Les portes d'entrada de la tecnologia del genocidi a Europa

La traçabilitat del sector militar i de vigilància israelià al mercat europeu

---

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

Les portes d'entrada de la tecnologia del genocidi a Europa

La traçabilitat del sector militar i de vigilància israelià al mercat europeu.

Autores: Observatori de Drets Humans i Empreses a la Mediterrània (Felipe Daza, Carlos Díaz, Nora Miralles) i Irídia – Centre per la Defensa dels Drets Humans (Cèlia Carbonell Cassanyes i Laura Riba Singla)

Coordinació: Maite Ramos i Alys Samson

Comunicació: Lucrecia Baquero Ramos

Assistència legal: Laia Serra Perelló

Maquetació: Carmela Márquez B @edicionescaseras

Traducció: Lia Giralt

Les autores volem expressar el nostre agraïment a MigrESS, Who Profits, DIMSE, l'European Digital Rights (EDRi) i a Access Now per la seva revisió i comentaris, que han contribuït a millorar la qualitat d'aquest informe.

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

Informe realitzat en el marc del projecte:

Alhimaya II: Estratègies per enfortir capacitats socials i protegir defensores com resposta als paradigmes d'espais cívics sense drets a Tunísia, Palestina, Marroc, Sàhara Occidental i Catalunya

Amb el suport de:

Agència Catalana de Cooperació al Desenvolupament · Generalitat de Catalunya · ICIP Institut Català Internacional per la Pau

Index

ACLARIMENTS SOBRE LA TERMINOLOGIA UTILITZADA:

El dret internacional considera el territori palestí de Cisjordània, incloent-hi Jerusalem Est, i la Franja de Gaza, territori ocupat il·legalment per Israel. Altres autores consideren que tota la Palestina històrica (el territori colonitzat sota el protectorat britànic entre el 1918 i el 1948) està ocupada, ja que la creació de l'Estat d'Israel es va crear a partir de la destrucció de més de 500 pobles palestins i l'expulsió de gran part de la població autòctona que hi vivia, el poble palestí. Quan es va votar el Pla de Partició a les Nacions Unides de la Palestina històrica, tots els països veïns van votar en contra i el poble palestí no va ser consultat.

En aquest informe, quan parlem de Territori Palestí Ocupat (TPO), ens referim a la Franja de Gaza, Jerusalem Est i Cisjordània.

En aquest informe, en general, emprarem el femení genèric com a expressió lingüística referida a persones.

LLISTAT D'ACRÒNIMS

ACCIÓ	Agència per a la Competitivitat de l'Empresa (Generalitat de Catalunya)
CAAT	Campaign Against Arms Trade (Campanya contra el comerç d'armes)
C4I	Comandament, control, comunicacions, computació i intel·ligència
CDH ONU	Consell de Drets Humans de les Nacions Unides
CRA	Cyber Resilience Act (Llei europea de ciberresiliència)
CSDD	Corporate Sustainability Due Diligence Directive (Directiva sobre diligència deguda de les empreses en matèria de sostenibilitat)
CTEM	Continuous Threat Exposure Management (Gestió contínua de l'exposició a amenaces)
DIANA	Defence Innovation Accelerator for the North Atlantic (Accelerador d'Innovació de Defensa per a l'Atlàntic Nord)
DM	Digital Markets Act (Llei de Mercats Digitals)
DPAP	Defence Production Action Plan (Pla d'acció per a la producció de defensa)
DSA	Digital Services Act (Llei de Serveis Digitals)
EDF	European Defence Fund (Fons Europeu de Defensa)
EDRI	European Digital Rights Network
EIC	European Innovation Council (Consell Europeu d'Innovació)
ELNET	European Leadership Network (Xarxa Europea de Lideratge)
EMFA	European Media Freedom Act (Llei Europea de Llibertat dels Mitjans de Comunicació)
ESDI	Security and Defence Initiative (Iniciativa de Seguretat i Defensa)
GCS	Ground Control Station (Estació de Control Terrestre)
GII	Global Israel Initiative (Iniciativa Global Israelí)

IAI	Israel Aerospace Industries
IED	Inversió estrangera directa
IDSF	Israel Defence and Security Forum (Fòrum de Defensa i Seguretat d'Israel)
INCIBE	Institut Nacional de Ciberseguretat d'Espanya
MFP	Marc Financer Plurianual
NSPA	NATO Support and Procurement Agency (Agència de Suport i Contractació de l'OTAN)
OCHA	Oficina de les Nacions Unides per a la Coordinació d'Afers Humanitaris
ONU	Organització de les Nacions Unides
OTAN	Organització del Tractat de l'Atlàntic Nord
PEGA	Comissió d'Investigació Pegasus del Parlament Europeu
PURL	NATO Prioritised Ukraine Requirements List (Llista de Requisits Prioritaris de l'OTAN per a Ucraïna)
R+D	Recerca i Desenvolupament
RGPD	Reglament General de Protecció de Dades
RPAS	Remote Piloted Aircraft Systems (Sistemes d'aeronaus pilotades remotament)
UAV	Unmanned Aerial Vehicle (Vehicle aeri no tripulat)
UE	Unió Europea
UNOSAT	United Nations Satellite Centre (Centre de Satèl·lits de les Nacions Unides)

Introducció

El genocidi d'Israel a la Franja de Gaza ha estat aprofitat pel complex-militar industrial global per desenvolupar noves tecnologies i estratègies militars amb grans beneficis per a les elits econòmiques i polítiques. Aquest fenomen es reflecteix en l'emergència del sector defence tech, caracteritzat per la simbiosis entre empreses militars i de seguretat tecnològiques. Entre les seves aplicacions destaquen la innovació i desenvolupament de tecnologies de ciberseguretat, intel·ligència artificial (IA), reconeixement biomètric i drons d'última generació, entre d'altres. En molts dels casos, aquestes empreses produeixen tecnologies de doble ús civil-militar, i per tant ofereixen els seus serveis a institucions de la indústria militar, agències de seguretat i altres actors públics per augmentar el control i la vigilància de la població, incloent el control migratori.

El present estudi analitza les empreses defence tech[1] israelianes que han emergit o s'han vist reforçades arran de l'actual genocidi a la Franja de Gaza i de la situació d'ocupació del territori palestí. I, més concretament, com aquestes estan transferint el coneixement adquirit i els productes desenvolupats a Europa. El Territori Palestí Ocupat ha estat utilitzat per Israel com un "laboratori" d'armes i tecnologies militars israelianes. La gran ofensiva desfermada sobre el territori palestí de la Franja de Gaza no només ha continuat amb aquesta lògica, sinó que l'ha amplificat fins a l'extrem. Una dada clau d'aquesta tendència és que més d'un terç de les startups israelianes del sector armamentístic s'han creat a partir del 7 d'octubre de 2023.[2]

Segons Sherrington Hoffman, director de Global Partnership de l'agència israeliana Startup Nation Central: "Estem veient un canvi en allò que el defence tech ha esdevingut com a sector. La despesa en armament s'està disparant arreu del món, sumat, evidentment, a les preocupacions locals i geopolítiques que afronta Israel i que han accelerat algunes de les innovacions. Això ha creat una situació en què la innovació testada en combat s'està validant ràpidament i a una velocitat i intensitat que feia temps que no veiem".[3] D'acord amb Startup Nation Central, l'ecosistema armamentístic israelià incloïa al 2025 més de 300 startups actives (en comparació amb les 160 de 2024). Aquest creixement disparat inclou nous projectes centrats en vehicles i drons no tripulats; sistemes C4I

1 Fa referència al conjunt de tecnologies, sistemes i innovacions desenvolupades per a ús militar o de seguretat. Inclou tant el desenvolupament d'armes com altres eines tecnològiques utilitzades per exèrcits, governs o empreses vinculades a la defensa.

2 Harris, L. (2024, 25 d'agost). 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 de febrer). AI, drones, and the explosive growth of Israel's dual-use defensetech industry. CTech. https://www.calcalistech.com/ctechnews/article/b16ehzo5kg

(comandament, control, comunicacions i intel·ligència); sistemes electrònics; sistema d'intercepció de míssils i altres tecnologies de doble ús.[4]

Alhora, amb el rearmament d'Europa i el conseqüent augment del pressupost militar dels Estats membre de l'OTAN, la regió s'ha consolidat com a pol d'atracció per a nombroses empreses israelianes del sector defence tech que han contribuït al genocidi i l'ocupació de Palestina. Aquestes empreses utilitzen diverses estratègies per penetrar al continent europeu i accedir a contractes en els sectors armamentístics i de seguretat. Tanmateix, no existeix un escrutini sistemàtic sobre com es realitza la penetració d'aquestes empreses i de les seves tecnologies de doble ús a Europa.[5] En aquest sentit, els objectius específics d'aquest informe són:

- Posar llum sobre qui es beneficia i qui finança el genocidi en termes d'empreses i tipus de tecnologia, així com dels fons financers que les permeten operar i en recullen dividends.

- Explorar la traçabilitat de les empreses del sector de defence tech i seguretat tecnològica, amb especial atenció als països d'entrada, mecanismes i actors que faciliten la seva penetració.

- Estudiar les condicions legals i burocràtiques que permeten a les empreses del sector defence tech establir-se a la Unió Europea (UE) amb facilitat.

- Investigar el registre i l'activitat d'empreses de ciberseguretat i vigilància creades a Europa amb vincles israelians o internacionals que operen com a empreses nacionals, evitant potencialment l'escrutini (mapa de filials, centres d'innovació i producció, etc.).

4 Startup Nation Central. (2025, 3 d'abril). 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-comp anies-in-the-sector-302419767.htm

5 Les tecnologies de doble ús són aquelles que poden tenir aplicacions tant civils com militars. És a dir, són tecnologies, equips, programes informàtics o coneixements que s'han desenvolupat amb una finalitat aparentment civil (per exemple, científica, industrial o comercial), però que també poden ser utilitzats per a objectius de defensa, vigilància o repressió.

La compra d'aquestes tecnologies per part de governs i empreses al continent europeu es produeix en un marc d'augment de la vigilància tecnològica i de repressió policial i judicial creixent a l'activisme,[6] on existeix el risc plausible que s'estiguin utilitzant tecnologies d'algunes de les empreses que s'assenyalen en aquest informe.

Per tant, l'anàlisi de les vies d'entrada d'aquestes tecnologies a Europa no constitueix únicament un exercici de traçabilitat empresarial, sinó també una interrogació sobre les responsabilitats estructurals dels Estats europeus en la reproducció d'un ordre global colonial, on la seguretat es prioritza per damunt dels drets humans i la innovació tecnològica es legítima fins i tot quan s'ha creat i usat en contextos de violència extrema.

6 United Nations. (2025, 16 d'octubre). 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
Veure també: AFP. (2025, 16 d'octubre). 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/

I

Contextualització: el genocidi i l'impacte de les tecnologies de seguretat i militars.

El passat setembre del 2025, the Independent International Commission of Inquiry on the Occupied Palestinian Territory, comissió establerta pel Consell de Drets Humans de l'ONU va determinar que Israel ha comès genocidi contra el poble palestí a la Franja de Gaza.[7] Aquesta conclusió per part d'aquest òrgan independent, arriba després que Israel hagi mantingut un bloqueig a la Franja de Gaza per terra,[8] mar i aire des de fa 18 anys i des que, a l'octubre del 2023, l'exèrcit d'Israel iniciés una nova invasió i atac sobre el mateix territori.[9]

El genocidi, entès com l'intent deliberat de destruir, totalment o parcialment, un grup nacional, ètnic, racial o religiós, constitueix una de les vulneracions més greus dels drets humans. Tradicionalment, l'anàlisi dels genocidis s'havia centrat en la seva dimensió política, ideològica i militar, però en les darreres dècades s'ha fet evident que les tecnologies de control, ciberseguretat, vigilància i IA exerceixen un paper creixent en la seva preparació, execució i fins i tot justificació. Segons Jalal Abukhater, Responsable de Polítiques de 7amleh, organització de defensa dels drets humans de les palestines, "els sistemes d'IA perfeccionats durant la guerra, ja sigui per a l'anàlisi predictiva, el monitoratge biomètric, la focalització automatitzada o l'extracció massiva de dades, consolidaran i expandiran el règim d'ocupació i apartheid. Aquestes eines no desapareixen després del conflicte: passen a formar part de la governança quotidiana".[10]

En un ordre global racialitzat, els territoris sotmesos a dominació colonial operen com a laboratoris on s'assagen tècniques de control, vigilància i violència que, un cop estabilitzades, es normalitzen i es reexporten com a "solucions" de seguretat. En aquest marc, l'ocupació prolongada de Palestina ha permès consolidar un ecosistema tecnopolític en què la innovació es valida sobre cossos racialitzats i despossetïts de drets, convertint l'excepcionalitat permanent en infraestructura i en model. Com adverteix Ruha Benjamin, lluny d'eliminar el racisme, les tecnologies contemporànies tendeixen a reproduir-lo i automatitzar-lo, camuflant-lo sota narratives de neutralitat, eficiència i progrés.[11]

El genocidi a Gaza seria, des d'aquesta anàlisi, una expressió especialment crua d'aquest règim global de poder, en què la tecnologia s'entrellaça amb formes històriques de do-

7 Nacions Unides. (2025, 16 de setembre). Israel ha comès genocidi en la Franja de Gaza. UN News. https://news.un.org/es/story/2025/09/1540443

8 El juny de 2007, després de l'arribada al poder de Hamàs a Gaza, les autoritats israelianes van intensificar significativament les restriccions de moviment existents, aïllant pràcticament la Franja de Gaza de la resta del Territori Ocupat Palestí i del món.

9 United Nations Office for the Coordination of Humanitarian Affairs. (2022, 30 de juny). 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 de novembre). 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.

minació colonial i racial.[12] Des d'aquesta perspectiva, el genocidi no s'entén com una anomalia o una alteració puntual del funcionament del mercat, sinó una condició que habilita noves formes d'acumulació i d'expansió empresarial. L'informe de la Relatora Especial de Nacions Unides, Francesca Albanese,[13] reforça aquesta lectura en assenyalar que múltiples empreses es beneficien directament o indirectament de l'ocupació, l'apartheid i el genocidi, aportant infraestructures, també tecnològiques, sense les quals la violència i vigilància massiva no podrien desplegar-se amb la mateixa eficàcia. La externalització de funcions militars i d'intel·ligència cap a empreses privades contribueix, així, a la privatització de la violència, diluint la responsabilitat política entre contractes, filials i cadenes de subministrament transnacionals. Des d'un enfocament antiracista, aquesta economia corporativa de la guerra reforça un ordre global en què la destrucció de poblacions racialitzades es converteix en oportunitat de negoci, alhora que es normalitza la impunitat empresarial.

Una part de la literatura menys hegemònica i més crítica, la de les perspectives decolonials i antiracistes, posa el focus en la seva inserció en estructures materials de dominació, i en particular en el capitalisme racial: un concepte desenvolupat per Cedric J. Robinson per descriure un sistema econòmic que depèn estructuralment de la jerarquització racial i de l'explotació desigual de poblacions considerades prescindibles.[14]

La qualificació dels fets ocorreguts a la Franja de Gaza com a genocidi es recolza en la definició establerta per la Convenció per a la Prevenció i Sanció del Delicte de Genocidi de 1948,[15] que tipifica com a tals els actes comesos amb la intenció de destruir totalment o parcialment un grup nacional, ètnic, racial o religiós.[16]

Aquesta definició no circumscriu el genocidi a una operació militar concreta ni a un període temporal tancat, sinó que el concep com un patró d'actes guiats per una intencionalitat específica, la destrucció, total o parcial, d'un grup. En aquest sentit, el genocidi no finalitza necessàriament amb la signatura d'un alto el foc o d'un acord polític, si persisteixen conductes orientades a fer inviable la supervivència física o social del grup afectat.

12 En aquesta línia, Achille Mbembe ha assenyalat que, en l'ordre contemporani, la sobirania s'exerceix cada vegada més a través de la capacitat de decidir quines poblacions poden viure i quines poden ser abocades a la mort o a condicions d'existència letals, una lògica que conceptualitza com a necropolítica.

13 United Nations Human Rights Council. (2025, 2 de juliol). 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 de setembre). 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 de setembre). Resolució de la IAGS sobre la situació a Gaza. Viento Sur. https://vientosur.info/resolucion-de-la-iags-sobre-la-situacion-en-gaza/

En el context actual de la Franja de Gaza, la privació sistemàtica d'aliments, d'accés a aigua potable, atenció mèdica, refugi, higiene i béns essencials pel desenvolupament de la vida, així com el desplaçament forçat i reiterat de la població civil, no poden ser analitzats com a fets aïllats o meres conseqüències col·laterals, sinó com a elements d'un patró continuat que pot constituir una prolongació del delicte de genocidi. Per tant, parlar de genocidi en relació amb la Franja de Gaza no implica únicament una lectura retrospectiva dels esdeveniments iniciats l'octubre de 2023, sinó una anàlisi en temps present de conductes que, per la seva naturalesa i intencionalitat, poden seguir encaixant en la tipificació del crim de genocidi segons el dret internacional vigent.

Però el projecte colonial d'Israel no es limita a l'ofensiva genocida a la Franja de Gaza. A Cisjordània, des de l'octubre de 2023 tant l'exèrcit israelià com els colons armats han intensificat el control, la vigilància massiva i els atacs sobre la població palestina.[17]

En aquest sentit, diversos organismes internacionals han documentat un augment molt significatiu de la violència perpetrada per colons israelians i per les forces de seguretat i l'exèrcit israelià a Cisjordània. Segons l'Oficina de Drets Humans de l'ONU al Territori Palestí Ocupat i l'Oficina per a la Coordinació d'Afers Humanitaris (OCHA), que monitoritza els incidents i atacs relacionats amb colons,[18] des del 7 d'octubre de 2023 fins a mitjans d'octubre de 2025 s'han produït més de 1.000 assassinats de persones palestines a la Cisjordània Ocupada i Jerusalem Est.[19]

L'informe del comitè especial de les Nacions Unides per investigar les pràctiques de l'Estat d'Israel, exposa que com a potència ocupant, l'Estat d'Israel té l'obligació de protegir la població civil i evitar que els colons escalin la violència, fet que no només no respecta, sinó que sovint hi ha una connivència dels cossos de seguretat israelians (policia i exèrcit) amb els colons armats.[20]

17 Palestinian Return Centre. (2025, 23 de setembre). 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 d'octubre). 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. (s.f.). 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 de setembre). 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/

Les noves tecnologies de control, ciberseguretat, vigilància i intel·ligència artificial no només amplien la capacitat letal de governs i empreses, sinó que transformen la manera com es planifica, s'administra i es legitima la violència massiva.

Aquest fenomen s'intensifica quan aquestes tecnologies es desenvolupen i es proven en contextos de conflicte i/o ocupació. En aquest sentit, el genocidi a la Franja de Gaza pot llegir-se com una expressió del que Mbembe descriu com a "mons de mort", on el poder no es limita a matar, sinó que organitza l'exposició a la mort i confina poblacions en condicions de vida degradada, com si la vida quedés reduïda a un residu.[21] Aquest règim, però, no opera només mitjançant la mort, sinó també mitjançant la producció de dany. Jasbir K. Puar amplia l'anàlisi en assenyalar que el poder colonial pot governar mantenint poblacions en un estat permanent de lesió i precarietat: el "dret a mutilar" descriu un sistema que administra la vida danyada com a estratègia de control.[22] Les amputacions, lesions irreversibles i el trauma psicosocial documentats a la Franja de Gaza poden llegir-se en aquesta clau: com a part d'una tecnologia de govern que no només mata, sinó que gestiona la vida ferida.

La incorporació de sistemes d'IA i vigilància massiva reforça aquest procés i converteix el genocidi en un dispositiu tecnopolíticament gestionat: la decisió letal es desplaça cap a infraestructures algorítmiques opaques i s'erosionen els principis de responsabilitat i control democràtic. En aquest marc, la vigilància biomètrica i l'automatització d'objectius faciliten l'exercici de la violència amb més distància, més velocitat i més impunitat.

Els efectes d'aquesta tecnificació del conflicte són múltiples. D'una banda, incrementa la capacitat de destrucció i accelera l'execució: l'automatització permet atacar a una escala i amb una rapidesa sense precedents, amb impactes directes sobre la població civil. De l'altra, la digitalització de la guerra debilita la rendició de comptes: quan decisions amb conseqüències immediates sobre els drets humans depenen d'algoritmes opacs, sovint de codi tancat i, per tant, difícilment auditables, la societat civil no en pot fiscalitzar els biaixos ni les lògiques de funcionament, i la responsabilitat humana es dilueix. Això dificulta la investigació posterior dels crims i la identificació de responsables.[23] Alhora, no s'inclouen en els contractes d'adquisició d'aquestes tecnologies la revocació de llicències en el cas de que s'usin per finalitats contràries als drets humans.

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, juny). 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

En paral·lel, el complex militar-tecnològic s'ha consolidat com un element estructural en l'exercici del poder i sovint opera amb tecnologies d'ús dual. Segons un informe publicat l'any 2024 pel Global Centre for the Responsibility to Protect, els avenços tecnològics poden "tant prevenir com facilitar el genocidi, depenent de com i per qui siguin emprats".[24] La mateixa infraestructura digital que pot servir per documentar crims de guerra també pot habilitar la vigilància massiva i la selecció automatitzada d'objectius civils, com ha evidenciat la Franja de Gaza.[25]

A més, els algoritmes i la IA tenen ratis d'error en la identificació i classificació d'objectius. Un informe d'Al-Haq sobre l'impacte del genocidi i l'ocupació en les dones i les nenes, publicat el desembre de 2025, exposa la relació directa entre l'ús generalitzat de la IA en el genocidi i la ràtio extrema de morts civils, entre elles un augment exponencial de l'assassinat de dones i criatures. Programari, com l'anomenat Gospel,[26] han doblat el nombre d'objectius militars diaris, normalitzant el foc contra edificis residencials sencers. De fet, 9 de cada 10 dones es trobaven en edificis residencials quan van ser assassinades, i el 95% d'aquestes van ser executades juntament amb criatures.[27]

Les dades aportades per les agències de les Nacions Unides són clares, a finals d'octubre del 2025, s'estimen al voltant de les 70.000 persones assassinades i 170.000 ferides a la Franja de Gaza, amb aproximadament un 90% de la seva població desplaçada.[28] Diversos estudis citen que el nombre de persones assassinades podria ser molt més elevat.[29] L'anàlisi satel·lital del United Nations Satellite Centre (UNOSAT) indica que prop del 83% de les infraestructures (hospitals, escoles, carreteres, dipòsits d'aigua) a la Franja de Gaza han estat malmeses o destruïdes.[30]

24 Global Centre for the Responsibility to Protect. (2024, març). 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

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

26 És un sistema d'intel·ligència artificial utilitzat per l'Exèrcit d'Israel per identificar i prioritzar objectius a gran escala, especialment en els atacs sistemàtics sobre la Franja de Gaza.

27 Al-Haq. (2025, 9 de desembre). 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 d'octubre). Humanitarian Situation Update #336 | Gaza Strip. https://www.ochaopt.org/content/humanitarian-situation-update-336-gaza-strip

29 Khatib, R., Abu-Rmeileh, N. M., Sclavi, G., Ewen, M., & McKee, M. (2025). The health situation in Gaza: A call for urgent action. The Lancet Global Health, 13(2), e145-e146. https://doi.org/10.1016/S2214-109X(25)00522-4

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

A més, segons dades de la OCHA, des de l'inici d'octubre de 2023, hi ha hagut una destrucció sistemàtica d'infraestructures palestines a Cisjordània i Jerusalem Est, en total més de 4.800 estructures palestines han estat destruïdes, el que ha tingut com a conseqüència que més de 9.000 persones hagin estat desplaçades de les seves llars.[31]

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

La Franja de Gaza com a laboratori de genocidi de tecnologies que arriben a Europa.

El genocidi a la Franja de Gaza ha deixat el món en estat de xoc. La impunitat amb que diàriament s'ha exterminat la població palestina en aquest territori i la manca de perspectives de depuració de responsabilitats per aquests fets, ha produït una deslegitimació global de les institucions internacionals. Però, aquest xoc no ha estat només en un sentit emocional, normatiu i humanitari, sinó també en el sentit econòmic que li atorguen autores com Naomi Klein.[32] Per a Klein, els grans episodis de crisi creen les condicions per "rendibilitzar" econòmicament la por i el desordre, privatitzant serveis públics o expandint el mercat de la seguretat.[33] En aquest cas, es rendibilitza econòmicament l'assassinat de desenes de milers de persones amb més contractes, exportacions i demanda de tecnologies militars i de vigilància.

Així, darrera d'aquesta nova fase colonial i extractivista que perpetra un genocidi sense conseqüències, hi trobem un entramat d'interessos econòmics i polítics, format per empreses de tecnologia de la indústria militar i seguretat israelianes, europees i nord-americanes. Però, també, pels fons i subfons d'inversió que ostenten les accions d'aquestes empreses. L'acció d'aquestes empreses succeeix en un context d'apartheid, genocidi, colonialisme i ocupació militar [34], on les grans empreses tecnològiques no tenen un rol neutre. Ben al contrari, estarien contribuint a perpetuar un ecosistema que aprofita la vulneració massiva de drets de la població palestina per lucrar-se econòmicament.

La manca de transparència en les dades no permet tenir una imatge clara i acurada del volum econòmic i financer que ha generat el genocidi a la Franja de Gaza. Però, algunes anàlisis apunten al fet que el genocidi ha convertit una població que li resultava "excedentària i improductiva", a causa de la pròpia ocupació israeliana, en un producte de mercat[35], on el principal al·licient pel guany era la letalitat i l'efectivitat de les armes emprades. És a dir, la mort, la mutilació massiva de la població palestina de la Franja de Gaza, la destrucció del seu territori i la posterior reconstrucció han esdevingut un nou aparador pels "productes" militars i tecnològics israelians, que ja es publiciten des de fa dècades com a "provats en combat" sobre la població palestina.

Si bé hi ha casos d'empreses que han perdut contractes per haver estat vinculades públicament amb el genocidi i l'ocupació, la realitat és que aquesta pèrdua de beneficis és residual respecte el creixement econòmic que experimenten.

32 La doctrina del xoc explica com les crisis són usades per imposar reformes neoliberals, reduint la resistència social mitjançant la por i la incertesa.

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

34 Apoorva, P. G. (2023, 24 de novembre). 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 d'octubre). Gaza and the economy of genocide. Jacobin. https://jacobin.com/2025/10/gaza-economy-genocide-capitalism-surplus

De fet, moltes empreses han trobat nous mercats, fruit de la normalització de l'exportació i del finançament de la tecnologia utilitzada en el genocidi, que ha fet que les portes d'entrada al continent europeu d'aquestes continuïn essent molt nombroses. Fins i tot, s'han afegit noves vies d'entrada vinculades al context actual, com ara el rearmament europeu, el reforç de la relació entre Israel i Ucraïna o un augment de l'arribada de personal especialitzat israelià i de les seves empreses a països europeus.

Aquest viatge del know-how militar des de l'Estat d'Israel cap a Europa permet aplicar les innovacions militars i de seguretat apreses en els darrers dos anys a la tecnologia europea. Aquesta transferència es fa principalment a través de la creació de filials i subsidiàries, de la compra d'empreses europees preexistents, d'organitzacions supranacionals com l'OTAN, d'institucions i fons de recerca europeus, d'Estats i de països amb acords bilaterals amb Israel o amb un marc regulador més laxa, des d'on poder començar a operar. En alguns casos, aquestes empreses s'han vist obligades a sofisticar el procés per dos motius: l'ampliació de la normativa de la Unió Europea que regula l'ús d'aquestes tecnologies i el rebuig que desperta el seu origen. Un rebuig que no és només territorial, sinó també vinculat a la finalitat per a la que es van crear i l'ús que se n'ha fet en la vulneració sistemàtica dels drets humans.

Per últim, cal assenyalar que la transferència de coneixement i tecnologia cap a Europa es produeix en un context d'increment del control i de la persecució policial i judicial creixent a l'activisme en suport a Palestina i contra el genocidi a la Franja de Gaza.[36] La majoria de cossos policials als països on s'estan duent a terme aquestes mobilitzacions operen amb eines d'extracció d'informació,[37] reconeixement facial i intercepció de comunicacions desenvolupades per empreses israelianes o amb vincles amb Israel,[38] com Cellebrite, Corsight i Excem.[39] És el cas, també, de cossos policials a l'Estat espanyol com els Mossos d'Esquadra i la Guàrdia Civil.[40]

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 de gener). 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 d'octubre). 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 de novembre). 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/

Cal destacar que, qualitativament parlant, es tracta d'una tecnologia que està transformant el paradigma de l'espionatge d'Estat mitjançant el desplegament de tècniques de ciberespionatge i repressió de caràcter transnacional, que permeten la intervenció de dispositius mòbils amb independència de la seva localització geogràfica.

III

Principals empreses i inversors clau en el desenvolupament i finançament de la tecnologia usada al genocidi des del 2023.

El juny del 2025, l'oficina de la Relatora Especial de les Nacions Unides per al Territori Ocupat de Palestina, Francesca Albanese, va publicar un informe d'extrema rellevància, titulat "De l'economia d'ocupació a l'economia del genocidi", que conté un llistat amb les principals entitats beneficiàries del genocidi a la Franja Gaza i de l'ocupació de Palestina.[41] En aquest llistat, figuren empreses públiques o privades, multinacionals, entitats amb ànim de lucre o sense que "es beneficien de l'economia il·legal d'ocupació, apartheid i ara genocidi, d'Israel"[42] sobre el Territori Palestí Ocupat. Hi apareixen, entre altres, grans companyies de Big Tech estatunidenques, com Microsoft, Google, IBM o Palantir Technologies, que han estat claus per a l'automatització del genocidi. Aquestes empreses han posat la seva tecnologia al servei d'alguns dels sistemes més controvertits de localització d'objectius usats a l'extermini de desenes de milers de persones a la Franja de Gaza. També hi apareixen empreses que porten anys identificades o que han estat recollides a la base de dades publicada per l'organisme supranacional el 2020 —actualitzada recentment—, i algunes de les majors empreses armamentístiques mundials i israelianes, amb àmplia presència a Europa a través de filials, subsidiàries i joint ventures.

Hi ha, però, moltes altres startup i empreses defence tech o de seguretat i vigilància tecnològica amb origen a Israel, o bé de capital israelià, que s'han beneficiat de contractes amb el Ministeri de Defensa israelià en els darrers dos anys, i que han proporcionat la tecnologia necessària per executar el genocidi. En alguns casos, aquestes companyies ja havien estat assenyalades en informes d'organitzacions com Amnistia Internacional, Who Profits, per la Campanya Internacional pel Boicot, les Sancions i les Desinversions a Israel (BDS), l'American Friends Service Committee (AFSC) o l'Observatori de Drets Humans i Empreses a la Mediterrània (ODHE). Empreses assenyalades bé per la seva contribució a fabricar l'armament, drons o el programari utilitzat a la Franja de Gaza, o per continuar facilitant el colonialisme digital, en forma de vigilància massiva i control de les vides de la població palestina sota ocupación.

41 Albanese, F. (2025, juliol). 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-5 9-23-aev.pdf

42 Ibid.

1. Les majors de la indústria militar i de seguretat, les grans beneficiades.

Les tres beneficiàries dels majors contractes directament relacionats amb el genocidi en curs a la Franja de Gaza són també tres de les grans companyies mundials de la indústria militar, d'armament i de seguretat: Elbit Systems LTD, Israel Aerospace Industries (IAI) i Rafael.[43]

Elbit Systems

Empresa israeliana amb filials arreu d'Europa i que és la gran proveïdora de drons a l'exèrcit d'Israel.[44] Al seu tancament del 2024, l'empresa va reportar 6.000 milions de dòlars en beneficis i una cartera de comandes pendents de 22.600 milions, un 14% més que l'any anterior.[45] Mentre que, fins al segon trimestre del 2025, Elbit va reportar 2.000 milions de dòlars en beneficis i una cartera de projectes futurs de 23.800 milions de dòlars.[46] Alguns d'aquests contractes corresponen a les bombes MPR-500, capaces de penetrar diverses capes de formigó [47], que l'exèrcit israelià està llançant sobre la Franja de Gaza.[48]

D'altra banda, els beneficis a la seva divisió Aerospace van augmentar un 9% el 2024 respecte al 2023, sobretot per les vendes de Vehicles Aeris No Tripulats (UAS). Del sector de la ciberseguretat, aquest augment va ser d'un 11%, mentre que dels sistemes terrestres va ser d'un 29% per l'increment de vendes en munició a l'exèrcit d'Israel.[49]

Israel Aerospace Industries (IAI)

Empresa propietat de l'Estat d'Israel, especialitzada en aviònica militar, però amb divisions en ciberseguretat i solucions per a infraestructures crítiques i policia. A principis del 2025, IAI va anunciar una facturació total de 6.100 milions de dòlars el 2024 i uns beneficis rècord de 493 milions de dòlars, un 55% més que el 2023, a més d'una previsió d'encàrrecs

43 Elmas, D. S. (2025, 1 de desembre). 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 de març). 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 de març). 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 d'agost). Elbit Systems reports second quarter 2025 results. https://www.elbitsystems.com/news/elbit-systems-reports-second-quarter-2025-results

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

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

49 Ynet News, cita 34

per valor de 25.000 milions de dòlars.[50] El 34% del benefici provenia de vendes internes al govern israelià, passant dels 1.500 milions de dòlars del 2023 als 2.000 milions del 2024.

La seva participació en el genocidi està vinculada a la venda de UAV com els Heron killer drones [51] [52]. IAI també proveeix l'exèrcit d'Israel amb el vehicle utilitari tàctic Zibar.

IAI és a punt de sortir amb bons a inversors per injectar efectiu a les arques de l'economia israeliana. Una economia seriosament afectada per l'ofensiva contra la Franja de Gaza després de 2 anys de despesa pública disparada en la indústria militar.[53]

La companyia ha rebut fins a 2,7 milions d'euros de la Comissió Europea a través de 8 projectes,[54] en alguns casos atorgats a través d'una empresa grega de la seva propietat, Intracom Defense, que participa actualment en 15 projectes del Fons Europeu de Defensa (EDF). Set d'ells es van adjudicar després de la venda d'aquesta empresa a IAI i de l'inici del genocidi a la Franja de Gaza, l'octubre de 2023. Tot i que Intracom Defense està registrada i té la seu a Grècia (i que també té presència grega al seu consell d'administració), els seus registres financers del 2024 mostren que el 94,5% de les accions són propietat d'IAI que, segons els últims registres de l'empresa israeliana, posseeix el 100% dels drets de vot a Intracom.[55]

Rafael Advanced Defense Systems

Rafael és una de les líders mundials en producció d'armament, propietat de l'Estat d'Israel. L'exèrcit israelià ha fet servir sistemes fabricats, com ara els míssils Spike, per Rafael per atacar persones dins dels edificis de Gaza,[56] i diverses fonts apunten que haurien utilitzat, també, els coets Matador, fabricats per la filial alemana de Rafael Dynamit Nobel

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

51 Ynet News, cita 34

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

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 de desembre). 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 de juny). 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 de desembre). Companies profiting from the Gaza genocide. https://afsc.org/gaza-genocide-companies

Defence.[57] Aquests coets són una arma antiblindatge de curt abast, altament eficaç contra vehicles blindats i poden travessar murs de maó.

L'1 d'abril de 2024, un dron Hermes 450 fabricat per Elbit Systems i que, segons el diari britànic The Times, anava armat amb míssils Spike de Rafael58[58] va atacar tres vehicles de l'organització humanitària World Central Kitchen a prop de Deir al-Balah, al centre de la Franja de Gaza, matant set treballadors humanitaris. De la mateixa manera, els drons assassins Orbiter 4 desenvolupats per Aeronautics, filial de Rafael, haurien estat usats per primera vegada a la Franja de Gaza el 8 de novembre de 2023.59 [59] A més, Rafael va col·laborar amb l'exèrcit israelià en el desenvolupament de l'Spark, un nou dron no tripulat utilitzat per dur a terme missions d'intel·ligència, escortar forces terrestres i dirigir atacs.[60] Organitzacions com Campaign Against Arms Trade (CAAT) apunten a què l'Spark hauria estat ja utilitzat en l'ofensiva contra la Franja de Gaza.[61]

L'empresa va aconseguir una facturació de 4.800 milions de dòlars el 2024 —un 27% més que el 2023— i un benefici net de 257 milions de dòlars. El CEO de l'empresa va reconèixer obertament que el genocidi a la Franja de Gaza ha suposat un impuls a les vendes i a les comandes, la meitat de les quals són ja per armar Israel.[62]

2. El sector dels drons, un pastís repartit entre molts inversors.

Israel és una potència mundial de la indústria dels drons, pionera en el seu desenvolupament militar des de la dècada de 1960 i líder en innovació, amb nombroses startups que lideren el mercat civil. Un grup nombrós d'aquestes, fundades majoritàriament per ex soldats, han proporcionat la seva tecnologia al Ministeri de Defensa en aquests darrers anys.

57 Tielke, N. (2023, 31 d'octubre). 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-pa nzerfaeuste-nach-israel-UXMIKBQTKZAS3E6YRLH4ZULRRE.html

58 Grylls, G. i Weiniger, G. (2024, 3 d'abril). 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

59 Walla News. (2023, 9 de novembre). *חושפים מחבלים ואוספים מודיעין: הכטמ"מים החדשים החלו לפעול בעזה*
[Exposant terroristes i recollint intel·ligència: els nous drons han començat a operar a Gaza].
https://news.walla.co.il/item/3621520

60 Breaking Defense. (2023, 12 de setembre). 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 de setembre). Rafael. https://caat.org.uk/data/companies/rafael/

62 Rafael Advanced Defense Systems. (2025, 26 de març). 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/

És el cas d'SpearUAV, fabricant del "dron suïcida" Viper, que localitza, segueix i ataca objectius xocant contra ells i autodestruint-se. La pròpia companyia ha reconegut que el seu desenvolupament s'ha accelerat pel genocidi a la Franja de Gaza,[63] per tal de complir amb els requeriments de l'exèrcit israelià.[64]

Al mateix camp hi ha NextVision, que desenvolupa les càmeres utilitzades pels drons d'Elbit Systems, provades a la Franja de Gaza durant el genocidi, motiu pel qual aquesta startup va perdre, a l'agost de 2025, el finançament del principal fons de pensions noruec, KLP.[65] NextVision Stabilized Systems presentava, el 10 de desembre de 2025, un valor de mercat de més de 5.000 milions de dòlars, així com uns beneficis de 150 milions d'euros.[66]

DRS RADA Technologies, propietat de Leonardo DRS, filial de la macroempresa italiana de defensa Leonardo, produeix i lliura els radars que apuntalen les capacitats de vigilància aèria i alerta primerenca de l'exèrcit israelià.[67] La companyia ha obtingut enguany uns ingressos nets de 265 milions d'euros.

D'altra banda, Ben Levinson, el fundador de la fabricant israeliana de drons propulsats amb hidrògen Heven Aerotech, subsidiària de la hindú Paras Defence & Space,[68] assegurava recentment que "moltes empreses han estat treballant en materials armamentístics des del 7 d'octubre, però nosaltres teníem una planta que podia produir 100 drons al mes quan va esclatar la guerra, cosa que ens va ajudar a convertir-nos en proveïdors de l'exèrcit israelià".[69]

63 Cohen, S. (2024, 3 de gener). 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-g round-israeli-defense-startups-flourish/0000018c-cf39-ddba-abad-cfb9a3ee0000

64 Mönch Publishing Group. (2025, 26 de març). SpearUAV announces completion of a significant funding round led by Deep Insight venture fund.
https://monch.com/spearuav-announces-completion-of-a-significant-funding-round-led-by-deep-insight-venture-fund/

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

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

67 Egozi, A. (2023, 6 de juny). 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 de maig). 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-d rones-to-make-cargo-drones-in-india-13043513.html

69 Wrobel, S. (s.f.). 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/

Aquestes declaracions il·lustren com l'empresa percep l'ús potencial de la seva tecnologia en el genocidi, a més de ser un reflex de les bones relacions entre Israel i països com l'Índia o els Emirats Àrabs Units. Heven podria penetrar a Europa a través dels canals que ja té ParasDefense amb països com Alemanya, i a més, és una de les empreses ben posicionades per a beneficiar-se del pla de rearmament europeu.[70]

Per últim, en aquest sector, trobem el cas d'XTEND Defense, que fabrica drons controlats remotament des de fins a 9.000 quilòmetres, que utilitzen intel·ligència artificial per a realitzar atacs precisos amb mínima intervenció humana. XTEND ha estat adjudicatària recentment d'un contracte del Ministeri de Defensa israelià per al subministrament de 5.000 drons kamikaze [71] per a l'exèrcit israelià per un valor de 5,5 milions de dòlars.[72] L'empresa ha estat senyalada per alguns mitjans com a fabricant del dron que va rastrejar i va filmar l'assassinat del líder de Hamas Yahya Sinwar.[73] L'empresa va ser creada l'any 2018 per Aviv Shapira, Matteo Shapira i Rubi Liana. Segons el seu CEO "pot reconèixer i seguir un objectiu amb precisió letal".[74] El Ministeri de Defensa israelià va anunciar, l'agost del 2025, un contracte de diversos milions de dòlars amb aquesta empresa per subministrar la seva tecnologia a les forces terrestres de l'exèrcit israelià.[75] En un article al New York Times, van reconèixer el seu ús a la Franja de Gaza.[76] Al 2025, l'empresa ha doblat la seva recaptació del 2024, assolint les desenes de milions de dòlars anuals.[77]

70 Vaishnav, A. (2025, 6 de març). 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-eur opean-union-spending-plan-19569885.htm

71 XTEND. (s.f.). Warfare has changed forever [Vídeo].
https://www.xtend.me/resources/warfare-has-changed-forever

72 SOFX. (2025, 22 d'agost). 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/

73 Noticias de Israel. (2025, 31 de gener). 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 d'abril). 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 Ministeri de Defensa d'Israel [Israel MOD]. (2025). Israel MOD to procure thousands of drones from XTEND worth millions of dollars [Publicació de LinkedIn]. LinkedIn.
https://www.linkedin.com/posts/israel-mod-to-procure-thousands-of-drones-share-7363873945214693377-nQt9/

76 The New York Times. (2025, 25 d'abril). 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 de desembre). Israeli firm XTEND, whose drones reportedly killed Sinwar, wins major US defense deal. Ynetnews. https://www.ynetnews.com/business/article/bkcdsowgzl

3. Software espia, robòtica, reconeixement facial i altres sectors.

L'empresa més important en l'àmbit de programari espia, i de la que es parla abastament en aquest informe, és la fabricant del conegut software espia Pegasus, NSO Group. Aquesta va ser la primera empresa capaç de desenvolupar una tecnologia d'espionatge amb propietats inèdites, com tenir accés i control total del contingut d'un dispositiu mòbil a distància sense el permís ni coneixement de la propietària; tecnologia que l'empresa ha destacat que té origen directe en l'experiència militar israeliana.

Des de 2010 fins a l'actualitat, l'empresa ha operat sota una regulació ambigua que ha permès una vigilància desproporcionada i sistemàtica de desenes de milers de persones arreu del món.[78] NSO ha aparegut en nombrosos informes i recerques independents [79] per haver proporcionat a governs i agències d'intel·ligència tecnologia de vigilància que posteriorment s'ha utilitzat per espiar periodistes, advocats, dissidents i activistes pels drets humans. A l'Estat espanyol s'han acumulat una desena de querelles per l'espionatge il·legal amb Pegasus; una de les quals s'ha convertit en la primera denúncia d'una persona afectada que ha aconseguit la investigació judicial de tres càrrecs directius de l'empresa NSO Group a Israel i Luxemburg.[80]

Després de 25 anys, l'empresa ha crescut i s'ha consolidat com un símbol de la indústria cibernètica ofensiva d'Israel. Pegasus, el seu programari espia, es comercialitza com a tecnologia d'armament "fet a Israel" i s'ha promogut com a eina de política exterior per reforçar relacions diplomàtiques.[81] Investigacions mostren una correlació directa entre visites de caps d'Estat a Israel i l'autorització de noves llicències d'exportació de Pegasus, un patró observat tant en processos de normalització diplomàtica com en negociacions internacionals, incloent votacions a Nacions Unides.[82]

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

79 Amnesty International. (2021, 18 de juliol). 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/

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

81 The New York Times Magazine. (2022, 28 de gener). 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 de gener). 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

Des de l'octubre de 2023, NSO Group es va oferir voluntàriament per col·laborar amb la seva tecnologia en la missió de localitzar els ostatges israelians.[83] De facto, NSO Group va iniciar un procés d'actualització de la seva tecnologia militar de vigilància per al seu ús durant l'actual genocidi a la Franja de Gaza.

Seguint la seva estela, una de les darreres incorporacions al mercat que ha aflorat al voltant del genocidi és Dream Security, fundada el novembre de 2023 per un dels antics propietaris de NSO Group, Shalev Hulio, juntament amb Sebastian Kurz, excanceller austríac, i Gil Dolev, exlíder de Wayout Group.[84] Dream ha desenvolupat una plataforma basada en intel·ligència artificial per anticipar atacs cibernètics i prevenir vulneracions de seguretat, que Hulio, vestit de militar, va anunciar al públic des de la Franja de Gaza.[85]

Corsight AI és la desenvolupadora de la tecnologia de reconeixement facial que duen les càmeres amb les què l'exèrcit israelià vigila permanentment i graven els rostres de la població palestina de la Franja de Gaza,[86] especialment en els checkpoints que s'estableixen a les rutes per les que la població civil palestina fuig dels bombardejos. L'empresa, amb seu als Estats Units i al Regne Unit, posseeix filials a Israel. A Europa, té presència a Portugal, i subministra tecnologia a Suïssa. Corsight és propietat de l'empresa israeliana Cortica i de la venture capital canadenca Awz Ventures.[87]

En el sector de l'equipament militar, Agilite és una empresa israeliana fundada per ex-soldats israelians i estatunidencs, que fabrica l'equip tàctic i les armilles antibales usades per l'exèrcit israelià. Des del 7 d'octubre, ha anunciat repetidament l'ús del seu equip per part de l'exèrcit israelià en la invasió terrestre de la Franja de Gaza.[88] Un dels lemes amb què venen els seus productes és que "com a israelians, sempre hem hagut d'innovar per sobreviure i protegir les nostres famílies i la nostra pàtria. El nostre equip sempre ha hagut d'anar un pas per davant dels nostres enemics."[89]

No podem deixar d'esmentar Cellebrite DI Ltd, una desenvolupadora de programari amb seu a Israel, especialitzada en eines d'extracció de la informació[90]. El seu producte estrella és

83 Haaretz. (2023, 19 d'octubre). 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-fir ms-like-nso-aiding-israeli-efforts/0000018b-4813-de3d-a58f-c87b7d950000

84 Aleph. (s.f.). Shalev Hulio & Sebastian Kurz (Núm. 50) [Episodi de podcast d'àudio]. https://www.aleph.vc/content/shalev-hulio-sebastian-kurz

85 Gee, G. (2024, 18 de gener). 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. (s.f.). Corsight AI. https://www.whoprofits.org/companies/company/7383?corsight-ai

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

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

89 Agilite Europe. (s.f.). About us. https://agiliteinternational.com/pages/about-us

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

l'Universal Forensic Extraction Device (UFED), que desbloqueja telèfons mòbils i altres dispositius saltant-se el xifratge i les contrasenyes del dispositiu. Durant els atacs a la Franja de Gaza, Israel ha utilitzat –segons American Friends Service Committee (AFSC), citant un article de l'Hareetz– les eines de Cellebrite per recopilar dades dels telèfons de milers de palestins que van ser capturats i segrestats.[91] Cellebrite també hauria rebut finançament d'una unitat d'innovació del Pentàgon per desenvolupar un producte per cartografiar els túnels subterranis de la Franja de Gaza.92 [92] Alhora, aquesta tecnologia ha estat usada recentment per a penetrar telèfons d'activistes pro-palestins a països com Jordània.[93]

El juliol del 2025, el Ministeri de l'Interior espanyol va renovar la seva col·laboració amb aquesta empresa, que proveeix de tecnologia diversos cossos policials de l'Estat espanyol.[94]

4. El genocidi com a producte financer.

Les empreses que produeixen la tecnologia utilitzada en el genocidi i exportada a Europa no són els únics actors que estan obtenint beneficis d'aquesta situació de vulneració extrema del dret internacional. El genocidi a la Franja de Gaza ha esdevingut una oportunitat de negoci fructífera per al capitalisme financer. Fons i societats d'inversió internacionals, així com iniciatives de capital risc, inverteixen en l'ecosistema israelià d'startups i companyies tecnològiques, aportant capital a canvi d'una participació accionarial a l'empresa, amb l'expectativa de rendibilitzar la inversió si el negoci té èxit. Sigui com a accionistes de les principals empreses armamentístiques i tecnologies de seguretat a Israel, o finançant els fons d'inversió israelians que nodreixen de capital aquestes empreses, existeix tot un entramat financer global disposat a repartir-se els potencials beneficis econòmics generats per l'economia de xoc i guerra en què s'ha sumit Israel. Tot i que, com suggereix un article d'El Salto, "queda pendent conèixer amb més profunditat les xarxes financeres que han operat com a inversores o com a gestores" [95] del capital que es lucra amb el genocidi.

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

92 Shulman, S. (2024, 15 d'agost). 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 de gener). 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 d'abril). 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/

95 Fernández, L. T. i Anred. (2025, 16 d'agost). 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

Un dels casos més il·lustratius és el d'Elbit Systems, que va repartir, el 2024, 89 milions de dòlars en dividends als seus principals accionistes,[96] entre els quals hi ha fons d'inversió israelians com Clal Insurance Enterprises i Altshuler Shaham, i les estatunidenques The Vanguard Group (la major gestora de fons d'inversió del món), 1832 Asset Management L.P., Morgan Stanley i Goldman Sachs.[97] The Vanguard Group també és accionista de Clal Insurance, així com altres fons financers internacionals, com el britànic Phoenix Group.[98] Això vol dir que The Vanguard Group no només obté beneficis d'Elbit de forma directa com a accionista d'aquesta empresa, sinó també de forma indirecta, invertint en els fons financers israelians que permeten a les empreses de defence tech israelianes continuar funcionant.

És representatiu, també, el cas de Cellebrite, que compta entre els seus accionistes amb Morgan Stanley i Black Rock, la major gestora d'actius del món, així com amb el fons japonès Sun Corporation i els estatunidencs True Wind Capital Management i Axon Enterprise.[99]

Pel què fa al finançament de les startups, són representatius el cas de Corsight i Dream Security. En el cas de Corsight, el seu major inversor és Awz Ventures, una financera canadenca que té un acord amb el Ministeri de Defensa israelià per a finançar el desenvolupament de tecnologies basades en la IA al sector de seguretat al país.

XTEND Defense està finançada per les israelianes Protego Ventures i ClalTech, braç inversor de Clal Industries and Technologies, que alhora és propietat del fons d'inversió global estatunidenc Access Industries.[100] Al juliol de 2025, l'empresa va obrir una nova ronda de finançament de 30 milions d'euros, en la qual van participar Union Tech Ventures –el braç inversor del holding israelià Union Group–, el fons singaporès Chartered Group i les estatunidenques Aliya Capital Partners, amb seu a Miami, i Enkore International.[101] El principal inversor d'XTEND, Protego Ventures, creada per les reservistes de l'exèrcit israelià Lital Leshem i Lee Moser, es vanta de ser "la única venture capitalisraeliana liderada per dones i focalitzada en finançar equipament i programari militar

96 Elbit Systems. (2025, 25 de març). 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. (s.f.). Elbit Systems Ltd. (ESLT). https://www.marketscreener.com/quote/stock/ELBIT-SYSTEMS-LTD-6497555/company/

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

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

100 ClalTech. (s.f.). About us. https://claltech.com/about/

101 PitchBook. (s.f.). XTEND Defense. https://pitchbook.com/profiles/company/266230-09#signals

després dels atacs del 7 d'octubre".[102] Des de llavors, han recaptat 100 milions de dòlars per a empreses del sector defence tech.

En el cas d'empreses propietat de l'Estat d'Israel, com IAI i Rafael, la intervenció financera ha estat a través dels anomenats "bons de guerra israelians", préstecs directes a l'Estat que han augmentat significativament des de l'octubre de 2023 i que es van emetre específicament per cobrir els costos de la seva economia de guerra anunciant-los com a oportunitats per donar suport a "Israel en guerra".[103] Israel va emetre, el gener de 2025, bons d'aquest tipus per valor de 19.400 milions de dòlars. Una recerca de Profundo, BankTrack i Pax apunta a que Goldman Sachs ha subscrit més de 7.000 milions de dòlars en "bons de guerra" israelians des del 7 d'octubre de 2023. Les altres institucions financeres identificades en aquesta recerca com a subscriptores de bons són Bank of America, Deutsche Bank, BNP Paribas, Citi, Barclays i JPMorgan Chase.[104] Aquests préstecs per part d'institucions financeres internacionals haurien jugat un rol imprescindible en l'ofensiva a la Franja de Gaza".[105]

102 Shulman, S. (2024, 10 de desembre). 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. (s.f.). Israel at war. https://israelbonds.com/israel-at-war

104 BankTrack, PAX i Profundo. (2025, 14 de febrer). 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_ne w_research_finds

105 Follow the Money. (2025, 6 d'octubre). 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

Factors estructurals de la penetració empresarial israeliana a Europa.

En els darrers anys, nombroses empreses israelianes dels sectors armamentístics, ciberseguretat i tecnologies de doble ús, han orientat la seva expansió cap al mercat europeu. Aquesta estratègia respon a una combinació de factors econòmics, tecnològics, polítics i normatius. La seva implantació al continent els permet accedir a nous mercats, fonts de finançament i talent, mentre reforcen la seva reputació empresarial i "amaguen" la seva implicació en l'ocupació i el genocidi de Palestina.

Establir-se a Europa ofereix a aquestes empreses una proximitat directa amb clients institucionals estratègics: governs, forces armades, agències de seguretat i institucions de la UE i l'OTAN. El rearmament al continent amb plans com Rearm Europe, que augmenten de forma accelerada els fons públics i privats destinats a la seguretat i la indústria militar, representa un mercat potencial de gran interès pels propers anys. Aquesta iniciativa política es reflecteix en el Marc Financer Plurianual (MFP) —el marc que fixa els límits de despesa de la UE a set anys— amb un augment de cinc vegades dels recursos destinats a armament entre el període 2021–2027 i el 2028–2034.[106]

En aquest sentit, la presència territorial dins la Unió Europea facilita la participació en licitacions públiques, l'accés a contractes de recerca i desenvolupament (R+D) o a iniciatives de cooperació tecnològica que serien molt més difícils d'obtenir des d'Israel. Més important encara, tenir una seu en un Estat membre els permet operar lliurement dins el mercat únic europeu, sense barreres internes ni restriccions administratives. En aquests casos, les empreses poden presentar-se directament com a startups o proveïdores "europees" de tecnologia avançada, i així diluir la imatge associada al seu origen o a l'ús militar dels seus productes. Un mecanisme similar és la participació de centres de recerca i empreses israelianes en programes europeus de recerca i innovació, de vegades sota noves marques o mitjançant la compra d'empreses directament europees, com veurem en el cas d'Intracom Defense i IAI.

Com a exemple, el rècord que van assolir el 2024 les exportacions de l'indústria militar d'Israel, amb aproximadament un valor de 14,7 mil milions de dòlars, està fortament lligat amb la decisió d'accedir amb més força al mercat europeu.[107] El 54 % dels contractes signats al 2024 i que van ajudar a assolir aquesta xifra rècord, van ser amb països europeus.[108] Europa es consolida com el principal mercat d'exportació per a Israel en l'àmbit de la indústria militar, no només pel volum de contractes sinó també per la seva

106 Unió Europea. (2000, 21 de juny). 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 de juny). 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.

rellevància estratègica, fins al punt de poder considerar-se un actor clau en la sostenibilitat i expansió de l'ecosistema industrial militar israelià. [109]

L'ús d'intermediaris europeus és una altra tàctica habitual. En lloc d'operar directament sota la marca israeliana, les companyies recorren a consultores locals o integradors tecnològics que comercialitzen serveis i productes sota una altra identitat empresarial. Aquest mecanisme no només complica la traçabilitat cap a l'empresa matriu, sinó que facilita l'accés a contractes amb administracions públiques que, altrament, podrien rebutjar la col·laboració a causa de la seva vinculació amb el genocidi del poble palestí. A escala geoestratègica, l'obertura de filials a Europa permet reduir la dependència tradicional de l'Estat d'Israel amb el mercat nord-americà i posicionar-se dins un entorn regulador més diversificat.

En síntesi, les empreses israelianes de la indústria militar i ciberseguretat troben als diferents països europeus un entorn atractiu per expandir-se ja que tenen accés directe a clients institucionals, finançament d'R+D, capital humà qualificat i la possibilitat de millorar la seva reputació internacional, aprofitant aquests vincles que els permeten inserir-se en projectes europeus d'innovació i presentar-se com a startups pioneres en ciberseguretat, diluint així la seva procedència i trajectòria en l'ús de les seves tecnologies en la vulneració sistemàtica de drets humans.

1. Fuga d'empreses, especialistes i capital israelià cap al continent.

L'escalada militar a la regió, incloent els atacs iniciats per Israel i Estats Units a Iran, han provocat un gradual èxode de ciutadania israeliana a altres parts del món. Segons fonts oficials, l'any 2024, 82.700 persones originàries de l'Estat d'Israel van abandonar el país.[110] Europa és un dels principals destins d'aquesta migració i, dins d'Europa, Alemanya és el país que més població israeliana ha acollit en els darrers anys.[111]

Aquests moviments humans també impliquen trasllat de capital i d'empreses israelianes cap a Europa. Un dels principals sectors que està desplaçant les seves operacions i inversions és el tecnològic, un factor alineat amb el fet que Israel és un dels països amb més startups i projectes d'innovació del món. Ja al 2021 es registra el moviment de 912 empreses tecnològiques israelianes cap a Europa, majoritàriament del sector IT (tecnologies de la informació) i programari, i amb destinació principal a Alemanya, Països Bai-

109 Campaign Against Arms Trade. (2025, 7 de desembre). 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 de gener). Multi-front war caused emigration from Israel, Knesset report says. https://www.jpost.com/israel-news/article-840501

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

xos, França, Regne Unit i Espanya.[112] Algunes fonts també indiquen Xipre, especialment la costa de Limassol, com una de les destinacions preferents per a la migració empresarial israeliana.[113] Un informe recent de la Israel Innovation Authority, revela que una de cada cinc empreses tecnològiques del país han mogut les seves operacions a l'estranger des de l'inici del genocidi.[114] L'informe també identifica que el 50% de les startups israelianes podrien quedar-se sense finançament en 6 mesos degut a les dificultats que tenen per aconseguir capital des d'Israel. La cancel·lació de vols, les disrupcions de les operacions industrials, la mobilització de reservistes i la reticència del capital estranger a invertir a Israel, són algunes de les causes que forcen a les empreses israelianes a implantar-se a l'estranger per continuar les seves activitats i aconseguir finançament.[115]

Aquesta situació està també provocant un procés de "fuga de talent", és a dir, l'emigració de persones expertes del sector tecnològic israelià del país.[116] La Israeli Innovation Authority va registrar la sortida de 8.300 treballadors especialitzats del sector d'alta tecnologia entre l'octubre de 2023 i el juliol de 2024.[117] Molts d'aquests professionals provenen de grans empreses tecnològiques com Google o Intel, que són reubicats a les oficines internacionals d'aquestes empreses. Alhora, els hubs tecnològics europeus actuen com a pols d'atracció per accedir a noves oportunitats laborals. Entre aquests destaquen els hubs de París, Londres, Munich, Tallin, Estocolm, Amsterdam, Vilnius i Barcelona, entre d'altres.

2. Marc Regulatori Europeu.

L'atracció d'empreses israelianes de ciberseguretat cap a Europa s'explica, en part, per les característiques del marc legal i normatiu de la UE. D'una banda, es caracteritza per la desregulació creixent, la manca de rendició de comptes i per inconsistències entre diferents jurisdiccions. D'altra banda, la UE ofereix seguretat jurídica i unes directrius

112 EIT Health. (2021, abril). 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 de novembre). 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, 19 de gener). 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 de març). 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 d'abril). 2025 High-tech employment status report. https://innovationisrael.org.il/en/press_release/2025-high-tech-employment-status-report/

reguladores laxes que protegeixen els interessos i beneficis de les empreses. Tot plegat sota una retòrica de defensa de drets i de protecció al consumidor.

Tot i que la UE assegura que estableix relacions d'igualtat en les relacions comercials amb països del Sud global i que treballa per al desenvolupament sostenible, la realitat és que aplica una política de dobles estàndards: mentre que el marc regulador europeu prohibeix l'ús de sistemes tecnològics incompatibles amb els drets humans dins la UE, aquest mateix marc legal permet a empreses europees beneficiar-se de la venda fora de la UE de productes considerats de risc inacceptable, segons les pròpies normatives europees.[118]

La UE té també l'obligació legal de garantir que les seves polítiques, també les industrials i comercials, no contribueixen a la vulneracions de drets humans fora del seu territori. Tanmateix, en permetre l'exportació de tecnologies de vigilància que estan prohibides dins la UE, incompleix aquesta obligació i consolida una incoherència estructural de polítiques en contradicció amb els seus propis compromisos en matèria de drets humans.[119]

3. Domini d'una narrativa de securitització.

Malgrat l'elevat risc d'abús i les greus amenaces que les tecnologies de vigilància intrusiva representen per als drets fonamentals, així com la llarga trajectòria de denúncia i escrutini públic que les acompanya, resulta preocupant constatar que encara no existeix un marc jurídic adequat i sòlid que en reguli l'ús, ni en l'àmbit internacional ni en l'estatal. Malgrat la incidència des de la societat civil per establir garanties efectives dels drets i llibertats fonamentals, molts dels instruments de regulació —tal com es mencionarà en casos concrets a continuació— son propostes no vinculants o legislacions insuficients, caracteritzades per excepcions molt àmplies en el seu articulat.

En un moment de proliferació del mercat de la vigilància,[120] es fa més necessari que mai un marc regulador consistent que estableixi els límits i apliqui mecanismes suficients de control i rendició de comptes. La desprotecció existent permet que el sector privat operi dins d'un espai jurídic ambigu, marcat per la falta de transparència i les aliances recurrents amb l'àmbit militar (com és el cas d'Israel, amb empreses com NSO Group o Paragon). S'identifica, doncs, una estreta connexió entre les lògiques polítiques de la

118 Amnesty International i 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-t he-rest-of-the-world-joint-briefing/

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

120 European Digital Rights. (2025, juny). 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

securitització i l'articulació i manteniment d'un marc normatiu en què els drets humans i la seva protecció queden, a la pràctica, subordinats als interessos del lucre empresarial.

L'auge de la narrativa de la securitització a la UE es fonamenta en la construcció de la idea de "falta de seguretat" i d'existència d'un "perill exterior" del que cal defensar-se. Aquest relat s'ha cristal·litzat en instruments legislatius com el Reglament d'Intel·ligència Artificial de la UE, en el qual les qüestions relacionades amb la seguretat impliquen sempre excepcions jurídiques. D'aquesta manera, l'àmbit policial i l'àmbit fronterer (i, per tant, les autoritats que hi operen) queden exemptes dels principals mecanismes de control, transparència i supervisió previstos per la llei.[121] Aquest règim d'excepcionalitat contribueix a consolidar una cultura institucional de la vigilància i la criminalització, en què la noció de "seguretat nacional" preval sobre la protecció dels drets fonamentals.

4. Desregulació: desprotegir drets en nom de la "competitivitat"

En els darrers anys, a la UE s'ha anat imposant una creixent tendència desreguladora que busca desmantellar les normes per a les empreses que operen al seu territori. En l'àmbit tecnològic, sota el pretext de "simplificar procediments" i "afavorir la competitivitat del bloc europeu", aquesta agenda busca alliberar el sector privat d'obligacions i erosionar progressivament els sistemes de protecció de la societat civil front els riscos dels sistemes tecnològics, incloent la protecció contra la vigilància intrusiva.[122]

La penetració del sector tecnològic de la indústria militar en termes generals, però també d'Israel, als països de la UE es veu afavorida per un doble estàndard normatiu que combina, d'una banda, discursos avançats en matèria de drets fonamentals i, de l'altra, polítiques de seguretat, rearmament i interoperabilitat que prioritzen l'eficàcia militar i policial. Aquest desajustament ha estat àmpliament documentat en l'anàlisi crítica de la securitització europea, que posa de manifest com la seguretat esdevé un principi rector capaç de suspendre garanties jurídiques i ètiques.[123]

121 European Center for Not-for-Profit Law. (2024, agost). 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, novembre). 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

El 19 novembre de 2025, la Comissió Europea va presentar la Proposta de Reglament Òmnibus Digital que,[124] d'aprovar-se, permetria reobrir i modificar lleis tan fonamentals com el Reglament General de Protecció de Dades, el Reglament sobre la privacitat i les comunicacions electròniques (en anglès, ePrivacy), el Reglament d'Intel·ligència Artificial (AI Act), la Llei de Serveis Digitals (DSA), la Llei de Mercats Digitals (DMA) o la Directiva de Diligència Deguda en Sostenibilitat Corporativa (CSDDD-Corporate Sustainability Due Diligence Directive). En el moment de la redacció d'aquest informe, el procés encara es troba en una fase inicial de negociació pel seu contingut polèmic.

Tal com han denunciat més de 470 organitzacions de la societat civil d'arreu del món,[125] aquesta onada de desregulació sense precedents s'està negociant sense les mesures d'avaluació pertinents, excloent la societat civil i cedint davant d'actors empresarials que busquen rebaixar els estàndards dels drets humans, laborals, socials i del medi ambient en benefici propi.

Tant la deriva securitària com la desregulació legislativa evidencien la voluntat d'enfortir el sector privat i de transferir-hi recursos públics, amb conseqüències directes sobre la qualitat democràtica de la UE i dels seus Estats membres. Aquesta tendència no només afecta les normatives vigents, sinó que també sotmet qualsevol nova proposta legislativa a una revisió de "competitivitat".[126]

5. Marc jurídic europeu aplicable a les tecnologies de vigilància intrusiva

A la UE, l'aplicació de tecnologies digitals amb impacte en els drets fonamentals s'emmarca en un conjunt d'instruments jurídics que busquen establir els principis bàsics de protecció dels drets humans, privacitat i garanties democràtiques. Aquesta arquitectura està basada en el **C**onveni Europeu de Drets Humans i la Carta de Drets Fonamentals de la Unió Europea i, sobre el paper, estableix principis com la dignitat humana, la protecció de dades personals, la necessitat i proporcionalitat, la igualtat i la no-discriminació, i el dret a la tutela efectiva. En els darrers anys, aquesta arquitectura s'ha ampliat amb l'adopció de nous instruments sectorials d'aplicació en àmbits específics.

124 Comissió Europea. (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 Comissió Europea. (2024). Competitiveness. https://commission.europa.eu/priorities-2024-2029/competitiveness_en

Tanmateix, és important assenyalar que aquest marc regulador coexisteix amb pràctiques de contractació i cooperació que faciliten la incorporació de tecnologies desenvolupades en contextos d'ocupació, apartheid i genocidi, sovint sota la categoria de "doble ús". Des d'una perspectiva antiracista, aquest procés comporta el risc de traslladar lògiques colonials de vigilància i control a les polítiques europees de fronteres, d'ordre públic i de gestió de la protesta i la mobilització social. Tal com adverteix David Lyon, la vigilància contemporània no és neutral, sinó que tendeix a classificar i governar de manera diferencial les poblacions, reforçant processos d'exclusió i estigmatització[127].

Sense ànim d'exhaustivitat, alguns dels principals instruments legislatius que regulen l'ús de les tecnologies de vigilància intrusiva són: [128]

- Reglament (UE) 2021/821 del Parlament Europeu i del Consell, de 20 de maig de 2021,[129] que estableix un règim de control de les exportacions, la intermediació, l'assistència tècnica, el trànsit i la transferència de productes de doble ús. Des de la seva primera formulació l'any 1994, aquest reglament té com a objectiu controlar la transferència de béns i tecnologies susceptibles de tenir aplicacions tant civils com militars. L'actualització de 2021 va introduir avenços significatius, entre els quals destaca la incorporació d'un mecanisme catch-all que permet sotmetre a control determinades exportacions que no figuren expressament en les llistes de productes regulats als annexos del Reglament quan existeix un risc clar que aquestes puguin contribuir a vulneracions greus dels drets humans o del dret internacional humanitari. Tanmateix, continua presentant nombroses limitacions, com són:
    - Definicions amb zones grises que permeten interpretacions discrecionals.
    - Dependència excessiva en la bona fe dels exportadors i en els seus programes interns de respecte a les normes.
    - Els Estats tenen una capacitat desigual de supervisar aquest reglament, en funció de voluntat política, normes internes, pes internacional.
    - Diferents nivells d'aplicabilitat, que generen diferències substancials dins del mercat europeu.

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

128 A nivell europeu cal diferenciar: els Reglaments són instruments vinculants en tots els seus elements i s'apliquen directament a tots els estats membres, sense necessitat de cap llei nacional (ni transposició). Obliga tant els estats com els particulars (empreses, administracions, ciutadania). Les Directives son vinculants pel que fa als objectius que estableixen, però no s'apliquen directament sinó que cada estat està obligat a transposar-la al seu dret intern.

129 Reglament (UE) 2021/821 del Parlament Europeu i del Consell, de 20 de maig de 2021, pel qual s'estableix un règim de la Unió per al control de les exportacions, el corretatge, l'assistència tècnica, el trànsit i la transferència de productes de doble ús. (2021). Diari Oficial de la Unió Europea, L 206/1. http://data.europa.eu/eli/reg/2021/821/oj

Davant l'augment del comerç de tecnologies de vigilància, el 2024 la Comissió Europea va publicar una guia específica sobre l'aplicació del Reglament (UE) 2021/821[130] en matèria d'exportació de d'eines de ciberespionatge. Aquest document interpreta formalment que el règim de productes de doble ús també aplica a categories com el programari d'intrusió, els programes de monitoratge de comunicacions o les eines forenses, entre les quals s'inclou el programari espia comercial. No obstant això, la mateixa guia reconeix la seva incapacitat per afrontar la proliferació creixent de programari comercial, atesa la manca d'un sistema efectiu d'inspecció, la falta de transparència en les exportacions i la persistència de buits legals que permeten la seva producció i distribució des de la UE, que ja s'ha convertit en dels principals nodes mundials d'aquest mercat[131].

- En relació als controls d'exportació d'armes convencionals i altres productes de doble ús, el Reglament europeu es fonamenta parcialment en instruments internacionals com l'Acord de Wassenaar[132] **i** la Convenció 108 del Consell d'Europa sobre protecció de dades.[133] L'Acord de Wassenaar estableix llistes de control per a la transferència d'armes convencionals i béns de doble ús que constitueixen la base del marc normatiu europeu. Tanmateix, el seu caràcter no vinculant i l'absència de mecanismes coercitius han limitat greument la seva eficàcia. Després de dècades d'estancament, es considera un instrument obsolet i ineficaç per abordar la realitat tecnològica actual.[134] Mentre que la Convenció 108 del Consell d'Europa és la primera eina internacionalment vinculant sobre protecció de dades. La norma exigeix que qualsevol transferència de dades personals a tercers països incorpori salvaguardes adequades de drets humans. Tanmateix, la falta de mecanismes coercitius forts (no hi ha sancions per als Estats que incompleixen), la falta d'estàndards tècnics per a tecnologies altament intrusives, així com la dependència de l'aplicació a nivell estatal, fan que es tracti d'una eina insuficient per regular els riscos actuals de les tecnologies de vigilància.

130 Comissió Europea. (2024, 16 d'octubre). Commission publishes guidelines for cyber-surveillance exporters. https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en

131 Recomanació (UE) 2024/214 de la Comissió, de 15 de gener de 2024, sobre l'aplicació del Reglament (UE) 2021/821 pel que fa als productes de cibersuport. (2024). Diari Oficial de la Unió Europea, 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 Consell d'Europa. (1981, 28 de gener). Conveni per a la protecció de les persones pel que fa al tractament automatitzat de dades de caràcter personal (Sèrie de Tractats Europeus - Núm. 108). https://rm.coe.int/1680078b37

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

- El Reglament General de Protecció de Dades (RGPD) de la UE,[135] aprovat l'any 2016, és una norma de referència mundial pel que fa a la protecció de dades i estableix principis i barreres legals davant la recopilació i processament d'informació personal. Les dades biomètriques (característiques del rostre, iris, petjades dactilars, característiques de la veu, patrons de les venes, entre d'altres) són considerades com a especialment sensibles pel RGPD, que en prohibeix la recopilació i ús per part d'actors públics i privats, amb algunes excepcions.[136] En aquesta direcció, des del 2018 el RGPD estableix com a requisit obligatori avaluacions d'impacte en la protecció de dades, així com mesures de mitigació i protecció en els casos de risc per als drets i llibertats, com ara en l'aplicació de tecnologies de perfilació o monitoratge massiu en espais públics o privats (com ara els sistemes de reconeixement facial).[137]

  Totes les empreses que operen en el mercat europeu, encara que tinguin la seu fora de la UE, han de garantir el compliment estricte de les seves exigències. Això requereix sistemes tecnològics robustos per assegurar la privacitat, el control d'accessos, la traçabilitat i la resposta davant bretxes de seguretat. Per aquest motiu, el RGPD ha propiciat un mercat ampli per a solucions tecnològiques avançades, especialment en xifratge, gestió de dades i ciberseguretat preventiva.

  Tot i tractar-se d'un dels marc normatius més robustos en la protecció contra les tecnologies de vigilància, l'organització de drets digitals EDRi alerta que la seva implementació no ha estat uniforme ni efectiva en tots els països membres, que les agències estatals de protecció de dades no tenen recursos suficients per fer-lo complir i que, a la pràctica, això suposa una aplicació poc garantista a l'àmbit estatal.[138]

  A més de trobar-se sota el risc i la pressió esmentada de la tendència a la "simplificació" legislativa a l'UE, que podria afeblir alguns dels pocs mecanismes legals que permeten a la societat civil impugnar els abusos de governs i empreses,[139] el RGPD no va ser dissenyat per regular sistemes de vigilància basats en la IA. Per aquest motiu, no inclou normes específiques en aquest àmbit i deixa buits de protecció que haurien de ser coberts pel Reglament d'Intel·ligència Artificial.

135 Comissió Europea. (2022, 28 d'octubre). Protecció de les dades personals (a partir de 2018). EUR-Lex. https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

136 European Digital Rights. (2020). Ban biometric mass surveillance (Position paper). https://edri.org/wp-content/uploads/2020/05/EDRi-Ban-Biometric-Mass-Surveillance.pdf

137 Lafede.cat, IA Ciudadana, i Algorace. (2024). Automatización del control y vigilancia biométrica en el espacio público: Un análisis desde los derechos y las resistencias. https://lafede.cat/wp-content/uploads/2024/03/Automatizacion-del-control-y-vigilancia-biometrica.pdf

138 European Digital Rights. (2020). Ban biometric mass surveillance (Position paper). https://edri.org/wp-content/uploads/2020/05/EDRi-Ban-Biometric-Mass-Surveillance.pdf

139 European Digital Rights. (2025, novembre). 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

- La Directiva 2016/680 del Parlament Europeu i el Consell sobre la protecció de dades en l'àmbit penal i policial [140] entra en vigor conjuntament i de forma complementària al RGPD i seguint els mateixos principis de protecció de dades com a dret fonamental. En ple funcionament des de 2018, la Directiva estableix les normes de processament de dades personals per part de les autoritats encarregades de fer complir la llei en procediments penals, quan es duen a terme amb fins d'aplicació de la llei (la prevenció, la detecció o la persecució de delictes).[141] Així, doncs, suposa un règim especial per al sector policial que, a diferència del que estableix el RGPD, no està basat en el consentiment però que igualment obliga a que les dades es tractin segons criteris d'estricta necessitat. Igual que el RGPD, les dades especialment sensibles (incloent les biomètriques) han de complir una llarga llista de salvaguardes i garanties i es prohibeix el processament massiu i indiscriminat de dades de la societat civil.[142] Tal com alerta EDRi, tot i que la Directiva requereix de justificacions molt sòlides per al tractament de dades policials, a la pràctica no es compleixen les garanties de forma efectiva i existeix una falta greu de mecanismes de transparència i control. Alhora, la Directiva no s'aplica de forma harmònica en tots els països membres i el solapament entre el RGPD i la Directiva de protecció de dades en l'àmbit penal i policial implica ambigüitats i zones grises que permeten utilitzar buits legals per justificar l'aplicació de tecnologies de vigilància.[143]

- El Reglament europeu d'Intel·ligència Artificial [144] és el primer instrument vinculant i específic sobre Intel·ligència Artificial a la UE i es vincula al RGPD pel que fa al tractament i processament de dades personals. En vigor des de l'agost de 2024, la seva implementació es desplega de forma gradual fins a l'agost del 2026, quan ha d'estar completament en aplicació (tot i una pressió creixent per suspendre o retardar la seva implementació per part de les mateixes institucions europees i com a part de l'agenda de desregulació).

  El Reglament classifica els sistemes d'IA en quatre categories de risc: inacceptable, alt, limitat i mínim; segons les quals s'estableixen obligacions específiques per agents

140 Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals per part de les autoritats competents a efectes de prevenció, investigació, detecció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades. (2016). Diari Oficial de la Unió Europea, L 119/89. http://data.europa.eu/eli/dir/2016/680/oj

141 European Digital Rights. (2020, maig). Ban biometric mass surveillance (Position paper). https://edri.org/wp-content/uploads/2020/05/EDRi-Ban-Biometric-Mass-Surveillance.pdf

142 European Digital Rights. (2020, maig). Ban biometric mass surveillance (Position paper). https://edri.org/wp-content/uploads/2020/05/EDRi-Ban-Biometric-Mass-Surveillance.pdf

143 European Digital Rights. (2020, maig). Ban biometric mass surveillance (Position paper). https://edri.org/wp-content/uploads/2020/05/EDRi-Ban-Biometric-Mass-Surveillance.pdf

144 Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial (Llei d'intel·ligència artificial). (2024). Diari Oficial de la Unió Europea, L 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

proveïdors i per a desenvolupadors, respectivament.[145] Tot i que les tecnologies de vigilància intrusives queden classificades com a risc inacceptable o risc molt alt, el Reglament permet a la UE desenvolupar i exportar sistemes d'IA prohibits per la seva incompatibilitat amb els drets humans, com ja s'ha documentat en la venda de tecnologies de reconeixement facial a Israel.[146] A la UE, els sistemes classificats com de risc inacceptable queden prohibits per la norma, que n'impedeix el desenvolupament i venda dins de la UE. Es tracta, per exemple, de: sistemes de puntuació social, sistemes de manipulació ciutadana o de reconeixement d'emocions en l'àmbit acadèmic o laboral, entre d'altres.[147]

Tanmateix, tal com alerta la coalició d'organitzacions IA Ciudadana, les nombroses excepcions i buits a les prohibicions (especialment en l'àmbit penal, policial i migratori) permeten l'aplicació de tecnologies de vigilància massiva i de discriminació que posen greument en risc els drets humans, com son:

- Reconeixement biomètric a l'espai públic en temps real (com ara càmeres de reconeixement facial): aquests sistemes no queden del tot prohibits i es poden utilitzar en supòsits de: cerca de persones, prevenció del terrorisme o identificació de persones sospitoses d'un delicte greu.
- Reconeixement biomètric a l'espai públic: està permès per part d'agents encarregats de fer complir la llei, amb autorització judicial o només administrativa[148].
- Reconeixement d'emocions: aquests sistemes d'inferència d'emocions, que no tenen cap base científica, es poden aplicar sempre que no sigui en l'àmbit laboral o acadèmic.
- Avaluació i perfilat en context fronterer: com ara sistemes d'anàlisi predictiu per prevenir la migració o polígrafs amb IA.[149]

Les tecnologies considerades d'alt risc estan sotmeses a una sèrie d'obligacions especials (de gestió de riscos, de governança de dades, de documentació tècnica, transparència, etc.), excepte quan són utilitzades per part d'agents encarregats de fer com-

145 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

146 Amnistia Internacional i European Digital Rights. (2023). Toxic double standards: How the EU's exports of surveillance technology are damaging human rights abroad. https://www.amnesty.org/en/documents/eur01/7161/2023/en/

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 El reconeixement biomètric ex post és una pràctica que es duu a terme després que hagin tingut lloc els fets.

149 IA Ciudadana. (2024, 18 de juny). 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-est andar-adecuado-de-proteccion-de-los-derechos-humanos/

plir la llei. Com a resultat de l'estratègia de lobby per part de la indústria tecnològica, a més, el Consell i Parlament Europeus van incloure una via que permet que siguin els mateixos proveïdors els qui decideixen si els seus productes son d'alt risc o no.[150]

De manera transversal, el Reglament d'IA eximeix d'obligacions de transparència i rendició de comptes a tots els sistemes d'IA creats i desenvolupats per "motius de seguretat nacional", eliminant qualsevol salvaguarda de drets sota aquest supòsit genèric.[151]

Tal com alerten les organitzacions en defensa dels drets, les llacunes en les prohibicions i obligacions de control en sistemes d'IA són altament perillosos per als drets humans, així com les deficiències estructurals del Reglament en aspectes clau com la classificació de risc, perquè obren perillosament la porta a formes de l'ús de tecnologies de vigilància intrusiva dins de la UE.[152]

Altres instruments legislatius que incideixen en la regulació sobre l'ús de tecnologies de vigilància són:

- La European Media Freedom Act (EMFA).[153] Aquesta legislació, adoptada el 2024 i en vigor des de l'agost de 2025, té com a objectiu establir un marc comú per protegir la llibertat i el pluralisme dels mitjans de comunicació dins la UE. Tanmateix, el text final de l'EMFA incorpora un règim d'excepció que permet l'ús de programari espia contra periodistes i fonts periodístiques sota determinades circumstàncies, com ara motius de "seguretat nacional" o "investigació d'infraccions greus". Aquest articulat, en particular l'Article 4, reprodueix un ambient de permissivitat que amenaça directament la llibertat de premsa, ja que obre la porta a pràctiques de vigilància sobre figures especialment protegides per l'Estat de Dret. Així, segons la legislació europea vigent, es pot arribar a utilitzar programari espia contra periodistes.

  Durant el procés legislatiu, diverses organitzacions de drets digitals i llibertats civils, com Access Now, EDRi o Reporters Without Borders,[154] van advertir sobre els riscos d'aquest enfocament i van demanar la prohibició absoluta de l'ús de programari espia con-

150 Ibid.

151 European Digital Rights. (2024, 15 de març). 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/

152 IA Ciudadana. (2025, març). 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 Comissió Europea. (s. d.). European Media Freedom Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democrac y/european-media-freedom-act_en

154 European Centre for Press and Media Freedom. (2023, 22 de juny). 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-s urveillance-in-the-emfa/

tra periodistes. No obstant això, la seva proposta va ser finalment desestimada i el text adoptat manté excepcions que en permeten el seu ús, amb un llenguatge ambigu que no resol de manera clara quan és admissible. Aquesta redacció no només contradiu l'esperit de protecció que inspira la norma, sinó que crea un precedent perillós en l'àmbit europeu: la normalització de l'ús d'eines de vigilància digital contra actors essencials per al funcionament democràtic, com són els periodistes i els mitjans de comunicació independents.

- El Pall Mall Process és un codi de pràctica de caràcter voluntari, adreçat als Estats, amb l'objectiu d'abordar "la proliferació i l'ús irresponsable de les capacitats comercials d'intrusió cibernètica".[155] Impulsat pel Regne Unit i França en un procés iniciat el febrer de 2024,[156] que va reunir representants d'Estats, empreses i organitzacions de la societat civil. El procés va entrar en vigor l'abril de 2025 amb la signatura de la Declaració. A data d'aquest informe, s'han elaborat dos documents, una declaració i un codi de pràctica per als Estats, als quals s'han adherit un total de 27 països, 19 dels quals pertanyen a la Unió Europea, entre els quals no figura l'Estat espanyol.

  Tot i que ambdós documents parteixen d'una voluntat constructiva per abordar "com l'ús de programari espia comercial pot debilitar la seguretat nacional, els drets humans, la pau internacional i l'estabilitat de l'espai cibernètic", el seu caràcter voluntari genera dubtes significatius sobre l'eficàcia real que poden tenir com a instruments per frenar els abusos associats a aquestes tecnologies o per impulsar canvis substancials en les polítiques i pràctiques dels Estats adherits. A més, des del seu inici, organitzacions de drets humans, com EDRi, han alertat que aquests documents podrien contribuir a legitimar l'ús de determinats tipus de programaris. Ara, d'ençà de la seva aprovació i adhesió per part de més de 21 països, es continua monitoritzant el procés per identificar ingerències.[157]

  En l'actualitat, el procés corre el risc de no assolir els seus objectius i malgrat no ser vinculant, de quedar reduït a un marc excessivament general i diplomàtic, que ni és aplicable de manera efectiva ni reflecteix la realitat creixentment preocupant del sector, ni els riscos i danys documentats en relació amb l'ús de programari espia. És important mencionar que, a causa del seu caràcter voluntari i ampli, ja s'han començat a documentar ingerències en el seu ús o abús amb la voluntat de sabotejar-lo i instrumentalitzar-lo. El 7 de gener de 2026, NSO Group va mencionar, en el seu Informe Anual de Transparència, la seva participació en el Procés de Pall Mall per justificar el seu compliment amb els drets humans, una

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

156 Ministry for Europe and Foreign Affairs. (2024, 6 de febrer). 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-pr oliferation-and-irresponsible-use-of

157 European Digital Rights. (2025, juny). 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

afirmació que va ser immediatament negada pels governs francès i britànic, els quals van confirmar que l'empresa israeliana no havia format part de cap conversa.[158] Una vegada més, es posa de manifest que, malgrat el pas dels anys i l'agreujament del problema, continua absent un marc regulador obligatori capaç d'afrontar aquestes situacions.

- La Directiva SRI 2. En vigor des del gener de 2023, reforça substancialment les obligacions de ciberseguretat en sectors considerats crítics (com l'energia, el transport, la sanitat, les telecomunicacions o les infraestructures digitals).[159] En aquest marc, milers d'empreses europees estan obligades a adoptar mesures avançades de protecció, resposta a incidents i gestió de riscos. Aquest marc regulador està impulsant una demanda creixent de serveis i tecnologies de ciberdefensa, generant oportunitats per a proveïdors especialitzats, inclosos empreses estrangeres amb alta capacitat d'innovació.

- La Llei europea de Ciberresiliència (Cyber Resilience Act – CRA).[160] Va entrar en vigor a finals de 2024 i exigeix que els productes digitals (tant maquinari com programari) incorporin la seguretat des del disseny i mantinguin actualitzacions de protecció durant tot el seu cicle de vida. També requereix sistemes de certificació per verificar que aquests productes compleixen estàndards d'alta seguretat.[161] Aquesta normativa potencia la demanda d'empreses capaces d'oferir solucions de defensa digital, auditories de seguretat, eines de monitoratge i serveis d'actualització contínua. Un dels principals riscos és que, per complir amb les noves exigències de seguretat, els fabricants puguin incorporar mecanismes de control remot o de monitoratge permanent dins dels productes digitals. Aquestes funcionalitats, tot i estar justificades en clau de protecció, poden derivar en formes de vigilància constant sense prou garanties democràtiques. La Electronic Frontier Foundation apunta un possible impacte indirecte sobre la llibertat d'expressió, ja que els dispositius connectats podrien limitar l'accés a determinades funcionalitats o continguts sota el pretext de la seguretat.[162] Aquest marc legal incrementaria la capacitat d'intervenció tècnica (i, eventualment, política) sobre el dret a comunicar i a rebre informació en l'entorn digital.

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

159 Comissió Europea. (s. d.). Directiva sobre medidas para lograr un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2). Estratègia Digital de la UE.
https://digital-strategy.ec.europa.eu/es/policies/nis2-directive

160 Comissió Europea. (s. d.). Cyber Resilience Act. Estratègia Digital de la UE.
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

161 European Digital Rights. (2022, 12 de desembre). 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 de maig). 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

Tot plegat configura un sistema normatiu insuficient i fragmentat, incapaç a dia d'avui de donar resposta adequada als riscos de les tecnologies de vigilància intrusiva per als drets fonamentals. Persisteixen buits legals importants, excepcions àmplies en nom de la seguretat nacional, mecanismes de supervisió febles i una manca de recursos per a les autoritats encarregades de fer complir les garanties existents. Alhora, els mecanismes de participació de la societat civil son gairebé inexistents i es constata la contradicció entre els compromisos de la UE en matèria de drets i la permissivitat amb l'exportació de tecnologies de vigilància que no són admissibles dins del seu propi territori. A aquestes limitacions s'hi afegeix l'actual agenda de desregulació, que amenaça amb erosionar els estàndards actuals del marc digital europeu.

V

Portes d'entrada de les empreses israelianes del sector *defence tech*.

1. El rearmament europeu a través de l'OTAN i del Pla *Rearm Europe*

El nou pla de despesa militar de l'OTAN fins al 2035, preveu un increment de fins al 5% del PIB dels pressupostos estatals en defensa. Una part molt significativa d'aquesta despesa es destinarà al desenvolupament de tecnologia militar i de seguretat.[163] Paral·lelament, el pla Rearm Europe, presentat per la Comissió Europea el març de 2025, proposa la mobilització de 800.000 euros addicionals en despesa militar dels Estats membre de l'UE.[164] El Pla, que té com a objectiu reforçar l'autonomia estratègica europea en matèria d'armament davant aliats i competidors externs, fixa que un 65% dels components del nou armament han de tenir origen a la UE o a països associats. Aquest marge del 35% d'obertura a la col·laboració amb Estats no membres pretén compensar les actuals mancances de la indústria militar europea en determinades tecnologies, que podria acabar afavorint una major cooperació amb empreses i proveïdors tecnològics d'Israel. Com hem mencionat anteriorment, aquesta iniciativa política es reflecteix, entre d'altres, en la proposta de la comissió d'augmentar el pressupost de defensa en els Fons Europeu de Competitivitat en 131.000 milions d'euros pel període 2028-34.[165]

Pel que fa a l'OTAN, el gener del 2025, el secretari general de l'OTAN, Mark Rutte, declarava: "Ara veus drons ucraïnesos de 400 USD destruint tancs russos que costen diversos milions de dòlars. La rapidesa és essencial, no la perfecció, per incorporar aquestes noves tecnologies".[166] Aquestes declaracions polítiques es tradueixen en documents de l'organització transatlàntica com Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies (2021), que prioritza nou àrees tecnològiques: l'IA, els sistemes autònoms, les tecnologies quàntiques, la biotecnologia i les tecnologies per a la millora humana, les tecnologies espacials, els sistemes hipersònics, els nous materials i la manufactura avançada, l'energia i la propulsió, així com les xarxes de comunicació de nova generació.[167]

163 Unidos por Israel. (2024, 11 de setembre). 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-defen sa-israeli-atrayendo-el-interes-mundial/

164 Comissió Europea. (s. d.). Future of European defence. https://commission.europa.eu/topics/defence/future-european-defence_en

165 Comissió Europea. (2024). La cooperación de la UE en materia de defensa: Hacia una Unión Europea de Defensa. Oficina de Publicacions de la Unió Europea. https://op.europa.eu/en/publication-detail/-/publication/06a73675-d5d4-11f0-8da2-01aa75ed71a1

166 Rutte, M. (2025, 10 de juny). Building a Better NATO [Discurs]. Chatham House, Londres. Transcripció oficial de l'OTAN. 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

Per implementar aquesta transformació tecnològica, l'OTAN ha creat diversos instruments, entre els quals destaquen el Defence Innovation Accelerator for the North Atlantic (DIANA), el NATO Innovation Fund o el NATO-Ukraine Innovation Cooperation Roadmap. Aquests nous instruments estan, al seu torn, facilitant l'augment de la producció militar als Estats europeus i l'atracció sense precedents d'empreses del sector defence tech i de seguretat tecnològica cap a Europa, moltes d'elles israelianes.

Interoperabilitat: el camí a la contractació i la producció massiva

L'OTAN centralitza la contractació conjunta d'armament i d'altres productes militars i logístics a través de la NATO Support and Procurement Agency (NSPA). Aquest sistema estableix requisits militars i operacionals per complir amb els estàndards de l'organització, així com obligacions en matèria de control d'exportacions de la UE.[168] Paral·lelament, el Defence Production Action Plan (DPAP) de 2023 defineix les operacions per a la producció massiva de municions i armament en cooperació amb l'indústria militar europea.[169] En aquest marc, la interoperabilitat de les tecnologies amb el nou armament de l'organització transatlàntica és un requisit fonamental per a la seva posterior contractació.

Una manera d'assolir aquesta interoperabilitat és que un Estat membre de l'OTAN incorpori prèviament aquesta tecnologia i armament en la seva arquitectura militar. Per exemple, el 2023, Alemanya va adquirir el sistema Arrow-3 de IAI per a la seva intercepció de míssils; aquesta integració va suposar la incorporació d'aquesta tecnologia a la European Sky Shield Initiative (ESSI), un sistema per al desenvolupament de capacitats aèries i d'intercepció de míssils europeu liderat per Alemanya en agrupació amb diversos països de l'UE.[170] Dos anys més tard, l'OTAN va adquirir el sistema Arrow-3.[171]

De manera similar, Elbit Systems i Rafael Advanced Defense Systems, fa anys que transfereixen les seves tecnologies i armament a l'OTAN. En ocasions, l'accés d'aquestes empreses es produeix de la mà d'empreses europees, com és el cas de la joint venture cre-

168 White & Case. (2024, 25 de gener). 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 de febrer). 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 Cambra de Comerç i Indústria Alemanya-Israel (AHK Israel). (2023, 28 de setembre). Germany signs nearly $4 billion deal for Israel's Arrow 3 missile defense system. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/updated-defence-production-action-plan

171 Arvizo, A. (2025, 22 d'agost). 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/

ada entre IAI i Airbus per desplegar el dron Heron TP des de l'OTAN.[172] Aquests contractes impulsen la instal·lació de plantes de producció militar a territori europeu. El 2004, Elbit Systems va crear una filial al Regne Unit, sota la denominació Elbit Systems UK Limited, per establir plantes de producció a Brighton, South Wales, Leicester, entre d'altres. Des de llavors, aquesta empresa israeliana ha rebut nombroses adjudicacions del govern britànic per al subministrament de drons i altres serveis. El 2025, una potencial adjudicació d'un servei de capacitació per a les Forces Armades britàniques valorat en 2 mil milions de lliures (aprox. 2,27 milions de euros) va provocar un gran debat polític.[173] Finalment, el contracte va ser concedit a l'empresa militar estatunidenca Raytheon.[174]

L'armament de les principals empreses militars israelianes, incorpora altres tecnologies desenvolupades per empreses menors però en fase de creixement. Per exemple, la start-up israeliana NextVision, especialitzada en càmeres d'alta precisió per a drons d'empreses com IAI, Rafael o Elbit Systems,[175] està certificada amb el Blue UAS Framework, un mecanisme d'interoperabilitat per a components de drons, fet que li permet accedir a contractes del govern dels Estats Units i de l'OTAN.[176] NextVision s'ha lucrat amb el genocidi a la Franja de Gaza i actualment es troba en fase d'expansió a Europa,[177] com mostra el fet que el 55% dels beneficis que ha obtingut al llarg de l'any 2025 provenen del mercat europeu, i que l'OTAN és un objectiu comercial clar, tal com evidencien els seus informes empresarials.[178]

Cas: l'Accelerador d'Innovació en Defensa per a l'Atlàntic Nord (DIANA)

L'any 2023, l'OTAN va crear DIANA, un accelerador descentralitzat per impulsar la innovació tecnològica militar amb centres a Londres, Halifax i Tallinn. La xarxa permet desenvolupar tecnologies de doble ús per ser després adquirides per l'Aliança Atlàntica. DIANA

172 Stenglin, W. (2025, 23 de juliol). 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

173 UK Parliament. (2025, 23 de juny). 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 de gener). 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. (s. 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%9F2-202 5FS_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%9F2-202 5FS_300625_isa.pdf

178 NextVision. (2025, agost). NextVision 1H-2025 Results Presentation [Presentació de resultats]. 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

selecciona cada any startups i pimes en àmbits com resiliència energètica, vigilància, infraestructures crítiques, sistemes d'informació segurs i salut. Durant un any, les empreses reben finançament, accés a centres de testatge, connexió amb actors de la indústria militar i seguretat, i mentoria per adaptar les seves solucions als requisits de l'OTAN.

En les dues úniques edicions del programa d'acceleració realitzades fins ara s'observen vincles amb empreses israelianes. L'any 2024, l'empresa estatunidenca Zepher Flight Labs, especialitzada en disseny i producció de drons, va beneficiar-se del programa DIANA.[179] Un any més tard, l'empresa va ser adquirida per la startup israeliana Heven Drones, especialitzada en el desenvolupament de drons propulsats amb hidrogen per al sector militar.[180] A la seva pàgina web corporativa, l'empresa indica que l'exèrcit israelià és un soci estratègic.[181] En l'edició del 2025, observem la participació de la filial britànica de SB Technologies,[182] SB Tech UK Ltd,[183] que té com a soci estratègic l'empresa israeliana XM Cyber per desenvolupar i comercialitzar conjuntament la tecnologia de ciberseguretat CTEM (Continuous Threat Exposure Management). XM Cyber és una empresa fundada per l'ex-alt càrrec del Mossad Tamir Pardo. Des de 2021, XM Cyber forma part del consorci Israeli Operational Technologies Cyber, liderat per l'empresa Rafael Advanced Defense Systems. El consorci té per objectiu subministrar solucions tecnològiques per la protecció d'infraestructures crítiques d'Israel a través de l'acord Cyber Emergency Response signat amb el govern d'Israel.[184] Actualment el grup alemany Schwarz Group és propietari de XM Cyber.[185]

Alhora, DIANA coopera amb 20 ecosistemes d'innovació[186] i 180 centres de testatge (laboratoris, camps d'assaig, centres de ciberseguretat, etc.) situats en països membre de

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 d'abril). 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-adv anced-drone-technology-302437947.html

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

182 ATO 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. (s. 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 de juny). Rafael sets up first-of-its-kind Israeli cyber consortium with leading cyber solution partners [Nota de premsa]. https://xmcyber.com/press-release/rafael-sets-up-first-of-its-kind-israeli-cyber-consortium-with-leading-cyber-solution-partner s

185 Ben-David, R. (2021, 22 de novembre). 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. (s. d.). Accelerator sites and test centres. Defence Innovation Accelerator for the North Atlantic. https://www.diana.nato.int/accelerator-programme.html#accsites

l'OTAN.[187] Un d'aquests és l'Institut Nacional de Ciberseguretat d'Espanya (INCIBE), que des de l'inici del genocidi a la Franja de Gaza el 2023, ha participat en fires de ciberseguretat a Israel (CyberTech Global 2025) i ha organitzat trobades amb empreses israelianes durant el 2024.[188] Una d'elles és una reunió d'INCIBE amb l'empresa Dream Security, creada per Shalev Hulio fundador d'NSO Group, en què aquesta li va oferir comprar la seva tecnologia.[189]

Un altre espai estratègic de l'OTAN és el hub de coordinació i desenvolupament tecnològic de Tallin.[190] Estònia ha apostat per esdevenir un pol de tecnologies disruptives, és a dir, aquelles que alteren mercats, empreses i patrons de consum, i atraure empreses d'arreu del món, creant un sistema d'e-Residency mitjançant el qual grups o individus poden registrar una empresa en qüestió de minuts. A més, el Govern d'Estònia i l'Estonian Centre for Defence Invesment estant creant un centre de testatge de tecnologies militars i producció de munició a la base militar d'Ämari, el Defence Industry Park.[191] En aquest context, al novembre del 2025, el govern d'Israel va inaugurar una nova ambaixada a Estònia per reforçar els llaços polítics i econòmics entre els dos països.[192] L'esdeveniment va estar acompanyat per l'organització d'un Fòrum de Negocis Estònia-Israel que va comptar amb la visita de més de 50 empreses del sector de ciberseguretat i aramamentístic d'Israel.[193]

Amb aquestes condicions, Estònia es posiciona com una porta d'entrada d'empreses del sector defence tech a Europa. A la presència i relacions de les grans empreses armamentístiques israelianes amb el govern d'Estònia, com IAI,[194] se suma també l'aterratge d'empreses de tecnologia de seguretat. Un exemple és l'empresa de ciberseguretat

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

188 INCIBE. (2018, 11 de maig). 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

189 El Confidencial Digital. (2025, 11 de setembre). 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/20250 910171218979303.html

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

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

192 Estonian World. (2025, 12 de març). 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 de novembre). 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 d'octubre). 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

Cyberbit, implicada en la vigilància massiva de la població palestina i activistes d'arreu del món,[195] i que al 2025 va adquirir l'empresa estoniana Rangefour, reforçant així la seva presència al país.[196]

2. La guerra a Ucraïna i la penetració d'empreses israelianes per l'Est d'Europa

Una part important de l'augment dels pressupostos de defensa europeus es destina a comprar armes i tecnologia militar per a Ucraïna. L'instrument NATO Prioritised Ukraine Requirements List (PURL) coordina les necessitats ucraïneses a nivell militar i tecnològic amb els inventaris europeus i estatunidencs. Alexus Grynkewich, Comandant Suprem Aliat de l'OTAN a Europa va declarar: "els ucraïnesos ens fan saber quins són els seus requeriments. Nosaltres ho traslladem a un grup de treball conjunt entre el Comandament Europeu dels EUA i l'OTAN que eleva aquestes necessitats."[197] Per tant, les empreses defence tech internacionals que operen a Ucraïna, proven les seves tecnologies en el terreny de combat i entren en contacte amb els militars ucraïnesos, tenen més oportunitats per accedir a contractes amb l'OTAN.[198]

La presència d'empreses israelianes a Ucraïna s'ha expandit per diversos canals. D'una banda, mitjançant acords directes amb el govern ucraïnès, com en el cas del Ministeri de Defensa i Elbit Systems. D'altra banda, empreses internacionals participen en plataformes d'innovació militar com Brave 1, com és el cas de l'empresa israeliana R2.[199] Paral·lelament, es formen aliances empresarials directes entre actors israelians i ucraïnesos, com succeeix amb Dronex Israel, que a més col·labora amb l'exèrcit israelià a través de la MAFAT Directorate of Defense, Research and Development.[200]

195 Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., i Deibert, R. (2017, 6 de desembre). 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 de maig). Cyberbit acquires RangeForce: Creating the world's leading cyber defense skills and readiness platform [Nota de premsa]. https://www.cyberbit.com/news/cyberbit-acquires-rangeforce/

197 Tucker, P. (2025, 28 d'agost). 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/4077 79/

198 Ibid.

199 Czerny, M. (2024, 19 de novembre). 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-drone s/

200 Ibid.

XTEND, la cara oculta de l'emergència de l'indústria del drons

La tecnologia de drons de l'empresa XTEND, tal com s'ha exposat a l'apartat anterior, ha estat utilitzada de manera massiva per l'exèrcit israelià en el genocidi a la Franja de Gaza.[201] La formalització de contractes milionaris amb el govern d'Israel [202] ha reforçat el seu posicionament i n'ha impulsat la projecció internacional.[203] En paral·lel, l'empresa preveu escalar la producció fins a 4,5 milions d'unitats destinades a Ucraïna.[204] Recentment, el seu director executiu també ha anunciat l'interès d'accedir al mercat de l'OTAN,[205] amb l'objectiu d'ampliar la comercialització cap a àmbits de seguretat i policials.[206]

Per poder assolir aquests objectius, XTEND ha desenvolupat una estructura empresarial a Estats Units i Europa. Als EUA, l'empresa hi ha establert la seva base de producció massiva de drons.[207] Mentre que a Europa la seva estructura es basa en un entramat d'oficines comercials i xarxes de distribució de productes a Regne Unit, Països Baixos, Alemanya i Est d'Europa.[208] La penetració d'XTEND al continent europeu ha combinat projectes de recerca CORDIS,[209] la participació en exhibicions militars —com la conferència LANDEURO a Wiesbaden (Alemanya) el juliol de 2025 i la realització de showcases i simulacions arreu d'Europa. A Espanya, l'any 2020 va dur a terme una demostració del sistema Skylord Hunter amb la participació dels Ministeris d'Interior i de Defensa.[210] Per últim, al Regne Unit, ha realitzat proves exclusives amb l'exèrcit britànic i l'industria militar del país.[211]

---

201 AFSC. (s. d.). XTEND. Investigate. Recuperat el 3 d'octubre de 2025, de https://investigate.afsc.org/company/XTEND

202 SOFX. (2024, 5 de juny). 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 de gener). 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/

204 Avigad, D. (2025, 4 de setembre). 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 d'agost). 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 de setembre). 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 de juliol). XTEND accelerates its global expansion and product development. https://techtime.news/2025/07/04/XTEND-4

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

209 Comissió Europea. (s. d.). SKYLORD: A new generation of aerial robotic systems for first responders (Projecte ID 887959). CORDIS. https://cordis.europa.eu/project/id/887959

210 UAS Weekly. (2020, 5 d'octubre). 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-syste ms/

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

Transferència de tecnologia ucraïnesa a Israel: el cas de Zvook

Les tecnologies disruptives utilitzades a Ucraïna estan generant també un interès creixent a Israel. Un exemple és Zvook, una startup ucraïnesa que desenvolupa sistemes de detecció acústica de drons, míssils i altres amenaces aèries mitjançant intel·ligència artificial que, segons el seu director, Maryan Sulym, poden detectar drons Shahed de fabricació iraniana en un radi de 3 a 5 km, i míssils de creuer en un radi de 5 a 7 km. Segons Sulym, tres empreses israelianes de tecnologia armamentística ja s'han posat en contacte amb Zvook per explorar possibles col·laboracions.[212]

Organitzacions ucraïneses com la Global Israel Initiative (GII)[213] promouen les relacions entre sectors defence tech dels dos països per intercanvi de tecnologia, aliances i recerca conjunta. Al portafoli de socis de GII, s'identifica l'empresa ucraïnesa SIGMA Software, que ofereix serveis de ciberseguretat per al sector armamentístic. L'empresa té com a client l'OTAN i disposa d'oficines a Israel.[214]

Aquesta situació fa que cada cop més, empreses israelianes aterrin a l'Est d'Europa per producció i comercialització de productes, encapçalades per grans companyies militars com Elbit Systems. Aquesta empresa va crear tres filials i quatre plantes de producció a Romania. A través de la seva filial Uzina Automecanica Moreni S.A. (UAM), ha aconseguit contractes amb el govern per a la producció d'artilleria, promovent acords amb empreses nacionals com CN ROMARM S.A.[215] Més recentment, la també israeliana Agilite, especialitzada en uniformes tàctics,[216] i assenyalada en l'apartat anterior per la seva participació en el genocidi a la Franja de Gaza, va registrar al 2022 una subsidiària a Eslovàquia sota la denominació Agilite Systems Europe S.R.O.[217]

212 Czerny, M. (2024, 19 de novembre). 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-drone s/

213 Global Investigations Initiative [GII]. (s. d.). XTEND Ltd. - Defense Export and Supply Chain Data. Recuperat el 4 de maig de 2026, de https://gii.global/#!/tab/329597132-2

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

215 Elbit Systems. (s. d.). Modernizing the eastern flank. Blog d'Elbit Systems. https://www.elbitsystems.com/blog/modernizing-the-eastern-flank

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

217 EMIS. (s. 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

3. L'epicentre del lobby militar israelià: Alemanya

Alemanya es el segon proveïdor d'armament a Israel després dels EUA. Les seves llicències van ascendir a 879,8 mil milions d'euros entre el 2018 i el 2022. Al 2023, les exportacions des del cor de la Unió Europea cap a Israel van augmentar de 32,3 milions de euros a 326,5 milions. La majoria d'aquestes llicències d'exportacions van ser atorgades després de l'inici del genocidi.[218] Al voltant d'aquests interessos econòmics s'ha desenvolupat una gran infraestructura de lobby, que no és un fenomen nou, però des de l'inici del genocidi de la Franja de Gaza, s'identifiquen noves tendències.

La Israel Defence and Security Forum (IDSF), formada per més de 35.000 reservistes militars i liderat per l'exoficial de l'exèrcit israelià Amir Avivi, va iniciar una campanya de lobby a les institucions europees per prevenir les sancions a Israel i per influir en la seva política davant el genocidi a la Franja de Gaza, així com per reduir el suport europeu a les iniciatives d'alt al foc i al cas de Sud-àfrica davant la Cort Internacional de Justícia.[219] Segons la seva pròpia activitat pública, l'organització ha viatjat repetidament a Brussel·les des del 2023 i s'ha reunit amb almenys 19 eurodiputats. Entre aquests, destaquen el comissari europeu de Defensa i Espai, Andrius Kubilius, i la vicepresidenta del Parlament Europeu, Pina Picierno.[220]

En una línia similar, la European Leadership Network (ELNET), amb seu a París i branques a diverses capitals europees (Berlin, Roma, Londres, i Bèlgica), actua com una estructura de lobby pro-Israel. Un dels seus objectius principals és millorar la imatge d'Israel a Europa. Per això impulsa missatges per a que França i altres països europeus adoptin postures més favorables a Israel, com ara reconèixer Jerusalem com a capital de l'Estat. També treballa per coordinar narratives i influir en mitjans de comunicació, think-tanks i centres d'investigació estratègica, promovent agendes alineades amb interessos israelians, inclosa la idea que Europa pot beneficiar-se de la tecnologia i el suport israelià en seguretat, innovació i intel·ligència.[221] Un tret característic d'ELNET és l'ús d'estratègies de diplomàcia econòmica per promoure Israel com a actor d'innovació i aliat estratègic europeu, mentre es minimitzen o invisibilitzen les implicacions de les polítiques que contribueixen a l'ocupació i apartheid contra el poble palestí.[222]

Les estratègies de lobby d'ELNET són especialment evidents a Alemanya, on ha impulsat la iniciativa Security and Defence Initiative (ESDI) enfocada a promoure l'adopció de

218 Ibid

219 Dillenbourg, N. (2025, 6 de març). 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. (s. d.). European Leadership Network: Strengthening relations between Europe and Israel.

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

tecnologia militar i de seguretat israeliana, així com la creació d'una acadèmia de defensa. Algunes empreses alemanyes involucrades són DND Digital, Code Blue by Dussmann, Elbit Systems, IAI, Lufthansa Technik, Renk, Rohde & Schwarz i Werter.[223]

Paral·lelament, ELNET també ha promogut l'establiment del Cyber and Security Pact entre el govern d'Alemanya i Israel. El ministre federal de l'Interior, Alexander Dobrindt i el primer ministre de l'Estat d'Israel, Benjamin Netanyahu, van signar al gener de 2026, l'expansió de l'acord de cooperació entre ambdos països en l'àmbit de la ciberdefensa.[224] També contempla impulsar la creació d'un centre de recerca cibernètica conjunt entre tots dos Estats, aprofitar la tecnologia israeliana per protegir-se de possibles atacs amb drons i ampliar de manera significativa la cooperació en intel·ligència, especialment entre el Servei Federal d'Intel·ligència i el Mossad.[225] Dobrindt també va anunciar la creació d'un centre de recerca cibernètica germano-israelià.[226] Una iniciativa que reforçaria encara més la implantació d'empreses israelianes dins l'ecosistema tecnològic alemany.

Del lobby econòmic a la cooperació entre ecosistemes tecnològics

Una altra iniciativa d'ELNET ha estat l'establiment de la plataforma German Israeli Network of Startups & Mittelstand (GINSUM) amb el suport del Ministeri Federal d'Economia i Acció Climàtica d'Alemanya, amb l'objectiu de connectar el Mittelstand alemany, sector d'empreses petites i mitjanes, i els actors municipals amb l'ecosistema d'empreses emergents d'Israel.[227]

La GINSUM afirma que la cooperació entre el Mittelstand alemany i startups israelianes ofereix importants avantatges competitius. Les startups, més àgils i orientades al client, aporten innovació externa que ajuda les empreses mitjanes a adaptar-se a les noves tecnologies, especialment en àmbits com la ciberseguretat, i a evitar quedar enrere davant competidors nacionals i multinacionals ja actius a Israel.[228]

223 ELNET Deutschland. (2024, 21 de febrer). 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, gener). Cybersecurity cooperation with Israel expanded. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2026/01/israel-dobrindt-en.html

225 Monroy, M. (2025, 24 de juliol). 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-benef it/

226 Reuters. (2025, 29 de juny). Germany seeks Israeli partnership on cyberdefence, plans 'Cyber Dome'. https://www.reuters.com/business/aerospace-defense/germany-seeks-israeli-partnership-cyberdefence-plans-cyber-dome-20 25-06-29/

227 Sommer, C. (2021, març 11). What can Israeli start-ups offer German mid-sized companies? GINSUM. https://www.ginsum.eu/what-can-israeli-start-ups-offer-german-mid-sized-companies/

228 Ibid.

Segons un estudi de la fundació alemanya Bertelsmann, els modes d'interacció i cooperació entre startups alemanyes i israelianes funcionen a través de diferents mecanismes: distribuint productes propis a Israel o adquirint tecnologia israeliana per al seu ús intern. En el primer cas, la col·laboració sol començar per vendes i, un cop establerts contactes locals, s'exploren opcions d'innovació i R+D. En el segon, la integració de productes israelians —sobretot en ciberseguretat o anàlisi de dades— permet conèixer l'ecosistema tecnològic d'Israel i les seves capacitats. Altres mecanismes són el scouting, és a dir, la identificació d'oportunitats tecnològiques i startups locals, a través d'especialistes sobre el terreny i la creació d'acceleradores o incubadores pròpies o en col·laboració amb actors locals, que permeten estar a prop de noves innovacions i controlar-les en diferents graus segons el model triat. També es poden establir activitats d'R+D conjuntes amb empreses israelianes o crear centres totalment propis. Finalment, les inversions estratègiques o adquisicions de startups israelianes sovint deriven en la transformació d'aquestes en centres d'R+D locals.[229]

Un exemple específic és el de C2A Security, una startup israeliana especialitzada en ciberseguretat per a infraestructures industrials i crítiques.[230] L'any 2024, l'empresa va establir una filial a Alemanya, C2A Security GmbH, amb l'objectiu de posicionar-se dins el mercat europeu de tecnologies de seguretat, especialment en l'àmbit alemany,[231] i així adaptar-se als requisits regulatoris de la UE en matèria de ciberseguretat.[232] Paral·lelament, C2A Security desenvolupa part de la seva tecnologia a través de la incubadora israeliana Labs/02 –un programa de suport i finançament a projectes tecnològics–[233] finançada per actors internacionals com OurCrowd, Motorola Solutions, Reliance Industries i Yissum, l'oficina de transferència de tecnologia de la Hebrew University of Jerusalem.[234]

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. (s. 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, maig 16). 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, agost 4). Navigating NIS2: Essential OT security for EU manufacturers. https://c2a-sec.com/navigating-nis2-essential-ot-security-for-eu-manufacturers/

233 Labs/02. (s. f.). Portfolio. https://labs02.com/portfolio/

234 OurCrowd. (2018, gener 31). 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/

En aquest context, cal assenyalar que Motorola Solutions i la seva filial a Israel figuren a la base de dades de Nacions Unides d'empreses vinculades a activitats als assentaments il·legals israelians a Territori Palestí Ocupat.[235]

4. Participació en fires de tecnologia i ciberseguretat com a mecanisme per accedir a la UE

En els darrers anys, les fires i congressos europeus de ciberseguretat com el Cybersec Europe (Brussel·les), el Barcelona Cybersecurity Congress, el Cyber Intelligence Europe (Madrid), el Cyberwise Con (Vilna), el Infosecurity Europe (Londres) o el IT-SA (Nuremberg) s'han convertit en plataformes clau per a que les empreses israelianes accedeixin al mercat europeu. Sota el paraigua de la innovació tecnològica, les companyies israelianes promouen solucions de vigilància i intel·ligència artificial que sovint provenen del sector militar.

La participació israeliana en aquests esdeveniments no és casual ni improvisada, forma part d'una estratègia diplomàtica i econòmica sostinguda, impulsada per les institucions israelianes d'internacionalització, que organitzen pavellons estatals i missions comercials per presentar el país com un "hub global de ciberseguretat". Aquesta presència es veu reforçada per acords d'associació amb la Unió Europea que permeten a aquestes empreses projectar una imatge d'actors legítims dins de l'ecosistema tecnològic europeu, malgrat que en el seu origen estan vinculades a contextos de genocidi, conflicte i ocupació militar.

Així, fires com la de Barcelona, Brussel·les o Nuremberg actuen com espais de "neteja" corporativa i legitimació, on empreses amb vincles amb l'ecosistema de ciberseguretat i la indústria militar israeliana poden redefinir-se com a startups civils d'innovació digital. Aquest fenomen posa en qüestió la capacitat de les institucions europees per distingir entre tecnologia civil i de doble ús, i evidencia la fragilitat dels controls ètics i polítics, com comercials i de protecció dels consumidors, davant els interessos comercials i geoestratègics.

La fira IT-SA a Nuremberg que va tenir lloc a finals d'octubre del 2025 també és un es-

235 Office of the United Nations High Commissioner for Human Rights. (2025, setembre 26). 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

pai on s'incentiva la relació amb empreses israelianes,[236] de fet, hi va haver un Pavelló Nacional d'Israel amb 8 companyies israelianes de ciberseguretat que presentaven els seus productes.[237]

A la Fira de Barcelona per exemple, apareix com a Oficina Internacional de la Fira de Barcelona a Israel l'empresa israeliana ViSerCo, propietat de Sergio Vinitzly.[238] Aquesta empresa és delegada de la Fira de Barcelona des de l'any 2007 i representa a Israel fins l'actualitat.[239] El CEO de l'empresa és a la vegada un dels co-fundadors de l'Israel Smartcity Institute.[240]

Segons la seva pròpia web corporativa, ViSerco és una empresa israeliana de consultoria empresarial especialitzada en donar suport a altres companyies, particularment israelianes, a posicionar-se en mercats internacionals mitjançant estratègies comercials, establiment de contactes i presència en fires o esdeveniments sectorials. L'empresa destaca el seu coneixement i experiència en l'àmbit de la indústria digital i les noves tecnologies, un sector que inclou la ciberseguretat i la innovació tecnològica.

Aquesta orientació converteix ViSerco en una autèntica facilitadora per a l'aterratge d'empreses israelianes del sector tecnològic i de la ciberseguretat a Europa, i especialment a ciutats com Barcelona, on la celebració de fires internacionals com el Mobile World Congress o el Barcelona Cybersecurity Congress ofereix un entorn òptim per connectar amb inversors, socis i clients europeus. En aquest sentit, el paper de ViSerco no és tant el de desenvolupar tecnologia pròpia, sinó el d'obrir portes i crear xarxes que permetin a altres empreses del sector israelià integrar-se i legitimar-se dins del mercat europeu.

En aquest context, la Fira de Barcelona ocupa un paper especialment rellevant com a espai recurrent d'acollida d'empreses israelianes i de pavellons estatals d'Israel en esdeveniments tecnològics i de ciberseguretat. Congressos com el Mobile World Congress, el Barcelona Cybersecurity Congress o altres salons vinculats a la innovació digital han comptat de manera reiterada amb la presència d'empreses israelianes del sector tecnològic, algunes d'elles amb vincles documentats amb la indústria militar i de seguretat. Aquesta presència no és neutra si es té en compte que la Fira de Barcelona és un consorci públic, participat per la Cambra de Comerç de Barcelona, la Generalitat de Catalunya i l'Ajuntament de Barcelona, fet que implica una responsabilitat institucional

236 it-sa Expo&Congress. (s. f.). 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 [Esdeveniment]. Messe Nürnberg, Alemanya. https://itrade.gov.il/germany/event/israeli-national-pavilion-at-it-sa-2025-7-9-october/

238 Vinitsky, S. (s. f.). Perfil de LinkedIn de Sergio Vinitsky. LinkedIn. https://www.linkedin.com/in/sergio-vinitsky-6b3a07

239 Viserco. (s. d.). Soluciones tecnológicas de seguridad y defensa. https://viserco.biz/

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

directa en relació amb els criteris ètics, polítics i de drets humans que haurien de regir la selecció d'expositors i col·laboradors. La normalització d'aquesta presència, sota el relat de la innovació i la competitivitat econòmica, contribueix a legitimar actors empresarials provinents de contextos de conflicte i ocupació militar, i posa de manifest la manca de mecanismes clars de diligència deguda en drets humans dins d'un espai firal sostingut amb recursos públics.

Durant els últims dos anys i mig, organitzacions com La Fira en La Mira i la Coalició Prou Complicitat amb Israel han denunciat la presència sistemàtica i reiterada a la Fira de Barcelona de pavellons israelians i d'empreses vinculades directament amb l'exèrcit israelià, l'ocupació militar israeliana i el genocidi contra el poble palestí. Aquesta situació persisteix tot i que tant l'Ajuntament de Barcelona i la Generalitat de Catalunya han aprovat mocions per demanar a la Fira de Barcelona que deixi de donar espai a aquests pavellons i empreses.

Recentment, diverses investigacions periodístiques han posat de manifest la presència creixent d'empreses europees i israelianes en esdeveniments de caràcter reservat com la fira ISS World, celebrada a Praga, considerada un dels principals punts de trobada del sector global de la ciberseguretat, vigilància i la intel·ligència.[241] En aquest tipus de fires, on l'accés està restringit a cossos policials, agències de seguretat i empreses del sector, s'han detectat també firmes amb seu a Europa que ofereixen tecnologia potencialment intrusiva. Un exemple il·lustratiu és el de First Wap, documentat per Lighthouse Reports l'any 2024.[242] Aquesta empresa, especialitzada en tecnologies de vigilància, ha estat vinculada a la comercialització i desplegament d'eines de control digital en diversos contextos, incloent-hi el mercat europeu. La seva presència en aquests entorns posa de manifest fins a quin punt el mercat europeu de la ciberseguretat pot operar com un espai de connexió entre actors públics i privats amb poca transparència, sovint amb dèficits d'escrutini democràtic i de supervisió dels impactes en drets humans.

En definitiva, aquesta xarxa de congressos i fires europees tecnològiques i de ciberseguretat funciona com un canal estructurat d'integració comercial per a les empreses israelianes, que hi troben visibilitat, accés a clients institucionals europeus i col·laboracions amb centres de recerca. A més, els pavellons estatals promoguts per les institucions públiques d'Israel reforcen aquest accés i permeten rebranditzar la indústria israeliana de tecnologies de vigilància i armamentística com a ecosistema d'innovació tecnològica civil.

241 Geiger, G., Black, C., Freudenthal, E., & Coluccini, R. (2025, octubre 14). 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-jare d-leto-anne-wojcicki/

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

5. Del soft-landing a Xipre a estructures empresarials opaques

Xipre és un país estratègic per a les empreses i startups tecnològiques israelianes, ja que ofereix un conjunt de condicions geogràfiques, legals, fiscals i financeres que faciliten el soft-landing, és a dir un aterratge avantatjós, d'aquestes empreses.[243] Per començar, la seva proximitat geogràfica a Israel permet vols directes i una logística senzilla. Molts empresaris israelians hi estableixen la seva residència i adquireixen propietats, sense perdre la possibilitat de viatjar amb freqüència al seu Estat d'origen. Xipre també ofereix accés al mercat de la UE sense les barreres habituals que es troben les empreses extracomunitàries.[244] Constituir una empresa a Xipre implica que aquesta pot operar i vendre productes i serveis a tota la Unió Europea sense llicències addicionals. A més, els fundadors i treballadors obtenen la residència europea i poden moure capital lliurement dins l'espai comunitari. El país també disposa d'un règim fiscal favorable —amb un impost de societats del 12,5%— que evita la doble imposició i ofereix una regulació flexible per al registre empresarial, amb processos àgils.[245] La infraestructura bancària també és sòlida i compta amb serveis fintech avançats.[246]

Les empreses israelianes que decideixen aterrar a Xipre compten amb el suport d'actors com la Cambra de Comerç Israel-Xipre, amb múltiples socis en els sectors legal, turístic, immobiliari, entre d'altres.[247] També existeixen iniciatives per a promoure la reubicació de tecnologia internacional al hub tecnològic de Xipre.[248] Paral·lelament, el país compta amb centres d'innovació i acceleradors a Nicòsia i Limassol, amb incubadores i hubs tecnològics atractius per a *startups* de ciberseguretat, fintech, armament i energies renovables.[249] A aquestes condicions s'hi suma l'absència d'un marc regulador efectiu per supervisar el desenvolupament o l'exportació de productes de cibervigilància, fet que permet que

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

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

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

246 El terme fintech prové de financial technology i fa referència a l'ús de la tecnologia per oferir serveis financers de manera més innovadora que la banca tradicional.

247 Israel–Cyprus Chamber of Commerce. (s. f.). Members. https://israel-cyprus.co.il/members/

248 Cyprus Tech Hub. (s. f.). Cyprus Tech Hub. https://www.cyprustechhub.com/

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

aquestes empreses operin amb un control mínim. Tot i que l'UE compta amb una normativa sobre programari espia, les autoritats xipriotes han demostrat escassa voluntat d'aplicar-la.[250]

Estructures opaques en el sector de ciberseguretat

El periodista d'investigació xipriota i ex-assessor presidencial, Makarios Drousiotis, explica en el seu llibre Mafia State que al 2019 operaven al país 29 empreses de tecnologia intrusiva de propietat israeliana. Segons l'autor, aquest imlantació a Xipre es basava en l'optimització d'impostos, però també en la capacitat d'establir estructures empresarials opaques en el sector de la ciberseguretat.[251]

El llibre destaca el cas de les empreses de ciberseguretat Circles i Intellexa, ambdues creades per Tal Dilian, ex-responsable de l'agència d'intel·ligència militar israeliana la Unitat 8200. D'una banda, Circles, la primera empresa creada per Dilian, ha estat àmpliament implicada en l'ocupació de Palestina i el ciberespionatge d'activistes a nivell global.[252] Mentre que les tecnologies de vigilància massiva d'Intellexa, com el programari espia Predator, van ser incloses a la llista de control d'exportacions del Departament de Comerç dels Estats Units per l'amenaça que suposaven a nivell de seguretat nacional i exercici dels drets humans.[253] No obstant això, aquest tecnologia continua utilitzant-se en nombrosos països com Angola, Egipte, Oman, l'Aràbia Saudita i Indonèsia, entre d'altres.[254]

A Xipre, Dilian va crear un entramat d'empreses per gestionar el seu capital i fer operacions internacionals. Aquest grup d'empreses estava liderat per Censura Ltd, primer dirigida per Dilian però, a partir de 2019, sota el control de Sara Hamou, associada i exdona de Dilian.[255] A Xipre, Hamou va col·laborar amb l'empresa DJC Accountants que suposadament hauria tingut la missió de facilitar l'opacitat de les activitats i propietat dels clients

250 Kenner, D. (2023, novembre 15). 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, desembre 1). Running in circles: Uncovering the clients of cyberespionage firm Circles. The Citizen Lab, University of Toronto.
https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

253 Bob, Y. J. (2024, març 5). 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, agost 20). 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, novembre 15). 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/

de Censura.[256]

Hamou també va ajudar a altres empreses del sector de ciberseguretat a establir-se a Xipre i Grècia per reforçar la seva expansió internacional. Al 2018 va crear una nova empresa Maravilhas Solutions Ltd i entre els seus clients hi ha rastre d'empreses subsidiàries de Q Cyber Technologies, empresa creada de la fusió entre NSO Group i Circles, per "serveis de subministrament i l'enviament de maquinari, la seva instal·lació a les seus dels clients i els serveis de suport i manteniment."[257]

Maravilhas Solutions Ltd va facilitar projectes a la UE, comprant i enviant equips per a empreses israelianes. A principis del 2019, va adquirir material per a un projecte de Q Cyber a Bulgària i, al maig, va comprar prop de 120.000 dòlars en equips que posteriorment es van enviar a Bèlgica, operació sobre la qual les autoritats fiscals xipriotes van rebre consultes d'un altre Estat europeu. Aquesta tàctica de fer servir societats europees per canalitzar vendes de material israelià, va facilitar l'accés d'aquest al mercat de la UE, alhora, que li va possibilitar potencialment eludir controls d'exportació, ja que l'equipament reexpedit i barrejat amb altres béns sovint no obliga a declarar l'usuari final.[258]

6. Luxemburg com a plataforma de llançament

Lluny de poder considerar Pegasus com una tecnologia obsoleta, empreses com NSO Group continuen treballant per perfeccionar i modificar les propietats dels seus productes amb la finalitat d'assolir l'objectiu inicial que va donar lloc a l'empresa: "desenvolupar una eina capaç de penetrar un dispositiu mòbil de manera remota i indetectable".[259] Niv Carmi, Shalev Hulio i Omri Lavie justificaven la importància de la tecnologia que havien desenvolupat assenyalant i apel·lant,[260] des de l'inici, a una necessitat de seguretat europea: "forces policials i agències d'intel·ligència d'Europa ens van dir que, amb la tecnologia que havíem desenvolupat, podríem ajudar a resoldre el seu problema".[261] Aquest element va ser el punt de partida que els va portar a fundar NSO Group Technologies Ltd, el 25 de gener de 2010.

Tot i que NSO desenvolupa un ampli ventall de productes, el seu producte més conegut

256 Ibid.

257 Ibid.

258 Ibid.

259 Ynet Global. (2019, novembre 1). 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, gener 28). The battle for the world's most powerful cyberweapon. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

és Pegasus**,** una tecnologia de vigilància que, segons l'empresa, només es ven a Estats i agències d'intel·ligència a escala internacional.[262] L'evolució de Pegasus ha estat constant en els darrers anys: ha passat de requerir la interacció de l'usuari per a la seva activació a incorporar mecanismes d'explotació de tipus zero-click i funcionalitats com la fabricació, modificació i inserció d'informació en el dispositiu.[263] Aquesta progressiva sofisticació comporta conseqüències greus, ja que el software atorga un accés i un control total i desproporcionat sobre el contingut dels dispositius mòbils. Mitjançant un mecanisme de ciberespionatge zero-click, ho aconsegueix sense cap interacció de l'usuari —ni clics, ni enllaços, ni descàrregues.

Si bé l'empresa justifica el seu producte per raons de "seguretat nacional", les dades disponibles mostren centenars de milers de casos en què aquesta tecnologia s'ha utilitzat contra actors de la societat civil que no representaven cap amenaça per als Estats implicats.[264] Aquestes pràctiques fomenten la construcció d'un futurible delictiu, és a dir, la presumpta existència d'una amenaça sense fonament, un mecanisme habitual en l'ús de tecnologies de vigilància. Davant aquesta situació, nombroses organitzacions internacionals han demanat la prohibició de Pegasus.[265]

Tot i que NSO Group Technologies Ltd és una societat privada incorporada i registrada a Israel, el nom "NSO Group" s'utilitza com a marca paraigua per designar el conjunt d'empreses associades, tant operatives com financeres, distribuïdes arreu del món. L'estructura corporativa de NSO reflecteix la ràpida expansió i proliferació d'aquest sector,[266] i adverteix d'una realitat preocupant a l'actualitat.[267] Amb un total de 13 societats hòlding i 12 filials en múltiples jurisdiccions, el grup opera mitjançant una estructura complexa i deliberadament opaca, en què les empreses sovint canvien estratègicament de nom i amplien les seves activitats a altres jurisdiccions per eludir regulacions més estrictes**.**[268] És per això que resulta fonamental analitzar com s'introdueix i actua a Europa, com un mirall de pràctiques i lògiques que es reprodueixen dins el mercat de la vigilància. Un element estructural d'aquest tipus d'empreses és la manca de transparència i de meca-

262 NSO Group. (2025, febrer). 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/

266 La marca comercial "NSO Group" és propietat exclusiva de l'empresa matriu israeliana 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/

nismes efectius de rendició de comptes sobre les seves activitats i exportacions, fet que dificulta l'accés a informació verificable, incloses les causes judicials iniciades per persones espiades amb Pegasus.[269]

L'entramat empresarial de NSO compta amb una presència especialment significativa a Luxemburg. Luxemburg, membre fundador de la UE i de la zona euro, s'ha consolidat com un hub estratègic per a empreses internacionals gràcies a l'accés al mercat europeu, un marc empresarial flexible, infraestructures tecnològiques avançades, estabilitat econòmica i una especialització destacada en ciberseguretat, i és activament promogut a Israel com a destinació per a l'expansió empresarial.[270] En el moment de redacció d'aquest informe, NSO hi té dinou societats domiciliades, onze de les quals comparteixen el mateix objecte social.[271] Aquesta estructura empresarial amplia el ventall d'actuació d'aquestes entitats, atorgant-los un caràcter instrumental, ja que amplia el seu àmbit d'actuació sense definir-ne amb claredat la finalitat. A més, les societats comparteixen no només l'objecte social sinó també la ubicació física.[272]

L'informe final de la Comissió PEGA del Parlament Europeu,[273] va concloure que el manteniment de NSO depèn en gran mesura del suport de les societats establertes a Luxemburg. L'informe identificava aquestes entitats com el centre de negocis europeu del grup, que facilita la seva activitat amb una regulació menys estricta tant dins de la UE com en tercers països, i gestiona facturació, contractes i pagaments vinculats al programari espia.[274] La permissivitat de la UE vers el mercat de programari espia comercial no només afavoreix que aquestes empreses operin sota un marc normatiu més lax que el que tindrien si ho fessin des d'Israel, sinó que també dota de legitimitat la comercialització dels seus productes des de territori europeu.

Entre les dinou societats vinculades a NSO Group registrades a Luxemburg, destaquen

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.ht ml

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

271 L'objecte social d'onze d'aquestes societats és ser designades formalment —mitjançant contracte, acord social o decisió d'un òrgan competent— per exercir càrrecs o funcions en altres societats, i actuar com a sòcies directores generals, adquirir participacions a Luxemburg o a l'estranger i intervenir em la seva gestió.

272 De les dinou societats de NSO Group a Luxemburg catorze tenen el mateix domicili social, mentre que les cinc restants es troben concentrades en una altra adreça

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

Osy Technologies Sàrl i Q Cyber Technologies Sàrl, tant pel seu vincle amb la ciberteconologia com per la seva rellevància estructural dins del grup Osy Technologies. Aquesta última, creada el febrer de 2014, va ser la primera societat del grup al país, seguida de Q Cyber Technologies, constituïda el gener de 2016 amb Osy com a accionista únic. Ambdues se situen en el nucli originari de la presència europea del grup, que es va consolidar posteriorment mitjançant una ràpida expansió societària, tres el 2017, quatre el 2018 i cinc el 2020. Osy i Q Cyber mantenen llaços directes amb NSO Group Technologies, fins al punt de compartir junta directiva en els primers anys. Dos dels fundadors d'NSO, Omri Lavie i Shalev Hulio, hi tenen una presència destacada.[275]

Cal destacar que, quan el 14 de febrer de 2019 l'equip directiu i fundador d'NSO Group va anunciar que la firma de capital privat britànica Novalpina Capital n'assumia el control, el grup ja es presentava com una "empresa de tecnologia cibernètica amb seu a Luxemburg", resultat de la "fusió d'empreses de tecnologia cibernètica israelianes i europees".[276] Aquesta presentació no només pretenia reformular la identitat corporativa del grup sota una aparença més europea, sinó que també responia a una estratègia de posicionament institucional orientada a legitimar la seva activitat dins del mercat europeu de la ciberseguretat i a distanciar-se parcialment de la seva vinculació directa amb Israel, especialment arran de les controvèrsies generades per l'ús de Pegasus.

Arran dels escàndols de Pegasus, a mitjans del 2022, Shalev Hulio va dimitir com a CEO de NSO Group i va ser subsituït per Yaron Shohat. El gener de 2023, Hulio va fundar Dream Security.[277] El 7 de novembre de 2023, des de la Franja de Gaza des d'on servia com a reservista israelià, Hulio va anunciar una ronda de finançament,[278] que va presentar com un "gran missatge per la comunitat tecnològica i pel poble d'Israel".[279] Tot i els seus intents de desvincular-se de NSO Group, una dotzena d'antics alts càrrecs i operatius l'han seguit a Dream Security, on la majoria del personal té base a Israel, malgrat disposar d'oficines també a Viena i Abu Dhabi. La companyia ha nascut envoltada de controvèrsia pels seus vincles amb la dreta israeliana i internacional, especialment per la participació com a cofundador de l'ex-canceller austríac Sebastian Kurz.[280]

---

275 Lavie apareix en nou juntes directives de societats luxemburgueses i Hulio en sis, reforçant la idea d'una estructura interconnectada i gestionada de manera unificada.

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/

277 Dream Security és una start-up dedicada a solucions defensives de ciberseguretat per a infraestructures crítiques, amb l'ambició pública de convertir-se en la "millor plataforma defensiva de ciberseguretat basada en intel·ligència artificial del món". Més informació disponible a: https://dreamgroup.com/about/

278 Biddle, S. (2024, 18 de gener). 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, gener 21). 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

WhatsApp vs. NSO Group i la responsabilitat de l'empresa

El 2019, WhatsApp i la seva matriu, Meta, van presentar una denúncia contra NSO Group als Estats Units. L'empresa israeliana va utilitzar els seus servidors per dur a terme ciberespionatge mitjançant Pegasus, que va afectar més de 1.400 usuàries. Aquesta denúncia va marcar un punt d'inflexió en la crisi reputacional de NSO Group.[281] Durant el procés, el Departament de Comerç estatunidenc va incloure NSO Group a la seva llista de sancions el 2021,[282] en considerar que les seves activitats contravenien els interessos de la «seguretat nacional». Des d'aleshores, NSO Group se li prohibeix operar al mercat estatunidenc i el seu personal té restringit l'accés al país.[283] Malgrat l'impacte econòmic i polític d'aquesta sanció dels EUA, la Unió Europea no ha adoptat mesures equivalents ni ha establert una posició comuna sobre la prohibició de Pegasus.

El desembre del 2024, un tribunal de Califòrnia va condemnar NSO Group per vulnerar lleis federals i estatals de frau i abús informàtic, a favor de WhatsApp,[284] imposant una indemnització superior als 168 milions de dòlars.[285] El procediment també va tornar a posar de manifest l'opacitat del grup i va demostrar que és NSO Group qui realitza les fases inicials d'infecció i extracció de dades dels dispositius atacats, contrariant el relat que havia sostingut fins llavors.[286] La sentència ha estat celebrada internacionalment com una fita clau en la lluita contra els abusos dels programes espia.[287]

Reorientació estratègica cap a l'estatunidització de NSO Group

Tot i la reubicació de desenes de treballadores arran de la crisi reputacional de NSO Group, l'empresa va continuar operant fins el novembre del 2025, sota el lideratge d'un dels seus fundadors, Omri Lavie. Després de 25 anys d'activitat i amb més de 22 clients només a

281 Perlroth, N., & Isaac, M. (2019, 29 d'octubre). 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 de novembre de 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 de febrer de 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. v. 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/

285 The Record by Recorded Future News. (2025, maig 6). 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, novembre 15). 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 v. NSO case.
https://www.accessnow.org/press-release/statement-on-whatsapp-v-nso-case-decision/

Europa, incloent-hi 12 dels 27 Estats membre,[288] el novembre del 2025 es va produir un canvi substancial en la direcció. Per primera vegada, els fundadors, alguns actius des del 2010, van deixar de tenir-hi qualsevol participació, fet que marca un punt d'inflexió en la trajectòria de l'empresa.

La nova etapa, encapçalada per l'advocat estatunidenc David Friedman,[289] coincideix amb l'adquisició total de la companyia per un grup d'inversors dels Estats Units, alguns amb nacionalitat israeliana. L'actual president executiu va ser l'ambaixador dels EUA a Israel durant la primera administració Trump i va participar en la negociació dels Acords d'Abraham. També destaca per les seves intervencions públiques en defensa dels assentaments il·legals israelians al Territori Palestí Ocupat i per impulsar campanyes de finançament destinades a aquest objectiu. Aquest canvi en la direcció i la propietat s'emmarca en una tendència d'estatunidització de NSO Group.

Paral·lelament, el canvi de direcció i de propietat ha comportat modificacions en tres societats d'NSO Group registrades a Luxemburg,[290] que passen a estar dirigides per Ohad Shazar Shalem Schremer. L'advocat israelià resideix a l'assentament il·legal de Neve Daniel, a Gush Etzion, dins del Territori Palestí Ocupat, i forma part de la junta directiva d'una associació de colons d'extrema dreta. Aquest nou lideratge reflecteix una orientació corporativa, que posa de manifest la seva connexió amb el govern israelià i amb la ultradreta, tant a Israel com a escala internacional, i amb interessos de caràcter colonial.

7. Adquisició d'empreses europees i rebranding per operar a la UE

Després de l'escàndol internacional provocat per Pegasus i l'escrutini creixent cap a les empreses israelianes de ciberseguretat, algunes d'aquestes empreses han optat per mo-

288 Benjakob, O. (2022, agost 9). 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, novembre 9). 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 Les tres societats de NSO Group a Luxemburg que canvien de direcció són: NorthPole Newco, Osy Technologies i Q Cyber Technologies.

dificar la seva marca, el que s'anomena un rebranding,[291] amb l'objectiu d'aterrar a Europa i accedir a nous mercats. Lluny de ser un fenomen aïllat, aquesta és una pràctica sistemàtica que combina canvi de nom, creació de filials constituïdes ad hoc, tancaments i creació de companyies noves i utilització d'intermediaris locals.

En aquest sentit, algunes empreses assenyalades per la seva participació en operacions de ciberespionatge contra activistes, periodistes i líders polítics han optat per adquirir empreses europees o constituir noves societats a Europa amb denominacions diferents de les de la matriu. D'aquesta manera, **b**usquen desvincular-se de la reputació negativa i presentar-se com a actors legítims de l'ecosistema tecnològic i de ciberseguretat. L'Informe PEGA del Parlament Europeu (2023),[292] elaborat després de l'escàndol de Pegasus, ja alertava que diversos estats membres com ara Grècia, Xipre i Portugal, oferien incentius a empreses tecnològiques israelianes per traslladar els seus negocis a aquests països. Segon fonts israelianes, els tres països presumptament oferien exempcions fiscals a les empreses tecnològiques israelianes i, en el cas de l'Estat Grec, proporcionava la ciutadania de manera immediata.[293]

Així, l'operació d'adquirir empreses europees per part d'altres empreses amb seu a Israel, pot interpretar-se com una estratègia calculada per mantenir l'accés al mercat europeu i als seus mecanismes de finançament públic, fent servir una estructura corporativa establerta dins de la UE. Aquesta pràctica posa de manifest una escletxa reguladora: el Fons Europeu de Defensa (EDF) té com a finalitat reforçar la capacitat tecnològica i militar pròpia de la Unió, però, a la pràctica, permet que empreses controlades per tercers països es beneficiïn dels seus recursos.

Cas d'estudi: Intracom Defence i Embention

Intracom Defense és una empresa grega que,[294] des de l'1 de juliol del 2023, és propietat de l'empresa estatal israeliana Israel Aerospace Industries (IAI).[295] Aquesta adquisició ha permès a IAI mantenir l'accés al mercat i al finançament europeu, malgrat ser una em-

291 El rebranding és una estratègia de màrqueting que té per objectiu canviar o modificar la identitat de marca. A través d'accions sobre els seus diferents elements, com ara nom, logotip, o fins i tot l'eliminació legal de la companyia per crear-ne una altra amb les mateixes persones a càrrec, mateix sector de treball i productes però amb un nom i logo diferent.

292 European Parliament, Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). (2023, maig 22). 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, març 23). 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

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, maig 9). IAI has acquired Greek defense company Intracom Defense. https://www.iai.co.il/iai-has-acquired-greek-defense-company-intracom-defense

presa d'un país tercer, fora de la Unió Europea i implicada en activitats militars abans i durant el genocidi a la Franja de Gaza.[296]

Així, Intracom Defense, tot i estar registrada i operant a Grècia, està controlada en un 90,91 % per IAI.[297] L'EDF ha destinat milions d'euros a aquesta empresa, tot i que, segons la seva pròpia normativa, s'exigeix que les empreses beneficiàries no estigui controlades per un Estat no associat a aquest fons, com seria el cas de l'Estat d'Israel.[298] No obstant això,[299] mitjançant la compra de la filial grega, la companyia israeliana ha trobat una via indirecta per continuar participant en programes europeus de defensa i innovació, esquivant de facto les possibles restriccions o sancions que potencialment li impedirien fer-ho directament des d'Israel.

Això ha fet possible que Intracom Defense, arrelada formalment a la Unió Europea, sigui seleccionada com a coordinadora del projecte ACTUS (Advanced Capabilities & Certification for Tactical UAV Systems) i participi a projectes de reforçament de capacitats tecnològiques militars com el Projecte Sentinel,[300] tots dos finançats per la Unió Europea a través del EDF.[301]

El projecte ACTUS, que està valorat en 59 milions d'euros, té com a objectiu impulsar el desenvolupament tecnològic dels sistemes aeris no tripulats europeus utilitzats en entorns militars, coneguts com RPAS (Remote Piloted Aircraft Systems) o drons tàctics. En essència, es tracta d'un programa destinat a dissenyar, provar i certificar una nova generació de drons militars europeus, capaços d'operar en conflictes d'alta intensitat i en condicions operatives extremes.

En aquest projecte hi participa com a soci tecnològic una empresa espanyola, Embention, amb seu a Alacant, que hi aporta el desenvolupament dels components d'aviònica i control de vol, especialment l'autopilot Veronte i la Ground Control Station (GCS). L'empresa alacantina ja mantenia col·laboracions prèvies amb la indústria militar israeliana abans de participar en el projecte ACTUS. Segons informava al setembre de l'any 2020

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

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

298 European Commission. (s. f.). 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. (s. f.). 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=F ACTSHEET_EDF_2024_DA_ENERENV_EEMC_STEP_101224400_SENTINEL.pdf

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

el portal especialitzat SUAS News, Embention havia treballat conjuntament amb IAI en el desenvolupament d'un helicòpter no tripulat de càrrega, integrant-hi el seu sistema de navegació Veronte Autopilot.[302]

Aquesta cooperació, documentada ja a informes interns de l'empresa espanyola demostra l'existència de vincles tecnològics entre la companyia espanyola i una de les principals empreses d'armament de l'Estat d'Israel almenys des de l'any 2017. Aquell any, els ingressos d'Embention van ascendir a 1,3 milions d'euros quan va col·laborar amb IAI en el projecte Air Hopper. L'objectiu del projecte era desenvolupar un petit vehicle aeri no tripulat capaç de volar de manera autònoma durant almenys 8 km, amb una capacitat de càrrega útil de 150 litres i un pes mínim de 60 kg. Com a resultat, l'aeronau podria transportar un enviament a una ubicació específica del camp de batalla, deixar la càrrega i tornar a la base el més ràpidament possible, tot volant de manera completament autònoma.[303] Aquesta relació planteja interrogants sobre la transferència de coneixement i la legitimitat d'incorporar a programes europeus de defensa, tecnologia provinent del complex militar israelià.

Tot i la dimensió tecnològica del projecte, la participació d'Embention s'ha d'analitzar també des de la perspectiva dels riscos associats al doble ús i de la responsabilitat empresarial en matèria de drets humans. Els sistemes UAV com el LOTUS,[304] un projecte anterior a l'ACTUS, també finançat pel Programa Europeu Industrial de Defensa i on el coordinador del projecte era Intracom Defence, poden tenir aplicacions civils (inspecció, logística o rescat), però també poden ser integrats fàcilment en contextos militars i de control on població civil és assassinada. Aquesta ambivalència situa les institucions i empreses participants del projecte d'aquest projecte dins d'una sospita fonamentada de potencials complicitats, especialment quan les tecnologies es desenvolupen o provenen de contextos vinculats a la indústria militar i de tecnologies de vigilància israeliana, líder mundial en aquest tipus de sistemes que són provats de forma continuada sobre població civil palestina (el que es denomina com "provat en combat").

Segons una investigació de l'EU Observer, l'estratègia d'IAI amb la compra de l'empresa grega té el vistiplau europeu, ja que, en paraules d'un expert en defensa europea "necessitem els coneixements israelians que ens manquen". L'expert afegeix que això explica la maniobra d'Intracom: "volem desenvolupar les nostres pròpies municions [drons

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

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

304 Embention Sistemas Inteligentes S.A. (2021, febrer 8). Programa LOTUS: Un pas endavant per al vol en formació de UAVs. https://www.embention.com/es/noticias/programa-lotus-un-paso-adelante-para-el-vuelo-en-formacion-de-uavs/

que poden estavellar-se contra objectius], i també volem una 'contribució israeliana' en aquest segment".[305]

El procés de rebranding també es veu reforçat per l'entrada de capital risc europeu.[306] Fons com Forestay Capital han tancat operacions milionàries dirigides expressament a finançar empreses israelianes i facilitar-ne l'expansió a Europa,[307] mentre firmes globals com Accel han aixecat fons per invertir en intel·ligència artificial tant a Europa com a Israel.[308] Aquest finançament no només impulsa l'expansió empresarial, sinó que també actua com a mecanisme de validació reputacional. La participació de fons com Forestay Capital o Accel transmet al mercat una imatge de solvència i compliment d'estàndards, contribuint a consolidar un relat de "tecnologia innovadora i responsable".

Els casos de Circles, filial de NSO dedicada a la intercepció telefònica, o de QuaDream,[309] empresa israeliana de programari espia que va tancar el 2023 després de ser exposada[310] per la premsa internacional, il·lustren com aquestes empreses intenten reinventar-se i reaparèixer sota noves estructures o amb noves filials a Europa. En definitiva, l'adquisició d'empreses europees i el rebranding de les empreses de tecnologies de control, militars i armamentístiques israelianes no es limita a un simple canvi de nom, sinó que constitueix una estratègia integral destinada a netejar la seva reputació, guanyar legitimitat institucional i atraure inversió europea.

8. L'accés a la Unió Europea a través dels programes de finançament.

Al setembre del 2009, Javier Solana, Alt Representant per a la Política Exterior i de Seguretat Comú (PESC) de la Unió Europea durant una dècada, afirmava davant una audiència a Jerusalem: "Israel és, permeteu-me dir-ho, membre de la Unió Europea sense ser mem-

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

306 El capital risc europeu (venture capital) és una modalitat de finançament destinada a empreses joves, innovadores i amb un alt potencial de creixement a Europa, a canvi d'una participació en l'empresa.

307 Gilead, A. (2024, juliol 3). 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, maig 13). 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 d'abril de 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, Abril 16). Offensive cyber company QuaDream shutting down amidst spyware accusations. Ctech. https://www.calcalistech.com/ctechnews/article/hy78kiym2

bre de les institucions".[311] Més recentment, a l'abril del 2023, la presidenta de la Comissió Europea, Ursula von der Leyen, en la commemoració del 75è aniversari de la creació de l'Estat d'Israel, va declarar: "Europa i Israel estan obligats a ser amics i aliats. La vostra llibertat és la nostra llibertat".[312]

Ja al 2025 i en plena escalada de la violència a la Franja de Gaza, Dimiter Tzantchev, ambaixador de la UE a Israel, va afirmar que "el lideratge d'alta tecnologia d'Israel i la sòlida base de recerca de la UE fan d'Horizon Europe un programa en què tothom hi guanya".[313]

Aquestes afirmacions no són anecdòtiques: sintetitzen una relació assumida com a natural i estratègica per les principals institucions europees, i ajuden a entendre el tracte preferent que Israel rep en diversos àmbits de la política de la UE. Un dels més rellevants és l'accés al finançament europeu en recerca i desenvolupament (R+D). Des del 1996, Israel té l'estatus de "país associat", una categoria que li permet participar en els successius programes marc de R+D de la Unió Europea en condicions equiparables a les dels Estats membres.[314]

Actualment, Israel consta com a país associat al programa Horizon Europe (2021-2027), fet que possibilita a les empreses israelianes poder participar en igualtat de condicions que les empreses amb seu als Estats membres de la UE. Tot i que el programa Horizon està destinat a recerca d'ús civil, les institucions i empreses israelianes que reben fons públics europeus mantenen forts lligams amb el sector armamentístic, i/o ciberseguretat de l'Estat, fins i tot formant part d'aquesta mateixa arquitectura securitària i armamentística. En aquest sentit, del 2008 fins a la redacció del present informe, Israel ha rebut per part de la Unió Europea més de 70 milions d'euros en projectes específics de seguretat.[315] El resultat és que fabricants d'armes o de tecnologia de ciberseguretat com ara Elbit Systems o Israel Aerospace Industries (IAI) estan beneficiant-se de subvencions públiques del programa Horizon.[316]

311 Hayes, B. (2010, Març 17). 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 d'abril de 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-c ooperation/association-horizon-europe/israel_en

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

316 Statewatch. (2024, 7 de febrer). 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-i nternational-law/

La Israel Innovation Authority va anunciar, el primer trimestre del 2025, que els equips d'investigació i empreses israelianes havien aconseguit 1.100 milions d'euros en finançament d'Horizon Europe entre el 2021 i el 2024, reafirmant la posició estratègica d'Israel en recerca, innovació i tecnologia a la UE.[317] Aquest programa ha concedit a empreses i projectes israelians 475 milions d'euros des d'octubre del 2023, incloses startups gestionades per ex-membres de l'exèrcit israelià, específicament de les unitats de ciberseguretat.[318] De fet, un informe publicat al 2018, assenyalava que el 80% de les 2.300 persones que van fundar les centenars d'empreses de ciberseguretat existents a Israel eren veterans de les unitats d'intel·ligència de l'exèrcit.

I és que, tal i com afirma l'expert en l'economia de l'ocupació, indústria militar i de seguretat i comerç d'armes israelianes Shir Hever, bona part del finançament europeu en matèria militar i de seguretat cap a Israel es vehicula "a través d'instituts de tecnologia i universitats utilitzant aquestes institucions per emmascarar els vincles militars corporatius etiquetant els intercanvis com a cooperació científica".[319]

En alguns dels projectes d'Horizon en actiu,[320] es poden trobar empreses que han tingut un rol fonamental en el genocidi de la Franja de Gaza, com ara la israeliana Rafael Advance Systems, un dels grans fabricants d'armes israelians que desenvolupen míssils, drons i altres sistemes armamentístics per a l'exèrcit israelià. Aquestes pràctiques semblen no afectar les relacions comercials de la companyia que recentment, a través del Consorci EuroSpike[321] i amb el suport de les empreses armamentístiques Rheinmetall i Diehl, ha tancat un contracte amb el Govern alemany per valor 2.500 milions de dòlars.[322]

Segons dades recollides per Transnational Institute, des del 7 d'octubre del 2023, la UE ha aprovat 130 projectes de recerca del programa Horizon Europe amb participants israelians, que han rebut un total de 126 milions d'euros. Almenys dos d'aquests projectes financen directament Israel Aerospace Industries (IAI), que rep gairebé 640.000 euros.[323]

---

317 Innovation Israel – Israel Innovation Authority. (2025, 19 de març). 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 de setembre). 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 Entrevista amb l'expert Shir Hever. 24 d'octubre de 2025.

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

321 Consorci alemany lider en defensa fundat l'any 2004 a través de la col·laboració de Diehl Defence, Rheinmetall Electronics i Rafael Advanced Defense Systems.

322 Global Defense Corp. (2025, 24 d'octubre). 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/

323 Ní Bhriain, N., & Akkerman, M. (2024, 4 de juny). 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

Segons Shir Hever, la major part del finançament d'Horizon Europe, fins i tot aquell dirigit a universitats israelianes, acaba repercutint al sector de la ciberseguretat i la indústria militar de l'estat, ja que sovint les universitats israelianes són sòcies properes de la indústria militar i armamentística.

La Unió Europea disposa d'altres programes de recerca i innovació que ofereixen finançament, com ara l'European Defence Fund (EDF) finança projectes d'R+D en defensa i seguretat, afavorint la participació d'empreses i centres tecnològics que contribueixen a l'autonomia armamentística europea. Si en una primera etapa l'EDF es vinculava sobretot al reforç de les fronteres, en la lògica de la denominada "Europa Fortalesa",[324] actualment ha evolucionat cap a un enfocament estrictament militar. Des de la seva creació, la inversió de la UE en projectes d'R+D militar supera els 3.000 milions d'euros.[325]

El finançament de la UE a Israel acaba essent una forma de legitimar un règim que utilitza la innovació tecnològica per sostenir un sistema colonial d'ocupació i control militar sobre el poble palestí, disfressant-lo de cooperació científica i progrés compartit. Aquesta col·laboració ha generat fortes divisions internes dins de la Unió Europea i un ampli rebuig per part de la societat civil, les ONG de drets humans i diverses eurodiputades, que denuncien la contradicció entre els valors proclamats per la UE i les seves pràctiques reals de finançament.

Com a resposta a aquestes pressions, la Comissió Europea va proposar el juliol del 2025 suspendre parcialment l'Acord d'Associació entre la UE i Israel, que és el que permet la seva participació en el programa Horizon Europe. La proposta era molt limitada, ja que només afectava a les entitats i empreses israelianes vinculades a l'European Innovation Council Accelerator, el segment destinat a startups i projectes de tecnologies d'ús dual, com la intel·ligència artificial, els drons o la ciberseguretat, sectors especialment sensibles pel seu potencial militar.[326]

La proposta de la Comissió era la primera vegada que una institució de la UE plantejava alguna forma de sanció a Israel. No obstant, aquesta proposta no va aconseguir el suport necessari dels Estats membres de la UE per ser aprovada i de moment la participació d'Israel segueix vigent al programa Horizon Europe.[327]

---

324 Akkerman, M. (2018). Expandiendo la fortaleza: Las políticas de externalización de las fronteras de la UE (Informe). Transnational Institute. https://www.tni.org/es/publicaci%C3%B3n/expandiendo-la-fortaleza

325 Calvo, J., Meulewaeter, C., & Font, T. (2025, 10 de setembre). 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 de juliol). European Commission recommends sanctions on Israel. Globes. https://en.globes.co.il/en/article-european-commission-recommends-sanctions-on-israel-1001517402

327 Euronews. (2025, 30 de juliol). 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

9. Barcelona com a hub tecnològic d'empreses de ciberseguretat

Segons l'informe de l'Agència per a la Competitivitat de l'Empresa de la Generalitat de Catalunya, ACCIÓ del maig del 2025 titulat "La Ciberseguretat a Catalunya", el sector viu una expansió notable i sostinguda. Actualment, 557 empreses formen part d'aquest ecosistema, amb un creixement mitjà anual del 7,9% i un increment global del 58,2% respecte l'any 2018.[328]

En aquest sentit, Catalunya, i especialment la ciutat de Barcelona, s'han consolidat com un territori interessant per a la inversió en ciberseguretat. En els darrers cinc anys, els projectes d'inversió estrangera directa (IED) en aquest àmbit s'han doblat, passant de 6 a 12, mentre que el volum d'inversió s'ha multiplicat per nou, arribant als 207 milions d'euros. Aquest creixement s'explica, en part, per la presència d'un teixit tecnològic sòlid: un 36% dels 160 hubs internacionals d'empreses tecnològiques establerts al territori es dediquen a la ciberseguretat. A escala europea, Catalunya ocupa la cinquena posició en finançament del programa Horizon Europe (2022-2024), amb 15 projectes actius i una inversió de 11,3 milions d'euros, fet que reforça la seva posició com a pol europeu d'innovació i desenvolupament en ciberseguretat.

Barcelona acull nombroses startups de ciberseguretat, consultores i filials d'empreses internacionals dedicades al desenvolupament de solucions de ciberseguretat. A més, el Mobile World Congress i el Barcelona Cybersecurity Congress han reforçat aquest posicionament, esdevenint punts de trobada estratègics per al sector, especialment per a empreses de l'ecosistema de ciberseguretat israelià.

El rol d'ACCIÓ,[329] ha estat fonamental per entendre el creixement del sector a Catalunya i a Barcelona i l'aparició d'empreses de ciberseguretat amb vincles amb Israel. ACCIÓ ha considerat l'Estat d'Israel com una economia altament innovadora, especialment en el sector tecnològic. L'any 2015, ACCIÓ va obrir una oficina exterior a Tel Aviv amb l'objectiu de fomentar els contactes comercials i la col·laboració empresarial. Per entendre els forts lligams entre ACCIÓ i l'Estat d'Israel, l'any 2017, Israel va ser inclòs entre els vuit àmbits territorials estratègics definits per l'agència catalana, fet que demostrava la voluntat d'enfortir els vincles econòmics i tecnològics entre ambdós territoris. Al maig del 2025, gràcies a les pressions derivades del debat públic sobre la relació amb Israel i la pressió

328 ACCIÓ – Agència per a la Competitivitat de l'Empresa, Generalitat de Catalunya. (n.d.). La ciberseguretat a Catalunya.
https://www.accio.gencat.cat/ca/serveis/banc-coneixement/cercador/BancConeixement/eic-la-ciberseguretat-a-catalunya#blo cMaterials_b62ef8b5-b28b-11e8-92dc-005056924a59

329 ACCIÓ és una agència pública adscrita al Departament d'Empresa i Treball de la Generalitat de Catalunya que té per objectiu millorar la competitivitat de l'empresa catalana a través de diferents serveis i ajudes públiques per a facilitar la transformació tecnològica, reforçar la innovació empresarial, donar suport a start-ups i augmentar la internacionalització del sector empresarial català.

sostinguda de la societat civil catalana, especialment de col·lectius i entitats compromeses amb la defensa dels drets de la població palestina, particularment la Coalició Prou Complicitat amb Israel, la Generalitat de Catalunya va anunciar el tancament de l'oficina comercial a Tel Aviv.[330]

Com ja vam alertar amb anterioritat,[331] les missions comercials del programa d'internacionalització de les empreses catalanes d'ACCIÓ, en el seu moment amb oficina operativa a Tel Aviv, permetien explorar sobre el terreny el potencial de nous mercats. L'any 2016, ACCIÓ va organitzar una missió comercial formada per empreses catalanes per participar a l'Israel Homeland Security, una de les exposicions del sector de ciberseguretat més importants del món, amb l'objectiu de crear llaços de cooperació en el sector. ACCIÓ va realitzar aportacions econòmiques a cadascuna de les empreses catalanes que van participar-hi.

Encara avui no existeix cap tipus d'informació sobre les empreses del sector de la ciberseguretat que s'haurien reunit amb la delegació d'empreses catalanes, ni amb quin resultat concret, fet que posa de manifest una manca notable de transparència en la gestió d'aquests contactes i en l'avaluació dels possibles riscos associats a la seva activitat. Aquesta opacitat és especialment preocupant si es considera que bona part d'aquestes empreses de ciberseguretat israelianes operen en sectors tecnològics vinculats a la indústria militar on, com ja s'ha produït, el risc de vulneracions de drets humans és molt elevat.

En aquest sentit, en els darrers anys, un nombre rellevant de companyies de ciberseguretat vinculades a l'ecosistema israelià han triat Barcelona per constituir societats i operar al mercat econòmic de la UE. No és un fenomen espontani, i respon a incentius reguladors i reputacionals per superar les potencials sancions a empreses israelianes arran del genocidi, així com obrir noves oportunitats comercials a Europa, entre d'altres. També ha influenciat el fet que a l'Estat d'Israel s'hagi establert un marc legal més restrictiu a l'hora d'atorgar llicències per exportar programari espia a altres països arran dels escàndols relacionats amb NSO Group, propiciant que les empreses es traslladin a l'estranger.[332]

Al desembre del 2024, un article del diari Haaretz va revelar que Barcelona s'estava convertint en un hub emergent per a empreses d'origen israelià de ciberseguretat i especi-

330 Toro, M., Esteve, M., & Sanz Guerrero, V. (2025, 21 de maig). 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 Observatori de Drets Humans i Empreses a la Mediterrània (ODHE), NOVACT, & SUDS. (2024, 17 d'abril). 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/

332 Franceschi-Bicchierai, L. (2025, 13 de gener). 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/

alistes en el desenvolupament de programari espia.[333] L'article identificava almenys tres equips de hackers israelians especialitzats a trobar vulnerabilitats i febleses de dispositius mòbils que operen des de la capital catalana per poder accedir al seu contingut.

Algunes de les empreses i iniciatives relacionades amb l'ecosistema de ciberseguretat israelià (per tenir origen a Israel o per disposar de personal israelià) i que es van identificar que operaven a Barcelona són: Palm Beach Networks, Epsilon, Paradigm Shift, Variston i Blue Ocean.[334]

De fet, una d'aquestes empreses, Epsilon, és l'organitzadora d'Offensive, una trobada d'empreses especialitzades en ciberespionatge i programari espia que ha tingut lloc a Barcelona durant el gener del 2026.[335] L'esdeveniment s'ha desenvolupat a través de reunions tancades i marcades per una opacitat que facilita que l'acció d'aquestes empreses escapi al control i transparència, amb la participació d'empreses vinculades a la venda de tecnologies de vigilància intrusiva a Estats.[336] Des d'una perspectiva democràtica i de drets humans, que aquest ecosistema prosperi a la ciutat converteix Barcelona en una plataforma europea d'atracció d'un tipus d'activitat empresarial vulneradora de drets humans.[337]

El CEO d'Epsilon, Jeremy Fetiveau,[338] ha estat la persona clau per l'organització de l'esdeveniment i és ex treballador d'una de les majors empreses de la indústria militar estatunidenca, L3 Harris.[339] No obstant, hi ha altres empreses que apareixen amb un rol organitzador com ara Bugscale, Epieos, Interrupt Labs, Randorisec, Paradigm Shift i Radiant

333 Benjakob, O. (2024, 26 de desembre). 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 de gener). 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 de gener). 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_12 910236.html

337 Pareja, P. (2025, 18 de desembre). 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

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

339 Franceschi-Bicchierai, L. (2025, 13 de gener). 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/

Research Labs, aquesta última amb connexions amb NSO Group i el Ministeri de Defensa Israelià.[340]

La idea de Barcelona com a "hub tecnològic" de la ciberseguretat no és cas aïllat; és la materialització europea d'un model de negoci que explota vulnerabilitats i erosiona drets fonamentals. El fet que empreses de ciberseguretat, membres d'un sector on les pràctiques de vigilància massiva i vulneració de drets fonamentals són una constant, segueixin operant a Europa sense grans restriccions i especialment a Catalunya, evidencia la manca de mecanismes de control i de rendició de comptes governamental efectius.

Cas d'estudi: Palm Beach Networks

Palm Beach Networks és una empresa amb seu a Barcelona que va sortir als mitjans al 2024 quan es va conèixer que Alexey Levin, anteriorment investigador de NSO Group, es trobava reclutant personal per Palm Beach.[341] L'empresa està especialitzada en el desenvolupament d'exploits zero day i programari espia.[342]

Segons testimonis recollits pel portal especialitzat TechCrunch, el procés de contractació es caracteritzava per un alt nivell de secretisme i manca de transparència.[343]

Des de llavors, Palm Beach Networks ha canviat de nom en múltiples ocasions (rebranding), imitant les tàctiques emprades per empreses com Candiru per amagar les seves operacions. Fins al maig del 2023, l'empresa Palm Beach Networks es deia Defense Prime Inc, i a mitjans de juny del 2023 una empresa anomenada Head and Tail va iniciar la seva activitat a Barcelona. Curiosament, un any més tard, al juny del 2024 Palm Beach Networks va ser dissolta, i segons l'article de TechCrunch tan Defense Prime com Palm Beach Networks estan lligades a Head and Tail, radicada a Barcelona i de la qual els seus directius són els mateixos que a les empreses esmentades anteriorment.

340 Intelligence Online. (2025, 13 de gener). 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-r adiant-research-labs,110283294-art

341 Franceschi-Bicchierai, L. (2025, 13 de gener). 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 Exploits Zero Day, és un tipus de vulnerabilitat que acaba de ser descoberta i que encara no té un pegat que la solucioni. La principal amenaça resideix que, fins que es llança aquest pegat correctiu i els usuaris l'instal·len als seus equips, els atacants tenen via lliure per explotar la vulnerabilitat i treure profit de la sentència de seguretat els usuaris l'instal·len als seus equips, els atacants tenen via lliure

343 Franceschi-Bicchierai, L. (2025, 13 de gener). 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/

Aquestes empreses defineixen el seu objectiu com el disseny, desenvolupament, programació, implementació, manteniment, actualització, suport tècnic, adquisició, llicència, venda i comercialització de software.[344]

En el procés d'establiment d'aquesta empresa a Barcelona figuren diversos noms clau. Una persona anomenada Sai Gopal figura com a signant autoritzat de Head and Tail als registres comercials de l'Estat Espanyol,[345] i al mateix temps, algú amb el mateix nom figurava com a tresorer de Defense Prime als registres comercials de Florida, als Estats Units d'Amèrica. Els registres comercials de l'empresa també indiquen que Alexey Levin, director de tecnologia que va intentar contractar per Palm Beach Networks, és ara el director de Head and Tail.[346]

L'empresa es troba actualment en un procés d'expansió i es pot comprovar a la seva pàgina web els diferents perfils professionals que sol·liciten.[347]

A banda d'aquesta empresa, trobem un conglomerat d'empreses que aglutinen els mateixos noms de persones. En aquest sentit, l'empresa Apex Software Solutions (abans coneguda com a CyberNinja SL) amb seu a Passeig de Gràcia, on des de juny del 2025, també apareixen com a apoderats solidaris tan Alexey Levin com Sai Gopal i Yosef Aloni.[348]

El fet que Alexey Levin, antic investigador de NSO Group, es trobi reclutant personal per una empresa amb seu a Barcelona és un indici clar de la facilitat amb què la ciutat s'ha convertit en un espai propici per a l'arrelament d'empreses de ciberseguretat, incloses aquelles empreses vinculades amb d'altres que tenen antecedents de vulneracions de drets fonamentals, com en el cas de NSO. Alhora, és un fet profundament preocupant, ja que posa en evidència la manca de mecanismes de control i supervisió sobre aquest tipus d'activitats, així com el risc que Barcelona es consolidi com un centre de desenvolupament de tecnologies de doble ús, amb aplicacions tant civils com militars, sense una reflexió ètica ni política sobre les seves conseqüències.

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.

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 i Recomanacions

Israel continua utilitzant Palestina continua com un "laboratori" per al testatge d'armament i tecnologies militars. Israel ha provat sobre el poble palestí armes d'última generació, incloent sistemes basats en intel·ligència artificial que incrementen la precisió letal sense cap consideració ètica, legal ni humana. Aquest "laboratori" és l'epicentre des d'on aquestes tecnologies, coneixements i pràctiques es transfereixen i s'exporten a altres parts del món, alimentant conflictes armats i reforçant la repressió de la dissidència política. Per exemple, l'externalització del control migratori, la repressió i la criminalització de la protesta i l'ús creixent d'eines algorítmiques d'avaluació del risc reprodueixen, en l'espai europeu, tècniques de govern assajades prèviament sobre poblacions colonitzades.

A partir del mapatge de les principals empreses israelianes còmplices, amb protagonisme o la tecnologia de les quals ha estat utilitzada al genocidi de Palestina i les seves estructures de finançament, l'estudi ha traçat els canals d'entrada d'aquestes a Europa. Les relacions militars i de seguretat entre la UE i Israel són especialment rellevants. La UE fa servir la tecnologia israeliana per avançar en els plans de rearmament, però també necessita vendre la seva producció armamentística a aquest país. Aturar aquestes relacions comercials, especialment en matèria d'armament i seguretat, és fonamental per posar fi al colonialisme, l'ocupació, l'apartheid i el genocidi d'Israel contra el poble palestí.

La present recerca ha identificat nou portes d'entrada de les empreses israelianes del sector defence tech a Europa. Cada porta revela jurisdiccions, mecanismes i condicions que faciliten aquesta penetració, il·lustrades amb casos específics d'empreses i d'aliances entre actors polítics i econòmics europeus. Aquestes portes d'entrada mostren com el know-how de tecnologia opressiva israeliana fa temps que ha trobat maneres de penetrar el mercat de la Unió Europea i això s'ha incrementat arran del genocidi del poble palestí a la Franja de Gaza. L'estudi també apunta tendències futures i pols d'atracció en fase de desenvolupament que podrien ser explotats pel complex militar-industrial israelià en els propers anys. Algunes d'aquestes tendències es resumeixen a continuació.

En primer lloc, totes les portes d'entrada serien impossibles sense la facilitació dels governs d'Israel i de la UE. Mentre que països com Xipre, en la seva recerca d'inversió estrangera, aspiren a convertir-se en una StartUp Nation inspirada en el model israelià, altres com Alemanya volen tecnologia militar israeliana per rearmar-se i expandir la seva indústria militar. Israel dona suport a les seves empreses mitjançant mecanismes polítics i econòmics com la creació d'ambaixades en hubs tecnològics de l'OTAN (com Estònia), l'organització de fires internacionals de ciberseguretat o tecnològiques, o l'establiment d'acords entre agències d'internacionalització i innovació amb contraparts europees. Paral·lelament, lobbies i actors econòmics com cambres de comerç contribueixen a crear narratives favorables i a influir sistemàticament per facilitar aquests acords, mentre intenten invisibilitzar el rol d'aquestes empreses en les polítiques de genocidi, apartheid i ocupació contra el poble palestí.

En segon lloc, l'expansió de l'OTAN i el pla de rearmament europeu actuen com un pol d'atracció per a centenars d'empreses israelianes de la indústria militar i seguretat tecnològica. El testatge d'armament i tecnologia a Ucraïna, així com l'establiment d'aliances militars en aquest país, obren la porta a contractes amb l'OTAN. Aquests contractes asseguren la interoperabilitat i el compliment amb els estàndards europeus i transatlàntics, requisits indispensables per accedir a més contractes en aquests espais. En aquest context, empreses amb vinculació amb el genocidi contra el poble palestí obren filials comercials, adquireixen empreses o creen plantes de producció d'armament i desenvolupament tecnològic a les principals capitals europees.

Europeu, així com comercialitzar programaris extremadament intrusius sense cap control governamental. Mentre que, a Catalunya, persones ex-treballadores d'empreses com NSO Group han impulsat el reclutament de professionals per a startups israelianes que operen a Barcelona, replicant models de negoci i pràctiques similars a les emprades a Palestina.

En quart lloc, l'expansió del sector defence tech tampoc seria possible sense les dinàmiques del capitalisme financer. Institucions financeres internacionals, bancs, governs, asseguradores, auditores i agències d'inversió asseguren el flux econòmic necessari per al creixement d'aquestes empreses. Paral·lelament, alguns països europeus redueixen traves administratives i impostos per atraure aquesta inversió estrangera. Luxemburg exemplifica aquest model, permetent l'aterratge de les principals empreses israelianes de vigilància massiva, com NSO Group, i creant un entramat empresarial que dificulta la traçabilitat i el control governamental. Altres empreses més petites accedeixen a fons del govern israelià o a programes europeus de recerca per desenvolupar prototips, amb l'objectiu d'obtenir finançament més ampli a través de rondes d'inversió internacional o préstecs de grans bancs europeus i israelians.

La Unió Europea no pot entendre's únicament com un espai receptor passiu de tecnologies desenvolupades en contextos de genocidi, ocupació o violència estructural, sinó també com un actor que, a través de marcs reguladors, financers i narratius, contribueix a la consolidació d'un règim tecnosecuritari global. Aquesta dinàmica, inserida en processos més amplis de securitització i en l'entrellaçament entre lògiques colonials externes i règims interns de control, tendeix a situar la seguretat com a principi rector de l'acció pública, fins i tot quan això entra en tensió amb els drets humans i amb les obligacions internacionals dels Estats.

Cal destacar que aquesta narrativa securitària, capitanejada pel desenvolupament i la implantació de tecnologies de vigilància, posa en evidència una contradicció alarmant pel que fa a la ciberseguretat. Aquestes tecnologies sovint depenen de l'explotació de vulnerabilitats en dispositius i infraestructures digitals, en lloc de la seva correcció. En

aquest sentit, contribueixen al que es coneix com a "mercat de vulnerabilitats"[349] en el qual errors de seguretat són comercialitzats i mantinguts actius per a usos operatius. En absència de marcs reguladors sòlids i de mecanismes de control efectius sobre aquestes pràctiques, la UE pot estar afavorint indirectament la persistència d'aquestes vulnerabilitats dins del seu propi entorn digital. Això genera un efecte paradoxal, tecnologies justificades en nom de la seguretat poden, alhora, incrementar els riscos per a la seguretat interna, la privacitat i la integritat de les infraestructures digitals. En termes pràctics, l'explotació d'aquestes vulnerabilitats pot deixar dispositius i sistemes més exposats a accessos no autoritzats, ampliant la capacitat d'atac i afectant també sistemes utilitzats per administracions públiques i actors crítics.

En aquest context, la Unió Europea i els seus Estats membres tenen l'obligació, derivada del dret internacional i dels seus propis tractats, de prevenir el genocidi, els crims de guerra i els crims de lesa humanitat, així com de no contribuir-hi directa ni indirectament. Aquest deure exigeix no només acció exterior, sinó també coherència interna mitjançant mesures administratives, contractuals, financeres i fiscals destinades a evitar que empreses implicades en crims internacionals accedeixin a contractes públics, finançament o altres beneficis econòmics dins la UE. En absència d'aquestes salvaguardes, es podria configurar una forma de complicitat o assistència prohibida pel dret internacional.

En aquest marc, les recomanacions pràctiques, per abordar aquesta problemàtica, s'adrecen a autoritats polítiques, reguladores i econòmiques a escala europea, estatal i local.

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/

Recomanacions

1. Prohibició i exclusió en la contractació pública:

Es recomana a la Comissió Europea i al Parlament Europeu que la futura reforma del règim de contractació pública de la UE (Public Procurement Act), en el marc de la revisió de les directives vigents) incorpori clàusules d'exclusió clares i vinculants per impedir la participació en licitacions d'empreses implicades en vulneracions greus dels drets humans, contextos d'ocupació il·legal o tecnologies de vigilància massiva, amb especial atenció al Territori Palestí Ocupat. Aquesta vinculació hauria d'acreditar-se mitjançant fonts verificables —incloent-hi mecanismes de Nacions Unides,[350] com la base de dades d'empreses vinculades als assentaments israelians, així com evidències documentades aportades per organitzacions de la societat civil—. L'aplicació d'aquestes clàusules hauria d'anar acompanyada de guies clares i mecanismes de verificació, seguiment i control durant tot el cicle del contracte.

2. Reforç de la regulació sobre productes i tecnologies de doble ús:

Es recomana reforçar l'aplicació del Regulation (EU) 2021/821, reconeixent les seves limitacions actuals en la prevenció d'usos indeguts en contextos de vulneracions greus dels drets humans. Les revisions previstes (2026 i 2028) haurien d'abordar aquestes deficiències i derivar en reformes vinculants. En particular, caldria reforçar la definició de risc, establir criteris harmonitzats entre Estats membres i impedir exportacions amb risc d'ús en repressió o vigilància massiva, aplicant el principi de precaució. Així mateix, s'haurien d'incorporar mesures per evitar l'elusió dels controls (incloent-hi reexportacions i intermediació) i obligacions reforçades de diligència deguda. Finalment, es recomana ampliar l'abast del règim a tecnologies i empreses no estrictament militars que, en contextos com Palestina, puguin contribuir a vulneracions greus del dret internacional.

3. Prohibició total del programari espia comercial:

La Comissió Europea ha de prohibir el desenvolupament, la producció, la comercialització, la venta, l'exportació i l'ús de programari espia per part d'empreses privades i agències governamentals. Així mateix, també ha d'imposar una prohibició del comerç de vulnerabilitats i exploits per a qualsevol finalitat que no sigui el reforç de la seguretat dels sistemes i infraestructures.

350 United Nations Human Rights Council, Office of the High Commissioner for Human Rights. (2025, 26 de setembre). 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-detail ed

4. Sancions específiques i restriccions econòmiques:

Es recomana que el Servei Europeu d'Acció Exterior impulsi l'adopció de sancions específiques, en el marc de la Política Exterior i de Seguretat Comuna, contra l'Estat d'Israel i contra empreses i entitats —incloent-hi nacionals de tercers països— vinculades a vulneracions greus del dret internacional a Palestina, en coherència amb les mesures provisionals del Tribunal Internacional de Justícia i el dictamen de la Relatora Especial de Nacions Unides. Aquestes mesures haurien d'incloure la congelació d'actius i altres restriccions econòmiques dirigides, prenent com a referència instruments similars dels Estats Units. Igualment, es recomana limitar l'accés al mercat europeu, incloent-hi la prohibició d'establiment, registre, participació en licitacions públiques i activitats de promoció empresarial, assegurant una aplicació harmonitzada entre Estats membres.

5. Embargament integral d'armes:

Es recomana que el Consell de la Unió Europea, en el marc de la Política Exterior i de Seguretat Comuna i a proposta del Servei Europeu d'Acció Exterior, adopti un embargament integral d'armes contra Israel, amb aplicació harmonitzada pels Estats membres. Aquesta mesura hauria d'incloure la prohibició d'exportació, transferència, trànsit i assistència tècnica de material militar i tecnologies associades, així com de components i tecnologies de doble ús amb possible aplicació militar. Igualment, hauria d'incorporar mecanismes per prevenir l'elusió (incloent-hi reexportacions i intermediació) i sistemes de seguiment que garanteixin el compliment efectiu a nivell europeu.

6. Control dels fluxos financers il·lícits:

Es recomana que la UE reforci l'aplicació dels instruments existents en matèria de control de fluxos financers il·lícits per intensificar la supervisió de les inversions i operacions vinculades a empreses —especialment dels sectors militar, defence tech i tecnologia de seguretat— associades a riscos elevats de vulneracions del dret internacional humanitari i dels drets humans, incloent-hi operacions vinculades al Territori Palestí Ocupat. Aquests riscos haurien d'identificar-se mitjançant un enfocament basat en múltiples fonts verificables —com mecanismes de Nacions Unides i evidència de la societat civil— utilitzades com a indicadors d'implicació i no com a classificacions automàtiques de risc. Així mateix, caldria reforçar la coordinació i harmonització dels criteris de supervisió a nivell europeu.

7. Diligència deguda reforçada:

Es recomana exigir a les entitats financeres, inversors i asseguradores europees l'aplicació de diligència deguda reforçada en operacions que involucrin empreses que operen en contextos de conflicte armat o ocupació —incloent-hi, de manera específica, el Territori Palestí Ocupat—, especialment en els sectors militar, defence tech i tecnologia de seguretat. Aquesta diligència hauria d'incloure la identificació de beneficiaris finals, l'anàlisi de cadenes de valor i d'ús final, i la detecció d'estructures societàries opaques, amb l'objectiu de prevenir la contribució directa o

indirecta a vulneracions greus del dret internacional humanitari i dels drets humans. Així mateix, hauria de basar-se en fonts fiables, incloent-hi mecanismes de Nacions Unides i evidència documentada per organitzacions de la societat civil.

8. Transparència obligatòria en acords militars i tecnològics:

Establir obligacions legals de transparència i auditoria independent en tots els acords comercials, de recerca i desenvolupament entre actors europeus i empreses israelianes del sector militar, defence tech i tecnologia de seguretat. Això inclou la publicació periòdica de dades sobre contractes, inversions i transferències tecnològiques, amb criteris clars de diligència deguda en drets humans. El sistema hauria d'integrar mecanismes per detectar rebrandings, creació de filials pantalla o adquisicions d'empreses europees utilitzades per esquivar la traçabilitat i diluir responsabilitats, i garantir que no es substitueixi la transparència per estructures opaques.

9. Exclusió de programes europeus de recerca i innovació:

Es recomana reforçar l'aplicació del sistema d'alerta i exclusió de la UE (EDES)[351] per incloure de manera explícita criteris relacionats amb vulneracions greus dels drets humans, de manera que empreses dels sectors militar, defence tech i tecnologia de seguretat implicades en contextos d'ocupació, apartheid o genocidi no puguin accedir a fons públics de R+D, inclosos programes com Horizon Europe. Això requeriria ampliar els supòsits d'exclusió més enllà de la mala conducta financera o administrativa, i incorporar evidència procedent de mecanismes de Nacions Unides i altres fonts verificables. Així mateix, caldria garantir mecanismes de revisió contínua i seguiment durant tota la implementació dels projectes, incloent-hi la possibilitat d'exclusió en fases posteriors si es detecten riscos o implicacions en vulneracions de drets humans.

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