecurity companies land in Europe, especially in cities like Barcelona, where international trade shows such as the **Mobile World Congress** or Barcelona Cybersecurity Congress offer an optimum environment for connecting with investors, partners and European customers. In this regard, **ViSerCo's role is not as a developer of its own technology, but company that opens doors and creates networks that enable other Israeli businesses to legitimise themselves and integrate into the European market.**

In this context, **Fira de Barcelona** plays a particularly significant role as a recurring venue hosting Israeli companies and official Israeli state pavilions at technology and cybersecurity events. Conferences such as the **Mobile World Congress, the Barcelona Cybersecurity Congress**, and other trade fairs linked to digital innovation have repeatedly featured Israeli technology companies, some of which have documented ties to the military and security industries. This presence is not neutral, considering that Fira de Barcelona is a public consortium jointly governed by the Barcelona Chamber of Commerce, the Government of Catalonia, and Barcelona City Council, which entails institutional responsibility.

Over the past two and a half years, organizations such as **La Fira en la Mira** and the Coalition **Prou Complicitat amb Israel** have denounced the systematic and repeated presence at Fira de Barcelona of Israeli pavilions and companies directly linked to the Israeli military, the Israeli military occupation, and the genocide against the Palestinian people. This situation persists despite the fact that both Barcelona City Council and the Government of Catalonia have passed motions calling on Fira de Barcelona to stop providing space to these pavilions and companies.

Within this context, **Fira de Barcelona plays an especially relevant role as a recurrent space for welcoming Israeli companies** and national pavilions in technology and cybersecurity events. Congresses like the Mobile World Congress, Barcelona Cybersecurity Congress or other trade shows connected to digital innovation have repeatedly counted on the presence of Israeli tech companies, some of which have documented links to the military and security industry. This presence is not neutral if it is borne in mind that Fira de Barcelona is a public consortium, integrated equally by the Chamber of Commerce of Barcelona, Government of Catalonia and Barcelona City Council, which implies a direct institutional responsibility with regard to ethical, political and human rights criteria that should govern the selection of exhibitors and collaborators. **The normalisation of this presence, under the pretext of innovation and economic competitiveness helps legitimise business actors from a context of conflict and military occupation**, and highlights the lack of clear human rights due diligence mechanisms within an exhibition centre supported by public resources.

Recently, different journalistic investigations have brought to light the growing presence of European and Israeli companies in events of a reserved nature, such as ISS World, held in Prague, considered one of the most important meeting points in the global cybersecu-

rity, surveillance and intelligence sector.[241] At these kind of trade shows, where access is restricted to police forces, security agencies and companies in the sector, Europe-based businesses have also been detected that offer potentially intrusive technology. An illustrative example is First Wap, documented by Lighthouse Reports in 2024.[242] This surveillance technology company has been linked to the marketing and deployment of digital control tools in diverse contexts, including the European market. Its presence in these environments makes it evident the extent to which the European cybersecurity market can operate as a space where public and private actors may connect with each other — companies that lack transparency and fail to properly scrutinise democracy and supervise impacts on human rights.

In conclusion, this network of European technology and cybersecurity congresses and fairs function like a structured business integration channel for Israeli companies, which find visibility, access to European institutional customers and collaborations with research centres. In addition, national pavilions promoted by public Israeli institutions reinforce this access and enable the Israeli industry of defence and surveillance technology to rebrand itself as an ecosystem of civil technology innovation.

5. From soft-landing in Cyprus to opaque corporate structures.

Cyprus is a strategic country for Israeli technology companies and startups, as it offers a set of geographic, legal, tax and financial conditions that facilitate soft-landing; in other words, these companies have an advantageous landing.[243] To start with, due to its geographic proximity to Israel flights are direct and logistics is simple. Many Israeli business owners become residents and buy property, without losing the possibility to make frequent trips to their country of origin. Cyprus also offers access to the EU market without the usual barriers found by extra-Community companies.[244] **Incorporating a company in Cyprus means that it can operate and sell products and services throughout the European Union without additional licences**. Furthermore, founders and workers obtain European residence permits and can freely move capital within the Community. The country

241 Geiger, G., Black, C., Freudenthal, E., & Coluccini, R. (2025, 14 October). *The surveillance empire that tracked world leaders, a Vatican enemy, and maybe you*. Mother Jones. https://www.motherjones.com/politics/2025/10/firstwap-altamides-phone-tracking-surveillance-secrets-assad-erik-prince-jared-leto-anne-wojcicki/

242 Geiger, G., et al. (2025, 14 October). *Surveillance secrets*. Lighthouse Reports. https://www.lighthousereports.com/investigation/surveillance-secrets/

243 CBN. (2025, 19 May). *Israeli companies thriving in Cyprus*. https://www.cbn.com.cy/article/108796/israeli-companies-thriving-in-cyprus

244 Sinai, A. (2020, 2 September). *Cyprus ready to serve as Israeli businesses' treasure island*. CTech. https://www.calcalistech.com/ctech/articles/0%2C7340%2CL-3847748%2C00.html

also has a favourable tax regime – the corporate tax rate is 12.5%, it avoids double taxation and offers a flexible regulation for business registrations and smooth processes.[245] The banking infrastructure is also solid, with advanced fintech services.[246]

Israeli companies that decide to land in Cyprus have the support of actors like the Israel-Cyprus Chamber of Commerce, with numerous members in the legal, tourist and real estate sectors, among sector.[247] There are also initiatives to promote the relocation of international technology to Cyprus's technology hub.[248] At the same time, the country has innovation centres and accelerators in Nicosia and Limassol, with appealing incubators and technology hubs for starts in the cybersecurity, fintech, arms and renewable energies sectors.[249] Added to these conditions is the absence of an effective regulatory framework to supervise the development or export of cybersurveillance items, a fact that allows these companies to operate under minimum control. Although the EU has a spyware regulation, Cypriot authorities have demonstrated they have little interest in its application.[250]

Opaque cybersecurity structures

Cypriot investigative journalist and former presidential adviser, Makarios Drousiotis, explains in his book *Mafia State* that in 2019 there were 29 Israeli-owned intrusive technology companies operating in Cyprus. According to the author, this implementation was based on tax optimisation, as well as the capacity to set up opaque corporate structures in the cybersecurity sector.[251]

The book highlights the case of **Circles** and **Intellexa**, two cybersecurity companies created by Tal Dilian, former commander of the Israeli military intelligence agency, Unit 8200. On the one hand, Dilian's first company, Circles, has been widely involved in the occupation of Palestine and global cyber espionage of activists,[252] while, on the other, Intellexa

245 PwC. (n.d.). *Cyprus: Corporate – Taxes on corporate income*. PwC Tax Summaries. https://taxsummaries.pwc.com/cyprus/corporate/taxes-on-corporate-income

246 The term *fintech* is an abbreviation for *financial technology* and refers to using technology to offer financial services in a more innovative way than traditional banks.

247 Israel-Cyprus Chamber of Commerce. (n.d.). *Members*. https://israel-cyprus.co.il/members/

248 Cyprus Tech Hub. (n.d.). Cyprus Tech Hub. https://www.cyprustechhub.com/

249 Spiro, J. (2022, 11 December). *Cyprus wants in on the Startup Nation game*. CTech (Calcalist Tech). https://www.calcalistech.com/ctechnews/article/bytr5hmoo.

250 Kenner, D. (2023, 15 November). *The spy, the lawyer and their global surveillance empire: How an Israeli cyber-surveillance kingpin and his attorney ex-wife exploited Cypriot loopholes to build one of the world's most notorious spyware firms*. International Consortium of Investigative Journalists (ICIJ). https://www.icij.org/investigations/cyprus-confidential/israeli-predator-spyware-cyprus-offshore-intellexa/

251 Ibid

252 Marczak, B., Scott-Railton, J., Prakash Rao, S., Anstis, S., & Deibert, R. (2020, 1 December). *Running in circles: Uncovering the clients of cyber espionage firm Circles*. The Citizen Lab, University of Toronto. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

was added to the US Department of Commerce Entity List due to its role in mass surveillance technologies, like Predator spyware, which were a threat to national security and the exercise of human rights.[253] Nevertheless, this technology continues to be used in numerous countries like Angola, Egypt, Oman, Saudi Arabia and Indonesia, among others.[254]

In Cyprus, Dilian created a network of interconnected companies to manage its capital and carry out international operations. This group of companies was led by Censura Ltd, originally managed by Dilian but since 2019, controlled by Sara Hamou, Dilian's ex-wife and business partner.[255] In Cyprus, Hamou collaborated with DJC Accountants, which supposedly had the mission to facilitate the opacity of the activities and property of Censura's customers.[256]

Hamou also helped other cybersecurity companies to establish themselves in Cyprus and Greece to boost their international expansion. In 2018, she created **Maravilhas Solutions Ltd** and among its customers there is a trail of subsidiaries owned by **Q Cyber Technologies**, a company created by the merger of NSO Group and Circles, for 'the supply and shipment of hardware equipment, its installation at customers' sites, and support and maintenance services.'[257]

Maravilhas Solutions Ltd facilitated EU projects by buying and sending equipment for Israeli companies. At the beginning of 2019, it purchased material for a Q Cyber project in Bulgaria and, in May, it spent nearly $120,000 on equipment that were subsequently sent to Belgium. In regard to this operation, Cypriot tax authorities received enquiries from another European country. This **tactic to use European companies to channel sales of Israeli equipment** facilitated access to the EU market, while potentially managing to evade export controls, as when equipment is reexported and combined with other goods, companies are often not obliged to declare the end user.[258]

253 Bob, Y. J. (2024, 5 March). US sanctions Israeli ex-intelligence officer, spyware CEO. The Jerusalem Post. https://www.jpost.com/israel-news/article-790354

254 May, P., & Šotová, Z. (2025, 20 August). *How a Czech supply chain feeds the global spyware machine*. VSquare. https://vsquare.org/how-a-czech-supply-chain-feeds-the-global-spyware-machine/

255 Kenner, D. (2023, 15 November). *The spy, the lawyer and their global surveillance empire: How an Israeli cyber-surveillance kingpin and his attorney ex-wife exploited Cypriot loopholes to build one of the world's most notorious spyware firms*. International Consortium of Investigative Journalists (ICIJ). https://www.icij.org/investigations/cyprus-confidential/israeli-predator-spyware-cyprus-offshore-intellexa/

256 Ibid

257 Ibid.

258 Ibid.

6. Luxembourg as a launch pad.

Far from considering Pegasus as outdated technology, companies like **NSO Group** continue to work to enhance and modify the properties of their products, to achieve its initial goal, which led the company: 'to develop a tool capable of penetrating a mobile device in a remote and undetectable manner'.[259] Niv Carmi, Shalev Hulio and Omri Lavie justify the importance of the technology they had developed by pointing out and claiming[260] from the beginning, that it was needed by European security: 'And then the police forces and the intelligence agencies of Europe told us: *"With the technology you developed, you could help us solve this problem"*'.[261] This element was the trigger that led them to set up NSO Group Technologies Ltd, on 25 January 2010.

Even though NSO develops a wide range of items, its best-known products is ***Pegasus***, a surveillance technology that, according to the company, is only sold to countries and international intelligence agencies.[262] In recent years, Pegasus has undergone continuous development: it has gone from requiring activation by a user to incorporating mechanisms of a zero-click-exploit nature and functionalities like the fabrication, modification and insertion of information inside the device.[263] This progressive sophistication has serious consequences, as **the software grants access and full and disproportionate control over mobile devices**. Without any interaction from the user, it is achieved by way of a zero-click cyber espionage mechanism – no clicks, no links, no downloads.

Although the company justifies its product for purposes of 'national security', available data show **thousands of cases in which this technology has been used against civil society actors that do not pose any kind of threat to the countries involved.**[264] These practices foster the construction of a potential crime; that is, the assumed existence of an ungrounded threat, a common mechanism in the use of surveillance technologies. In view of this situation, numerous international organisations have called for a ban on Pegasus.[265]

259 Ynet Global. (2019, 1 November). *Weaving a cyber web*. Ynetnews. https://www.ynetnews.com/articles/0,7340,L-5444998,00.html

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

261 The New York Times. (2022, 28 January). *The battle for the world's most powerful cyberweapon*. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

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

263 European Digital Rights (EDRi). (2025). *Spyware and state abuse: The case for an EU-wide ban* (Position paper, pp. 7–8). https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/

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

265 European Digital Rights (EDRi). (2025). *Spyware and state abuse: The case for an EU-wide ban*. https://edri.org/our -work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/

Although NSO Group Technologies Ltd is a private company incorporated and registered in Israel under the name 'NSO Group', it is used as an umbrella brand to designate the associated companies, of both an operational and financial nature, distributed around the world. NSO's corporate structure reflects the sector's rapid expansion and proliferation,[266] and warns about a currently worrying reality.[267] **With a total of 13 holding companies and 12 subsidiaries in multiple jurisdictions, the group operates through a complex and deliberately opaque structure, in which the companies often strategically change their names and broaden their activities in other jurisdictions to thus evade stricter regulations.**[268] For this reason, it is essential to analyse how it enters and acts in Europe, like a successful model of practices and logics that are reproduced in the surveillance market. A structural element of this type of company is the lack of transparency and effective accountability mechanisms as regards their activities and exports, a fact that makes it difficult to access verifiable information, including court proceedings initiated by victims targeted by Pegasus.[269]

The NSO's interconnected network of businesses has an especially significant presence in Luxembourg. Luxembourg, a founding member of the EU and euro zone, is firmly established as a strategic hub for international companies, thanks to the access to the European market, a flexible business structure, advanced technology structures, economic stability and a prominent specialisation in cybersecurity. It is also actively promoted in Israel as a business expansion destination.[270] At the time of writing this report, NSO had 19 registered companies, 11 of which shared the same corporate purpose.[271] This business structure broadens the action of these entities, granting them an instrumental nature, as it widens their scope of action without clearly defining the purpose. Moreover, not only do the companies share the same corporate purpose, they are also in the same physical location.[272]

---

266 The commercial brand 'NSO Group' is the exclusive property of the Israeli parent company NSO Group Technologies Ltd.

267 European Digital Rights (EDRi). (2025). *Spyware and state abuse: The case for an EU-wide ban*. https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/

268 SMEX. (2025). *Click, load, kill: A look into the cyberweapon industry in the WANA region* (pp. 28–45). https://smex.org/new-research-click-load-kill-a-look-into-the-cyberweapon-industry-in-the-wana-region/

269 ElDiario.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

270 Luxembourg Trade & Invest. (n.d.). *Your gateway to Luxembourg and Israel*. https://luxembourgtradeandinvest.com/our-international-network/ltio-tel-aviv

271 The corporate purpose of 11 of these companies is to be formally designated – by way of a contract, company agreement or decision of a competent body – to hold office or exercise duties in other companies, and act as general managing partners, purchase equity units in Luxembourg or abroad, and intervene in their management.

272 Of the 19 NSO Group companies in Luxembourg, 14 have the same registered address, while the remaining five are concentrated at another address.

The final report of the PEGA Committee of the European Parliament[273] concluded that the maintenance of NSO largely depends on the support of the companies based in Luxembourg. The report identified these entities as the group's European business centre, which facilitates its activity with a more flexible regulation both inside the EU and in third countries, and manages invoices, contracts and payments linked to its software.[274] **The EU's permissiveness towards the commercial spyware market does not only enable these companies to operate under a laxer regulatory framework than the one they would have if they operated from Israel, but it also endows the products they market from European territory with legitimacy.**

Standing out among the 19 companies linked to NSO Group and registered in Luxembourg are Osy Technologies Sàrl and Q Cyber Technologies Sàrl, due to both their ties with cybertechnology and their structural relevance within the Osy Technologies group. Osy Technologies Sàrl was created in February 2014 and was the group's first company in the country, followed by Q Cyber Technologies, constituted in January 2016 with Osy as the sole shareholder. Both companies are situated in the original heart of the group's European presence, which was subsequently consolidated through a fast company expansion: three in 2017, four in 2018 and five in 2020. Osy and Q Cyber maintain direct ties with NSO Group Technologies, even sharing the same board of directors for the first few years. Two of the NSO founders, Omri Lavie and Shalev Hulio, have a prominent presence.[275]

It is worth noting that when the management team and founder of NSO Group announced on 14 February 2019 that the British private equity firm, Novalpina Capital, had taken over control, the group immediately presented itself as a 'a cyber-technology company headquartered in Luxembourg', as a result of from 'the combination of Israeli and European cyber technology companies'.[276] This presentation did not just intend to reformulate the group's corporate identity under a more European appearance, it also responded to an institutional positioning strategy aimed at legitimising its activity within the European cybersecurity market and partially move away from its direct link with Israel, especially after the controversies generated by the use of Pegasus.

273 European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs. (2024). *Pegasus and equivalent surveillance spyware: Study/briefing* (IPOL_BRI(2024)761472). https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf

274 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* (pp. 397–399). https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

275 Lavie appears in new boards of directors of Luxembourg-based companies and Hulio in six, thus reinforcing the idea of an interconnected structure with unified management.

276 Amnesty International, Privacy International, & SOMO. (2021). *Operating from the shadows: Inside NSO Group's corporate structure* (pp. 2–27). https://www.amnesty.org/es/documents/doc10/4182/2021/en/

Following the Pegasus scandals in mid-2022, Shalev Hulio resigned as NSO Group's CEO and was replaced by Yaron Shohat. In January 2023, Hulio founded **Dream Security**[277] and on 7 November 2023, he announced a funding round while on duty in the Gaza Strip, where Hulio was serving as an Israeli reservist,[278] which he presented as a 'great message to the high-tech community and the people of Israel'.[279] Despite his attempts to separate himself from NSO Group, a dozen former senior officers and operational staff have followed him to Dream Security, where most of the personnel is based in Israel, even though there are also offices in Vienna and Abu Dhabi. The company's birth is surrounded by controversy, due to its links with the Israeli and international right wing, and especially the participation of Sebastian Kurz, ex-chancellor of Austria, as co-founder.[280]

WhatsApp vs NSO Group and the company's liability

In 2019, WhatsApp and its parent company, Meta, sued NSO Group in the United States. The Israeli company was using its servers to carry out cyber espionage with Pegasus, affecting over 1,400 users. This lawsuit represented a turning point in NSO group's reputational crisis.[281] During the process, in 2021, the US Department of Commerce added NSO Group to its list of sanctions, [282] as it considered that the Group's activities were a threat to 'national security'. Since then, NSO Group is banned from operating in the US market and its staff have restricted access to the country.[283] **Despite the economic and political impact of the sanction imposed by the US, the European Union has not adopted equivalent measures or established a common position on the Pegasus ban.**

In December 2024, a court in California determined that NSO Group had to pay damages to WhatsApp, due to violating federal and state laws on computer abuse and fraud,[284] impos-

277 Dream Security is a startup that provides cybersecurity defence solutions for critical infrastructure, with the public ambition to becomes 'the best AI-driven cybersecurity defence platform in the world'. Further information at: https://dreamgroup.com/about/

278 Biddle, S. (2024, 18 January). *In video from Gaza, former CEO of Pegasus spyware firm announces millions for new venture*. The Intercept. https://theintercept.com/2024/01/18/israel-nso-group-shalev-hulio-dream-security/

279 Elorduy, P. (2024, 21 January). *Los señores israelíes de la ciberguerra*. El Salto Diario. https://www.elsaltodiario.com/espionaje/senores-israelies-ciberguerra-pegasus-predator

280 Follow the Money [FTM]. (2025). *The talented Mr. Kurz: How Austria's ex-leader made it big in Israeli cyber industry*. https://www.ftm.eu/articles/spyware-sebastian-kurz

281 Perlroth, N., & Isaac, M. (2019, 29 October). WhatsApp says Israeli firm used its app in spy program. The New York Times. https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html

282 Kirchgaessner, S. (3 November 2021). *Israeli spyware company NSO Group placed on US blacklist*. The Guardian. https://www.theguardian.com/us-news/2021/nov/03/nso-group-pegasus-spyware-us-blacklist

283 Singman, B. (5 February 2024). *US announces new restrictions to curb global spyware industry*. The Guardian. https://www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions

284 WhatsApp Inc. vs NSO Group Technologies Ltd. (2024). *U.S. District Court for the Northern District of California, Case No. 4:19-cv-07123-PJH* (judgment / court order). https://www.documentcloud.org/documents/25467209-gov/

ing compensation of more than $168 million.[285] The proceedings also exposed once again the opacity of NSO Group and demonstrated that **it is the party that initially installs and extracts data from targeted devices, which is contrary to what the group had claimed** until then.[286] The court ruling has been applauded internationally as a key milestone in the battle against spyware.[287]

Strategic move for NSO Group's Americanisation

Albeit the relocation of dozens of workers following NSO Group's reputational crisis, the company continued to operate until November 2025, under the leadership of one of its founders, Omri Lavie. After 25 years of activity with over 22 customers just in Europe, including 12 of the 27 EU Member States,[288] in November 2025 there was a substantial change in management. For the first time, the founders, some of whom had been active since 2010, were no longer shareholders, which marked a turning point in the company's roadmap.

The new phase, led by US attorney, David Friedman,[289] coincides with the acquisition of the company by a United States investment group, some of whom are Israeli. The current executive chairman served as US ambassador to Israel during Donald Trump's first White House term and participated in the negotiation of the Abraham Accords. Friedman also stands out for his public interventions in defence of illegal Israeli settlements in the Occupied Palestinian Territory and promoting fundraising campaigns for this purpose. This change of management and ownership is in line with NSO Group's Americanisation trend.

In parallel, the change of management and ownership has implied making changes in three NSO Group companies registered in Luxembourg,[290] which are now managed by

285 The Record by Recorded Future News. (2025, 6 May). *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

286 Kirchgaessner, S. (2024, 15 November). *NSO – not government clients – operates its spyware, legal documents reveal*. The Guardian.
https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp

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

288 Benjakob, O. (2022, 9 August). *Pegasus spyware maker NSO has 22 clients in the European Union. And it's not alone*. Haaretz.
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

289 Benjakob, O. (2025, 9 November). *Ex-Trump ambassador to Israel David Friedman named NSO chairman, as spyware firm shifts to U.S. ownership*. Haaretz.
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

290 The three NSO Group companies in Luxembourg that changed their management are: NorthPole Newco, Osy Technologies and Q Cyber Technologies.

Ohad Shazar Shalem Schremer. The Israeli lawyer lives in the illegal Neve Daniel settlement, in Gush Etzion, within the Occupied Palestinian Territory, and forms part of the governing committee of a far-right settlers' association. **This new leadership reflects a corporate direction with colonial interests, which displays its connection with the Israeli government and the far right, in both Israel and at international level.**

7. Acquisition of European companies and rebranding in order to operate in the EU.

After the international scandal caused by Pegasus and the growing scrutiny of Israeli cybersecurity companies, some of these firms have **decided to change their brand, known as rebranding**,[291] **in order to land in Europe and access new markets**. Far from being an isolated phenomenon, it is a systematic practice that combines a change of name, affiliates constituted ad hoc, closure and creation of new companies and use of local intermediaries.

In this regard, some companies singled out as a result of their participation in cyber espionage operations against activists, journalists and political leaders have decided to purchase European companies or set up new businesses in Europe with different names to the parent company. In this way, t**hey seek to break away from the negative reputation and present themselves as legitimate actors in the cybersecurity and technology ecosystem**. The 2023 report of the European Parliament's PEGA Committee,[292] drawn up after the Pegasus scandal warned that different Member States, such as Greece, Cyprus and Portugal, were offering incentives to Israeli technology companies to relocate their businesses to these countries. According to Israeli sources, the three countries allegedly offered tax exemptions to Israeli technology companies and, in the case of Greece, it offered immediate citizenship.[293]

Consequently, the operation carried out by Israel-based companies to acquire European businesses can be interpreted as a calculated strategy to maintain access to the European market and its public funding mechanisms, using a corporate structure established within the EU. This practice reveals a regulatory fissure: **the purpose of the European De-**

291 Rebranding is a marketing strategy used to change or modify a brand's identity. By way of actions on its different elements, such as, name, logotype or even legally eliminating the company to create another one with the same people in charge, same field of work and products but with a different name and logotype.

292 European Parliament, Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). (2023, 22 May). *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 (2022/2077(INI))* (A-9-2023-0189). https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf

293 Gilead, A. (2023, 23 March). *Israeli entrepreneurs in talks over tech exodus*. Globes — Israel Business News. https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106

fence Fund (EDF) is boosting the EU's technology and military capacity but, in practice, it enables companies controlled by third countries to benefit from its resources.

Case study: Intracom Defense and Embention

Intracom Defense is a Greek company that,[294] since 1 July 2023, is owned by Israel Aerospace Industries (IAI),[295] a company owned by the government of Israel. This acquisition has enabled IAI to maintain access to the European market and funding, despite being a third-country company, outside the European Union and involved in military activities before and during the genocide in the Gaza Strip.[296]

This means that although **Intracom Defense** is registered and operating in Greece, IAI owns a controlling interest of 90.91%.[297] The EDF has granted millions of euros to this company, even though, in accordance with EDF regulations, beneficiary companies may not be controlled by a country not associated to this fund, as is the case of Israel.[298] Nevertheless,[299] **by purchasing the Greek subsidiary, the Israeli company has found an indirect path to continue participating in European defence and innovation programmes, avoiding de facto the possible restrictions or sanctions that would potentially prevent the company from doing it directly from Israel.**

Thanks to this, Intracom Defense, formally established in the European Union, has been selected to coordinate the ACTUS (*Advanced Capabilities & Certification for Tactical UAV Systems*) Project and participate in projects to enhance military technology capabilities, such as the Sentinel Project,[300] both funded by the European Union through the EDF.[301]

---

294 Intracom Defense S.A. (2024). *Annual report IFRS 31 December 2023*. https://www.intracomdefense.com/wp-content/uploads/2024/07/Annual-report-IFRS-31-12-2023-Defense-final-english.pdf

295 Israel Aerospace Industries (IAI). (2023, 9 May). *IAI has acquired Greek defense company Intracom Defense*. https://www.iai.co.il/press/iai-has-acquired-greek-defence-company-intracom-defence/

296 American Friends Service Committee. (n.d.). *Israel Aerospace Industries Ltd*. Investigate.info. https://investigate.info/company/IAI

297 Kourkoulas, I. (2023, 10 May). *Intracom Defense sells majority stake to IAI*. eKathimerini. https://www.ekathimerini.com/economy/1210573/intracom-defense-sells-majority-stake-to-iai/

298 European Commission. (n.d.). *List of third-country participation in the European Defence Fund (EDF)*. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/edf/guidance/list-3rd-country-participation_edf_en.pdf

299 Intracom Defense S.A. (n.d.). *National & European funded programs*. https://www.intracomdefense.com/national-european-funded-programs/

300 European Commission, Directorate-General for Defence Industry and Space. (2024). *SENTINEL project factsheet (EDF 2024)*. https://defence-industry-space.ec.europa.eu/document/download/3bb03680-d415-47a7-a470-3e0a781a298a_en?filename=FACTSHEET_EDF_2024_DA_ENERENV_EEMC_STEP_101224400_SENTINEL.pdf

301 ACTUS Project. (n.d.). *ACTUS – Advanced capabilities & certification of tactical UAV systems*. https://www.actus-project.eu/

The purpose of the ACTUS Project, worth €59 million, is to promote the technological development of European unmanned aerial systems used in military environments, known as RPAS (*Remote Piloted Aircraft Systems*) or tactical drones. En essence, it is a programme aimed towards designing, testing and certifying a new generation of European military drones, capable of operating in high-intensity conflicts and extreme operational conditions.

One of the project's technology partners is a Spanish company, **Embention**, headquartered in Alicante. It provides the development of avionics and flight control components, especially the Veronte autopilot and the Ground Control Station (GCS). The Alicante-based company had already collaborated with the Israeli military industry prior to participating in the ACTUS Project. According to information published on the specialised SUAS news portal in September 2020, Embention had previously worked with IAI on the development of an unmanned helicopter for heavy-lift operations, integrating its Veronte Autopilot navigation system.[302]

This cooperation, already documented in Embention's internal reports, demonstrates that the Spanish company and one of the leading defence companies in the State of Israel had had technology-related ties since at least 2017. That year, Embention's revenues reached €1.3 million, as a result of its collaboration with IAI on the Air Hopper project. The purpose of the project was to develop a small unmanned aerial vehicle capable of covering distances of up to 8 km, with a payload capacity of 150 litres and a minimum weight of 60 kg. As a result, the aircraft could transport a shipment to a specific location in the battle field, drop off the load and return to the base as quickly as possible, all while flying autonomously.[303] This relationship raises questions about knowledge transfer and the legitimacy of incorporating technology from the Israeli military complex into European defence programmes.

In spite of the project's technological dimension, Embention's participation also needs to be analysed from the perspective of risks associated to dual-use and corporate responsibility regarding human rights. UAV systems like LOTUS,[304] a project prior to ACTUS, also funded by the European Defence Industry Programme, which was coordinated by Intracom Defence, may have civil applications (inspection, logistics or rescue), but they may

302 sUAS News. (2020, 5 September). Embention and IAI cargo helicopter. https://www.suasnews.com/2020/09/embention-and-iai-cargo-helicopter/

303 Euronext. (2022, April). Embention Sistemas Inteligentes S.A. information document. https://live.euronext.com/sites/default/files/2022-04/EMBENTION%20SISTEMAS%20INTELIGENTES%20Information%20Document.pdf

304 Embention Sistemas Inteligentes S.A. (2021, 8 February). LOTUS program. A step forward in the UAV Formation Flight. https://www.embention.com/es/noticias/programa-lotus-un-paso-adelante-para-el-vuelo-en-formacion-de-uavs/

also be easily integrated into military and control contexts where civilians are killed. This vagueness places institutions and companies participating in this project under suspicion grounded on potential complicities, especially when the technologies are developed or come from contexts linked to the military industry and Israeli surveillance technologies, global leader in these types of systems that are continuously tested on Palestinian civilians (known as 'tested in combat').

According to an investigation by EU Observer, IAI's strategy to purchase of the Greek company has Europe's approval, as demonstrated with the words of a European defence expert, 'We need the Israeli know-how that we lack'. The expert goes on to say that this explains Intracom's manoeuvre. 'We want to develop our own loitering munitions [drones that can crash into targets], and we also want an "Israeli input" in this segment.'[305]

The rebranding process is also reinforced by the entry of European risk capital.[306] Funds like Forestay Capital have closed multi-million operations expressly aimed towards funding Israeli companies and facilitate their expansion in Europe,[307] while global firms such as Accel have raised funds to invest in artificial intelligence in both Europe and Israel.[308] This funding not only boosts business expansion, it also acts as a reputational validation mechanism. The investment of funds like Forestay Capital or Accel transmits an image of solvency and standards compliance, thus helping to consolidate a message of 'innovative and responsible technology'.

The cases of Circles, affiliated with NSO, dedicated to telephone interception, or QuaDream,[309] an Israeli spyware firm that closed down in 2023 after exposure[310] by international media, illustrate how these companies attempt to reinvent themselves and reappear under new structures or with new affiliates in Europe. In conclusion, **the acquisition of European companies and rebranding of Israeli military and arms control technology companies is not limited to a simple change of name, but is made up of a comprehensive strategy aimed towards sanitising their reputation, gain institutional legitimacy and attract European investment.**

---

305 Maggiore, M., Miñano, L., & Maltepioti, K. (2025, 6 June). *European Defence Fund millions benefiting Israeli state-owned drone manufacturer*. EUobserver. https://euobserver.com/eu-and-the-world/ar201316e5

306 European venture capital is a form of financing aimed at young, innovative companies with high growth potential in Europe, in exchange for an equity stake in the company.

307 Gilead, A. (2024, 3 July). *Forestay Capital raises $220 million to invest in AI and SaaS startups in Israel and Europe*. Calcalist Tech (CTech). https://www.calcalistech.com/ctechnews/article/h1jur3mdr

308 Mukherjee, S. (2024, 13 May). *VC firm Accel raises $650 mln to invest in AI, cybersecurity startups*. Reuters. https://www.reuters.com/business/finance/vc-firm-accel-raises-650-mln-invest-ai-cybersecurity-startups-2024-05-13/

309 Bill Marczak, John Scott-Railton, Astrid Perry, Noura Aljizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak i Ron Deibert, *"Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers"* (11 April 2023), Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

310 Kabir, O., & Orbach, M. (2023, 16 April). Offensive cyber company QuaDream shutting down amidst spyware accusations. Ctech. https://www.calcalistech.com/ctechnews/article/hy78kiym2

8. Access to the European Union through funding programmes.

In September 2009, Javier Solana, who, for a decade, was High Representative for the Common Foreign and Security Policy (CFSP) of the European Union, affirmed before an audience in Jerusalem that, 'Israel is, allow me to say, a member of the European Union without being a member of the institutions'.[311] More recently, in April 2023, during the commemoration of the 75th Anniversary of the State of Israel, President of the European Commission, Ursula von der Leyen, declared, 'Europe and Israel are bound to be friends and allies. Your freedom is our freedom'.[312]

Later, in 2025, during the escalation of the violence in the Gaza Strip, Dimiter Tzantchev, EU Ambassador to Israel, commented that, 'Israel's high-tech leadership and the EU's strong research base make Horizon Europe a win-win'.[313]

These affirmations are not anecdotical; they synthesise **a relationship assumed to be natural and strategic by European institutions, and help understand the preferential treatment received by Israel in different areas of EU policy.** One of the most relevant, is its access to European research and development (R&D) funding. Since 1996, Israel has held the status of 'associated country", a category that allows it to participate in successive EU Framework Programmes for Research and Technological Development in conditions comparable to those of Member States.[314]

At present, Israel figures as an associated country in the Horizon Europe programme (2021-2027), a fact that enables Israeli companies to participate in the same conditions as companies based in EU Member States. **Even though the Horizon programme centres on civil research, the Israeli institutions and companies that receive European public funds maintain strong ties with the country's defence and/or cybersecurity sector**, to the point that they even form part of this same security and defence architecture. In this regard, between 2008 and when this report was written, **the European Union had granted Israel €70 million in specific security projects.**[315] The result is that arms and cybersecurity

311 Hayes, B. (2010, 17 March). Should the EU subsidise Israeli security? POLITICO. https://www.politico.eu/article/should-the-eu-subsidise-israeli-security/

312 Ursula von der Leyen, 'Statement on the 75th Anniversary of the Establishment of the State of Israel,' European Commission (27 April 2023).

313 Diplomacy.co.il. (2025). *Diplomatic Magazine #83 – Frontpage*. https://diplomacy.co.il/diplomatic-magazine/83-frontpage

314 European Commission. (2024). *International cooperation with Israel in research and innovation – Association to Horizon Europe*. https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/association-horizon-europe/israel_en

315 Open Security Data Europe. (n.d.). *Israel (IL)*. https://opensecuritydata.eu/countries/il?p=1&limit=25

technology manufacturers like **Elbit Systems** or **Israel Aerospace Industries (IAI)** are benefitting from public funds from the Horizon programme.[316]

During the first quarter of 2025, Israel Innovation Authority announced that between 2021 and 2024, Israeli investigation teams and companies had received €1.1 billion from Horizon Europe grants, thus reaffirming Israel's strategic position as regards research, innovation and technology in the EU.[317] Since October 2023, this programme has granted €475 million to Israeli companies and projects, including startups managed by former members of the Israeli army, specifically from cybersecurity units.[318] Indeed, according to a report published in 2018, 80% of the 2,300 people who founded the hundreds of cybersecurity firms existing in Israel were veterans from army intelligence units.

As affirmed by Shir Lever, expert in the economy of he Israeli occupation, military and security industry, and arms trade, **a large part of European funding for military and security matters received by Israel is channelled 'through technology institutes and universities, using these institutions to mask corporate military links and calling the exchanges scientific cooperation'.**[319]

In some of the active Horizon projects,[320] there are companies that have had a fundamental role in the Gaza Strip genocide, such as **Rafael Advance Systems**, one of Israel's largest arms manufacturers that develops missiles, drones and other defence systems for the Israeli army. It would seem that these practices do not affect the company's business relationships, as recently, through the EuroSpike consortium[321] and with the support of defence companies, Rheinmetall and Diehl, it won a contract with the German government worth €2.5 billion.[322]

316 Statewatch. (2024, 7 February). *Palestine: 300 academics call for halt to EU research funding that violates international law*. https://www.statewatch.org/news/2024/february/palestine-300-academics-call-for-halt-to-eu-research-funding-that-violates-international-law/

317 Innovation Israel – Israel Innovation Authority. (2025, 19 March). *Israeli researchers and companies secure over €1.1 billion in Horizon Europe grants, cementing global leadership in innovation*. https://innovationisrael.org.il/en/press_release/1-1-billion-to-israel-from-horizon-europe-in-2021-24/

318 Carter, B. (2025, 2 September). *EU science grants funnel millions to Israeli military-linked tech startups amid Gaza genocide*. Newstarget. https://www.newstarget.com/2025-09-02-eu-funnels-millions-to-israeli-military-linked-tech.html

319 Interview with expert, Shir Hever. 24 October 2025.

320 UnderSec Project. (n.d.). *Consortium*. https://undersec-project.eu/consortium

321 Leading German defence consortium founded in 2004 through the collaboration of Diehl Defence, Rheinmetall Electronics and Rafael Advanced Defense Systems.

322 Global Defense Corp. (2025, 24 October). *EuroSpike awarded $2.5 billion contract to produce Rafael's Spike missile for Germany*. https://www.globaldefensecorp.com/2025/10/24/eurospike-awarded-2-5-billion-contract-to-prodcue-rafaels-spike-missile-for-germany/

According to information collected by Transnational Institute, since 7 October 2023, the EU has approved 130 Horizon Europe research projects with Israeli participants, which have received a total of €126 million. At least two of these projects directly fund **Israel Aerospace Industries (IAI)**, which receives nearly €640,000.[323]

According to Shir Hever, most of the Horizon Europe grants, even those reserved for Israeli universities, end up impacting the country's cybersecurity and military industry, as Israeli universities often work closely with the military and defence industry.

The European Union has other research and innovation programmes that offer funding. For example, the European Defence Fund (EDF) funds R&D projects for defence and security, thus favouring the participation of companies and technology centres that contribute to Europe's defence autonomy. If during the first stage, the EDF especially focused on strengthening borders, in the logic of the so-called 'Fortress Europe',[324] it has currently progressed towards applying a strictly military focus. Since its creation, the EU has invested over €3 billion in military R&D projects.[325]

EU funding received by Israel **ends up becoming a way to legitimise a regime that uses technology innovation to support a colonial system of occupation and military control over the Palestinian population, disguising it as scientific cooperation and shared progress**. This collaboration has generated strong internal divisions within the European Union and widespread rejection from the civil society, human rights NGOs and diverse Euro-MPs, who denounce the contradiction between the values proclaimed by the EU and its real funding practices.

To respond to this pressure, in July 2025, the European Commission proposed partially suspending the association agreement between the EU and Israel, which enabled it to participate in the Horizon Europe programme. It was a very limited proposal as it only affected Israeli entities and companies linked to the European Innovation Council Accelerator, the segment that offers support to startups and dual-use technology projects, such as artificial intelligence, drones and cybersecurity – especially sensitive sectors due to their military potential.[326]

---

323 Ní Bhriain, N., & Akkerman, M. (2024, 4 June). *Partners in crime: EU complicity in Israel's genocide in Gaza* (Policy briefing). Transnational Institute. https://www.tni.org/files/2024-06/Partners-in-Crime-Report-TNI-web.pdf

324 Akkerman, M. (2018). *Expanding the fortress: The policies, the profiteers and the people shaped by EU's border externalisation programme* (Report). Transnational Institute. https://www.tni.org/es/publicaci%C3%B3n/expandiendo-la-fortaleza

325 Calvo, J., Meulewaeter, C., & Font, T. (2025, 10 September). *Informe 74: L'economia de la guerra*. Centre Delàs d'Estudis per la Pau. https://centredelas.org/wp-content/uploads/2025/09/informe_74_LEconomia-de-la-Guerra_DEF_CAT_compressed.pdf

326 Weinreb, G., & Uni, A. (2025, 29 July). *European Commission recommends sanctions on Israel*. Globes. https://en.globes.co.il/en/article-european-commission-recommends-sanctions-on-israel-1001517402

The Commission's proposal was the first time that an EU institution had considered imposing some sort of sanction on Israel. However, the proposal failed to receive the necessary support from EU Member States for its approval and, at the moment, Israel's participation in the Horizon Europe programme is still in force.[327]

9. Barcelona as a technology hub of cybersecurity companies.

According to the report published in May 2025 by ACCIÓ, the Agency for Business Competitiveness of the Government of Catalonia, titled 'Cybersecurity in Catalonia', the sector is undergoing a notable and sustained expansion. At present, 557 companies form part of this ecosystem, with an average annual growth of 7.9% and an overall increase of 58.2% compared to 2018.[328]

In this regard, Catalonia, particularly the city of Barcelona, has become firmly established as an attractive territory for investing in cybersecurity. In the last five years, Direct Foreign Investment (DFI) projects in this field have doubled, going from 6 to 12, while the investment volume has multiplied by nine, reaching €207 million. The explanation for this growth is partly due to the presence of a solid technology business network: 36% of the 160 international technology hubs established in the territory is made up of cybersecurity companies. At European level, **Catalonia occupies the fifth position in the Horizon Europe (2022-2024) funding programme, with 15 active projects and an investment of €11.3 million**, a fact that strengthens its position as a European pole of attraction for cybersecurity innovation and development.

Barcelona is home to numerous cybersecurity startups, consultancies and affiliates of international companies that are engaged in the development of cybersecurity solutions. Moreover, **the Mobile World Congress and Barcelona Cybersecurity Congress have reinforced this positioning, becoming strategic meeting points for the sector, especially for companies in the Israeli cybersecurity ecosystem.**

327 Euronews. (2025, 30 July). *EU fails to agree Israeli suspension from research fund over Gaza*. https://www.euronews.com/my-europe/2025/07/30/eu-fails-to-agree-israeli-suspension-from-research-fund-over-gaza

328 ACCIÓ – Agency for Business Competitiveness, Government of Catalonia. (n.d.). *La ciberseguretat a Catalunya*. https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya#blocMaterials_b62ef8b5-b28b-11e8-92dc-005056924a59

The role played by ACCIÓ,[329] is fundamental to understand the growth of the sector in Catalonia and Barcelona, and the appearance of cybersecurity companies linked to Israel. **ACCIÓ has considered the State of Israel as a highly innovative economy, particularly in the technology sector**. In 2015, ACCIÓ opened an offshore office in Tel Aviv, in order to foster trade contacts and business collaboration. To comprehend the strong ties between ACCIÓ and the State of Israel. In 2017, Israel was included among the eight strategic territorial areas defined by the Catalan agency, thus demonstrating the will to strengthen the economic and technological links between both territories. In May 2025, thanks to the pressure resulting from the public debate on the relationship with Israel and the sustained pressure from the Catalan civil society, especially from collectives and entities committed to defending the Palestinian population's rights, particularly *Coalició Prou Complicitat* [End Complicity Coalition], the Government of Catalonia announced that it had closed the trade office in Tel Aviv.[330]

As we mentioned above,[331] the trade missions included as part of ACCIÓ's internationalisation programme for Catalan companies, at the time with an office operating in Tel Aviv, meant that the potential for new markets could be explored in the field. In 2016, ACCIÓ organised a trade mission made up of Catalan companies to participate in Israel Homeland Security, one of the largest cybersecurity exhibitions in the world, with the purpose of creating cooperation ties in the sector. ACCIÓ remunerated each one of the Catalan companies that participated.

There is still no type of information about the cybersecurity companies that met with the delegation of Catalan companies, nor is there any information about the specific result of the experience, which shows a considerable lack of transparency in the management of these contacts and assessment of the possible risks associated to their activity. This opacity is especially worrying if it is borne in mind that a large part of these Israeli cybersecurity companies operate in technology sectors linked to the military industry where, there is a high risk of human rights violations, as has already happened.

In this regard, **in recent years a relevant number of cybersecurity companies linked to the Israeli ecosystem has chosen Barcelona to set up companies and operate in the EU economic market**. It is not a spontaneous phenomenon; it responds to regulatory and

329 ACCIÓ is a public agency that is part of the Department of Business and Knowledge of the Government of Catalonia. Its purpose is to improve the competitiveness of Catalan businesses through different services and grants to facilitate technology transformation, strengthen business innovation, support startups and boost the internationalisation of the Catalan business sector.

330 Toro, M., Esteve, M., & Sanz Guerrero, V. (2025, 21 May). *El Govern tanca la seva oficina a Israel per la situació a Gaza*. ARA. https://www.ara.cat/politica/govern/govern-tancara-seva-oficina-tel-aviv-situacio-gaza_1_5386180.html

331 Observatory for Human Rights and Business in the Mediterranean (ODHE), NOVACT, & SUDS. (2024, 17 April). La inACCIÓ de Catalunya davant la vulneració dels drets humans del poble palestí. https://www.odhe.cat/informe-la-inaccio-de-catalunya-davant-la-vulneracio-dels-drets-humans-del-poble-palesti/

reputational incentives to overcome the potential sanctions imposed on Israeli companies following the genocide, as well as open new business opportunities in Europe, among other factors. Another influencing feature is that the State of Israel has established a more restrictive legal framework when it comes to granting licences to export spyware to other countries following the scandals related to NSO Group, encouraging companies to move abroad.[332]

In December 2024, **an article in the Haaretz newspaper revealed that Barcelona was turning into an emerging hub for Israeli cybersecurity companies and spyware development specialists.**[333] The article identified three teams of Israeli hackers, specialised in finding vulnerabilities and weaknesses in mobile devices that operate from Barcelona, to be able to access the content of these devices.

Some of the companies and initiatives related to the Israeli cybersecurity ecosystem (they originate in Israel or employ Israeli staff) identified to be operating in Barcelona are: Palm Beach Networks, Epsilon, Paradigm Shift, Variston and Blue Ocean.[334]

Actually, one of these companies, **Epsilon**, **is the organiser of Offensive, a meeting between companies specialised in cyber espionage and spyware that took place in Barcelona in January 2026.**[335] The event developed through closed-door meetings – marked by an opacity that made it easier for the activities of these companies to evade control and transparency – and was attended by companies linked to selling intrusive surveillance technologies to countries.[336] From a democratic and human rights perspective, if this ecosystem prospers in Barcelona, it turns the city into an attractive European platform for enticing a type of business activity that violates human rights.[337]

332 Franceschi-Bicchierai, L. (2025, 13 January). *How Barcelona became an unlikely hub for spyware startups*. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

333 Benjakob, O. (2024, 26 December). *Israeli hackers flock to Barcelona as spyware industry shifts*. Haaretz. https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000

334 Franceschi-Bicchierai, L. (2025, 13 January). *How Barcelona became an unlikely hub for spyware startups*. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

335 Offensive Barcelona. (n.d.). *About / Organization information*. https://offensive-bcn.com/org.html

336 Pareja, P. (2026, 15 January). *La reunión de ciberespías en Barcelona preocupa a las ONG: "Anima a más empresas de 'spyware' a venir a Europa"*. elDiario.es. https://www.eldiario.es/catalunya/reunion-ciberespias-barcelona-preocupa-ong-anima-empresas-spyware-venir-europa_1_12910236.html

337 Pareja, P. (2025, 18 December). *Sol, marisco y 'spyware': una empresa israelí cita a ciberespías de todo el mundo a un encuentro secreto en Barcelona*. elDiario.es. https://www.eldiario.es/catalunya/sol-marisco-spyware-empresa-israeli-cita-ciberespias-mundo-encuentro-secreto-barcelona_1_12846798.html

The CEO of Epsilon, Jeremy Fetiveau,[338] was the key person in the organisation of the event; he used to work for one of the largest companies in the US military industry, L3 Harris.[339] However, other companies appear with an organising role, such as Bugscale, Epieos, Interrupt Labs, Randorisec, Paradigm Shift and Radiant Research Labs, the latter with connections with NSO Group and the Israeli Ministry of Defence.[340]

The idea of Barcelona as a 'cybersecurity technology hub' is not an isolated case; it is the European materialisation of a business model that exploits vulnerabilities and erodes fundamental rights. The fact that cybersecurity companies, members of a sector where mass surveillance practices and human rights violations are constant, continue to operate in Europe without great restrictions and especially in Catalonia, clearly shows the lack of effective control and government accountability mechanisms.

Case study: Palm Beach Networks

Palm Beach Networks is a company headquartered in Barcelona that appeared in mid-2024 when it was made known that Alexey Levin, a former researcher at NSO Group, was recruiting staff for Palm Beach.[341] The company specialises in the development of zero-day exploits and spyware.[342]

According to first-hand accounts collected by the specialised portal, TechCrunch, the contracting process was characterised by a high level of secrecy and lack of transparency.[343]

Since then, **Palm Beach Networks has rebranded on multiple occasions, copying the tactics used by companies such as Candiru to hide its operations.** Until May 2023, Palm Beach Networks was called Defense Prime Inc, and in mid-June 2023 a company named Head and Tail initiated its activity in Barcelona. Curiously, one year later, in June 2024, Palm Beach Networks was dissolved and, according to the article by TechCrunch, both

338 MISP Project. (n.d.). *Surveillance vendor*. https://misp-galaxy.org/surveillance-vendor/

339 Franceschi-Bicchierai, L. (2025, 13 January). *How Barcelona became an unlikely hub for spyware startups*. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

340 Intelligence Online. (2025, 13 January). *Former NSO stars behind vulnerability research firm Radiant Research Labs*. https://www.intelligenceonline.com/middle-east-and-africa/2024/09/06/former-nso-stars-behind-vulnerability-research-firm-radiant-research-labs,110283294-art

341 Franceschi-Bicchierai, L. (2025, 13 January). *How Barcelona became an unlikely hub for spyware startups*. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

342 *Zero Day Exploits* are a type of vulnerability that has just been discovered and for which no solution or patch yet exists. The main threat lies in the fact that, until this corrective patch is released and users install it on their systems, attackers have free rein to exploit the vulnerability and take advantage of it.

343 Franceschi-Bicchierai, L. (2025, 13 January). How Barcelona became an unlikely hub for spyware startups. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

Defense Prime and Palm Beach Networks are linked to Barcelona-based Head and Tail, which has the same managers as those mentioned above.

These companies define their corporate purpose as the design, development, programming, implementation, maintenance, update, technical support, acquisition, license, sale and marketing of software.[344]

In this company's setting up process in Barcelona, a number of key names appear. One person called Sai Gopal figures as an authorised signatory of Head and Tail in the Spanish trade registers[345] and, at the same time, someone with an identical name figured as the treasurer of Defense Prime in the trade registers of Florida, in the United States of America. The company's trade registers also indicate that Alexey Levin, the technology director who Palm Beach Networks tried to hire, is now the director of Head and Tail.[346]

The company is currently undergoing a process of expansion and the different professional profiles they are looking for can be verified on the corporate website.[347]

Besides this company, **we find a conglomerate of companies that group together people with the same names.** In this regard, **Apex Software Solutions** (previously known as CyberNinja SL) with its registered office in Passeig de Gràcia where, since June 2025, Alexey Levin, Sai Gopal and Yosef Aloni all figure as joint and several attorneys.[348]

The fact that Alexey Levin, a former researcher at NSO Group, is currently hiring staff for a Barcelona-based company is a clear indication of the ease with which the city has become an ideal place for the establishment of cybersecurity companies, including those linked to others with a background of fundamental rights violations, as in the case of NSO. At the same time, it is extremely worrying, since it makes evident the **lack of control and supervision mechanisms for these kinds of activities, as well as the risk of firmly establishing Barcelona as a development centre of dual-use technologies, with both civil and military applications, without an ethical or political reflection on the consequences.**

344 DatosCIF. (n.d.). *Headandtail Services S.L.* https://www.datoscif.es/empresa/headandtail-services-sl

345 Información Corporativa. (n.d.). Headandtail Services S.L. https://infonif.economia3.com/ficha-empresa/headandtail-services-sl

346 North Data. (n.d.). *Headandtail Services S.L.* https://www.northdata.com/Headandtail+Services+SL,+Barcelona/NIF+B13946488

347 Headandtail Services S.L. (n.d.). *About us*. https://headandtail.io/about.html

348 DatosCIF. (n.d.). *Cyber Ninja S.L.* https://www.datoscif.es/empresa/cyber-ninja-sl

Conclusions and recommendations.

Israel continues to use Palestine as a 'laboratory' for testing armament and military technologies. Israel has tested state-of-the-art weapons on the Palestinian population, including AI-based systems that increase lethal precision without any ethical, legal or human consideration. This 'laboratory' is the epicentre from where these technologies, knowledge and practices are transferred and exported to other parts of the world, feeding armed conflicts and reinforcing the repression of political dissent. For example, the externalisation of migration management, the repression and criminalisation of protests, and the growing use of risk assessment tools reproduce in European territory, government techniques previously tested on colonised populations.

Based on the mapping of the main Israeli accomplice companies, with protagonism or the technology that has been used in the Palestinian genocide and their funding structures, the study has traced their entry channels into Europe. The military and security relationships between the EU and Israel are particularly relevant. The EU uses Israeli technology to advance its rearmament plans, but it also needs to sell its armament production to this country. It is essential to stop these business relationships, especially when they concern armament and security, to end Israeli colonialism, occupation, apartheid and genocide against Palestinian people.

This research has identified nine European gateways used by Israeli defence tech companies to enter the territory. Each one reveals jurisdictions, mechanisms and conditions that facilitate this penetration, illustrated by specific cases of companies and alliances between European political and economic actors. These gateways show how **a long time ago, Israeli oppressive technology know-how found ways to penetrate the European Union market, which has increased after the genocide against Palestinians in the Gaza Strip**. The study also points out future trends and poles of attraction at the development stage that could be exploited in oncoming years by the Israeli military-industrial complex. Some of these trends are summarised below.

First of all, **none of the gateways would exist without the facilitation of the governments of Israel and the EU**. While countries like Cyprus, in their quest to find foreign investment, hope to become a Startup Nation inspired on the Israeli model, others like Germany want Israeli military technology to rearm themselves and expand their military industry. Israel supports its companies through political and economic mechanisms such as the creation of embassies in NATO's technology hubs (like Estonia), organisation of international cybersecurity or technology fairs, or the establishment of agreements between internationalisation and innovation agencies with European counterparties. **In parallel, lobbies and economic actors such as chambers of commerce help create favourable narratives and systematically influence to facilitate these agreements**, while they try to conceal the role played by these companies in genocide, apartheid and occupation policies against the Palestinian population.

Secondly, **the expansion of NATO and European rearmament plan act like a pole of attraction for hundreds of Israeli companies in the tech security and military industry**. Armament and technology testing in Ukraine, as well as the establishment of military alliances in this country, open the door to contracts with NATO. These contracts ensure interoperability and compliance with European and transatlantic standards, essential requirements to access more contracts in these countries. Within this context, companies linked to the genocide against the Palestinian people set up affiliates, acquire companies or create armament and technology development plants in the principal European capitals.

Thirdly, **violence in the region, started by Israel's attacks, has led to the relocation of Israeli technology companies, including the migration of professionals in the sector, to other European countries**. Specifically, to cities with technology hubs like Berlin, London, Paris, Tallinn and Barcelona. These economic actors often blend in with local companies, change their names or create opaque structures in order to continue operating. Cyprus is a paradigmatic case of deregulation in the cybersecurity sector, which has allowed Israeli companies to integrate capital obtained from illicit activities into Europe's formal economic system, as well as market extremely intrusive software with absolutely no governmental control; while in Catalonia, former employees of companies like NSO Group have fostered hiring professionals for Israeli startups that operate in Barcelona, replicating business models and similar practices as those used in Palestine.

Fourthly, **the expansion of the defence tech sector would also be impossible without the dynamics of financial capitalism**. International financial institutions, banks, governments, insurance companies, auditors and investment agencies ensure the necessary economic flow for the growth of these companies. In parallel, some European countries reduce administrative barriers and taxes to attract this foreign investment. Luxemburg is an exemplifies this model, providing a landing area for Israel's largest mass surveillance companies, such as NSO Group, and creating an interconnected business network that makes traceability and governmental control difficult. Other, smaller, companies access funds from the Israeli government or European research programmes to develop prototypes, with the purpose of increasing the funds they receive through international investment rounds or loans from large European and Israeli banks.

The European Union may not only be understood as a passive receiver of technologies developed in contexts of genocide, occupation or structural violence, but also as an actor that, by way of regulatory, financial and narrative frameworks, contributes towards the consolidation of a comprehensive techno-security regime. This dynamic, inserted into broader securitisation processes and the entanglement between external colonial logics and internal control systems tends to place security as the main guiding principle of public action, even when it comes into tension with human rights and countries' international obligations.

It is worth noting that this security-based narrative, led by the development and implementation of surveillance technologies, brings to light an alarming contradiction as regards cybersecurity. These technologies often depend on exploiting vulnerabilities in digital devices and infrastructure, instead of correcting them. In this regard, **they contribute towards what is known as 'vulnerability market'[349] in which security errors are marketed and kept active for operational uses**. In the absence of solid regulatory frameworks and effective control mechanisms over these practices, the EU may be indirectly favouring the persistence of these vulnerabilities within its own digital environment. This generates a paradoxical effect, technologies justified for the sake of security may, at the same time, increase the risks for the internal security, privacy and integrity of digital infrastructures. In practical terms, the exploitation of these vulnerabilities could leave devices and systems more exposed to unauthorised accesses, increasing the capacity to attack and also affecting systems used by public authorities and critical actors.

In this context, **in accordance with international law and the European Union's own treaties, the EU its Member States are obliged to prevent genocide, war crimes and crimes of lese-humanity, and not contribute either directly or indirectly**. This duty does not only require exterior action, but also internal coherence through administrative, contracting, financial and tax measures aimed towards preventing companies involved in international crimes from accessing public contracts, funding or other financial benefits within the EU. In the absence of these safeguards, a form of complicity or assistance, prohibited by international law, could be established.

Within this framework, the practical recommendations for dealing with these issues are addressed to political, regulatory and economic authorities at European, Member State and local level.

349 Roberts, J., Herr, T., Bansal, N., Messieh, N., Taylor, E., Le Roux, J., & Gelava, S. (2024). *Mythical beasts and where to find them*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them/

Recommendations

1. Ban and exclusion from public contracts.

In regard to the future reform of the EU Public Procurement Act – as part of the review of the guidelines in force – we recommend that the European Commission and European Parliament incorporate clear and binding exclusion clauses to prevent the participation in tenders of companies involved in serious human rights violations, contexts of illegal occupation or mass surveillance technologies, placing special attention on the Occupied Palestinian Territory. This involvement should be proven through verifiable sources – including mechanisms of the United Nation,[350] such as the databases of companies linked to Israeli settlements as well as documented evidence provided by civil society organisations. The application of these clauses should be accompanied by clear guides and verification, monitoring and control mechanisms throughout the entire term of the contract.

2. Enhancement of the Regulation on dual-use products and technologies.

We recommend reinforcing the application of Regulation (EU) 2021/821, acknowledging its current limitations on the prevention of misuse in contexts of serious human rights violations. The planned evaluations (2026 and 2028) should address these deficiencies and result in binding reforms. In particular, it would be necessary to reinforce the definition of risk, establish harmonised criteria between Member States and prevent exports that are at risk of being used in repression or mass surveillance, applying the precautionary principle. Likewise, measures should be incorporated to prevent control evasion (including reexports and intermediation) and enhanced due diligence obligations. Finally, we recommend extending the scope of the regime to technologies and companies not strictly military that, in contexts such as Palestine, could contribute towards committing serious breaches of international law.

3. Ban on commercial spyware.

The European Commission must prohibit the development, production, commercialisation, sale, export and use of spyware by private companies and governmental agencies. Likewise, it must also ban the trade of vulnerabilities and exploits for any purpose other than enhancing the security of systems and infrastructures.

4. Specific sanctions and financial restrictions.

We recommend that the European External Action Service promote the adoption of specific sanctions, within the Common Foreign and Security Policy framework, against the

350 United Nations Human Rights Council, Office of the High Commissioner for Human Rights. (2025, 26 September). *Database of all business enterprises involved in the activities detailed in paragraph 96 of the report of the Independent International Fact-Finding Mission... (A/HRC/60/19)*. https://www.ohchr.org/en/documents/thematic-reports/ahrc6019-database-all-business-enterprises-involved-activities-detailed

State of Israel and against companies and entities – including third-country nationals – linked to serious breaches of international law in Palestine, to be consistent with the provisional measures established by the International Court of Justice and the report by the UN Special Rapporteur. These measures should include the freezing of assets and other targeted economic restrictions, using similar instruments implemented in the United States as a reference. We likewise recommend limiting access to the European market, including the prohibition to establish, register and participate in public tenders and business promotion activities, ensuring harmonised application between Member States.

5. Full arms embargo.

We recommend that the Council of the European Union, within the Common Foreign and Security Policy framework and at the proposal of the European External Action Service, adopt a full arms embargo against Israel with a harmonised application by Member States. This measure should include a ban on the export, transfer, transit and technical assistance of military material and associated technologies, as well as dual-use components and technologies that have a possible military application. Likewise, it should incorporate mechanisms to prevent evasion (including reexports and intermediation) and monitoring system that ensure effective compliance at European level.

6. Control of illegal financial flows.

We recommend that the EU enhance the application of existing instruments for controlling illegal financial flows, in order to intensify the supervision of investments and operations linked to companies – especially as regards the military, defence tech and security technology sectors – associated to high risks of breaching international humanitarian law and international human rights law, including operations linked to the Occupied Palestinian Territory. These risks should be identified through a focus based on multiple verifiable sources – such as United Nations mechanisms and evidence from the civil society – used as involvement indicators and not automatic risk classifications. It is also necessary to reinforce the coordination and harmonisation of supervision criteria at European level.

7. Enhanced due diligence.

We recommend demanding European financial entities, investors and insurance agencies to apply enhanced due diligence in operations involving companies that operate in contexts of armed conflict or occupation – specifically including, the Occupied Palestinian Territory – especially in military, defence tech and security technology sectors. This diligence should include the identification of end beneficiaries, value chain and end-use analyses and the detection of opaque corporate structures, with the purpose of preventing direct or indirect contribution to serious breaches of international humanitarian law and international human rights law. It should be based on reliable sources, including United Nations mechanisms and documented evidence provided by civil society organisations.

8. Mandatory transparency in military and technology agreements.

Establish legal obligations regarding transparency and independent auditing in all trade, research and development agreements between European actors and Israeli companies of the military, defence tech and security technology. This includes the periodical publication of information about contracts, investment and technology transfers, with clear criteria on human rights due diligence. The system should integrate mechanisms for detecting rebranding, the creation of paper companies or the acquisition of European companies used to evade traceability and dilute responsibilities, ensuring that transparency is not replaced by opaque structures.

9. Exclusion from European research and innovation programmes.

We recommend enhancing the application of the Early Detection and Exclusion System (EDES)[351] to explicitly include criteria relating to serious human rights violations, to ensure that military, defence tech and security technology companies involved in contexts of occupation, apartheid or genocide are unable to access public R&D funds, including programmes like Horizon Europe. This would require taking the grounds for exclusion beyond bad financial or administrative conduct, incorporating evidence from United Nations mechanisms and other verifiable sources. Likewise, it would be necessary to guarantee continuous review and monitoring mechanisms throughout the entire implementation of the projects, including possible exclusion at subsequent stages in the event that risks or involvement in human rights violations are detected.

351 European Parliament. (n.d.). *Commission replies to questionnaire MFF H1* [PDF]. https://www.europarl.europa.eu/cmsdata/299410/Commission%20replies%20to%20questionnaire%20MFF%20H1.pdf