Arab Reform Initiative

TECH , POWER & CONFLICT DOSSIER

THE EUROPEAN NETWORK: CORPORATE INVOLVEMENT AND DEVELOPMENT FUNDING BEHIND ISRAEL'S AI-POWERED WARFARE IN GAZA

Dima Samaro

Published by:

Arab Reform Initiative
The Arab Reform Initiative is an independent Arab think tank working with expert partners in the Middle East and North Africa and beyond to articulate a home-grown agenda for democratic change and social justice. It conducts research and policy analysis and provides a platform for inspirational voices based on the principles of diversity, impartiality, and gender equality.
https://www.arab-reform.net/

About the author

Dima Samaro is a Palestinian lawyer and tech policy researcher with over a decade of experience at the nexus of technology, law, and human rights in the MENA region. She leads Skyline International's work documenting digital rights violations—including surveillance, biometric data misuse, and AI-driven repression—by state and corporate actors. Her advocacy focuses on corporate accountability and human rights due diligence in conflict-affected settings, and she champions robust privacy and freedom of expression laws. Previously, she has held roles with positions with Access Now, Internews, the Business & Human Rights Resource Centre, and DAI Consulting. Dima also serves on the boards of Innovation for Change MENA Hub and the Surveillance in the Global Majority Network and is a member of the steering committee for the VUKA! Coalition for Civic Action.

Disclaimer:

The information and views set out in this report are those of the author(s) and do not necessarily reflect the views of the Arab Reform Initiative, its staff, its board or its funders.

© 2026 Arab Reform Initiative.

This license allows re-users to distribute, remix, adapt, and build upon the material in any medium or format for non-commercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.

Cover photo: People gather in front of the European Union (EU) Council building to stage a demonstration demanding the immediate suspension of the EU-Israel Association Agreement and an urgent halt to all arms supplies, in Brussels, Belgium - 15 July 2025.

© Dursun Aydemir/Anadolu Images

This paper is a part of the Tech, Power, and Conflict in MENA dossier, coordinated and edited by Nada Kabbary Mousa (Mozilla Fellow 2024-2026) and Andrew Findell-Aghnatios (Program Lead - Tech & Society) and co-funded by the Mozilla Foundation and ARI.

September 2026

Table of Contents

Introduction 4

Methodology 5

European Corporate Ties to the Military Web in Gaza 7

- The Greek Gateway to EU Public Funds 7
- The Spanish Technology Bridge and Diplomatic Dissonance 8
- French Engineering and the Dual-Use Deception 8
- The German Industrial Backbone 9

Subsidizing the Military Operations in Gaza Through Research and Development Funding 11

European Soil as the Digital Architecture of AI Warfare 13

The Failure of Legal Standards and Corporate Responsibility Mandates 14

Recommendations 16

- For EU and national policymakers 16
- For companies 16

Conclusion 17

Annex I: Registry of Contribution to Genocide 18

Annex II: EU-Funded R&D Projects 24

Introduction

The acceleration of warfare to an industrial scale in Gaza is not a solo Israeli achievement. It also depends on a wider transnational ecosystem of military, technological, and industrial cooperation, including with European actors. While most European governments have issued formal statements expressing concern over the humanitarian catastrophe in Gaza and condemning the relentless bombardment and scale of military operations,[1] many European companies have continued to supply components, technologies, and services that support Israel's military capabilities, transitioning in the process from passive suppliers to active participants in the deployment of autonomous systems.

The European stance on Palestinian rights rings hollow against the backdrop of its own industrial supply chains. In 2024 and 2025, a historic wave of diplomatic recognition of the State of Palestine by nations such as Spain, Belgium, Norway, and France signaled a symbolic commitment to international law, bringing the total number of recognizing states to over 150.[2] Yet, while these gestures suggest a major shift in Western policy, the flow of dual-use Artificial Intelligence (AI) and surveillance technology remains largely uninhibited. This political moment shields a systemic hypocrisy: diplomatic support for a Palestinian state exists alongside corporate contracts that arm the machinery of its dismantling. Even in Sweden, which recognized Palestine in 2014,[3] celebrated diplomatic gestures coexist with a vast network of European corporate and institutional support that continues to furnish a key part of the technological backbone of the warfare that makes such recognition necessary.

For the past two years, the genocidal war on Gaza has moved into a paradigm of AI-driven destruction. Israel's large-scale use of targeting systems such as Lavender and "Where's Daddy?" has turned family shelters and childhood homes into data points for execution.[4] According to media reports citing Israeli intelligence officers, Lavender carries a known 10% error rate, meaning one in 10 people it flags is a civilian, a fact that did not deter its widespread use. Human oversight for these machine-generated lists was reduced to a mere 20 seconds per target, a window used solely to verify that the target was male before authorizing a strike.[5] These tools are often programmed to wait for an individual to enter their residence, which means that strikes often occur at night, when multi-generational families are gathered together. This process of "automated domicide" has contributed to more than 71,000 Palestinians killed and 171,152 living with life-altering wounds.[6] The human outcome is a catastrophic erasure of entire lineages in a single flash, compounded by the systematic destruction of the hospitals and schools that once held the fabric of Palestinian society together.[7]

Corporate ledger sheets document a massive commercial benefit from this devastation. The Israeli company Elbit Systems, for example, reported a staggering revenue jump to nearly US$2 billion (around €1.7 billion[8]) in late 2025, reaching an unprecedented order backlog of

1 Francesca Albanese, "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, United Nations Human Rights Council, 2 July 2025, available at https://www.un.org/unispal/document/a-hrc-59-23-from-economy-of-occupation-to-economy-of-genocide-report-special-rapporteur-francesca-albanese-palestine-2025/ (Albanese, "*From Economy of Occupation to Economy of Genocide*").

2 Al Jazeera, "Which are the 150+ countries that have recognized Palestine as of 2025?", 23 September 2025, available at https://www.aljazeera.com/news/2025/9/23/which-are-the-150-countries-that-have-recognised-palestine-as-of-2025.

3 UNISPAL, "Human Rights Council Adopts Seven Resolutions on the Situation of Human Rights in the Occupied Palestinian Territory", 4 April 2024, available at https://www.un.org/unispal/document/auto-insert-203405/.

4 Yuval Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza", +972 Magazine, 3 April 2024, available at https://www.972mag.com/lavender-ai-israeli-army-gaza/ (Abraham, "'Lavender': The AI machine").

5 Abraham, "'Lavender': The AI machine".

6 Alex Croft, "Israeli military accepts that 71,000 Palestinians were killed in Gaza war for first time, says report", The Independent, 29 January 2026, available at https://www.independent.co.uk/news/world/middle-east/israel-gaza-war-death-toll-military-hamas-b2910276.html.

7 Al Jazeera, "Timeline: Israel's attacks on hospitals throughout its war on Gaza", 13 April 2025, available at https://www.aljazeera.com/news/2025/4/13/timeline-israels-attacks-on-hospitals-throughout-its-war-on-gaza.

8 This and other USD/EUR conversions are calculated based on approximate rates in September 2026.

US$25.2 billion (around €21.7 billion).[9] This is not an isolated success; by providing the sensors and data processing units that power these strikes, companies such as the German-based Hensoldt and French-Italian STMicroelectronics have turned a humanitarian collapse into a lucrative business opportunity. By converting documented human rights violations into a "combat-proven" brand and providing the Research and Development (R&D) backbone through programs such as Horizon Europe (which has granted over €1.1 billion – around US$1.3 billion – to Israeli entities), these European actors have become actively involved in a campaign of automated genocide.

This paper recenters the narrative on the essential European network that sustains this ecosystem to answer three main questions:

1. How do Israeli defense companies use European subsidiaries to get around arms embargoes and tap into public funding?
2. What is the actual scale of European Union (EU) research grants, such as Horizon Europe, in supporting the technology used in Gaza?
3. How does the hosting of military targeting data and AI infrastructure on European servers implicate the EU as the digital architecture of the very practices its own regulations prohibit?

Methodology

The findings in this paper result from an investigative synthesis necessitated by the limited availability of public information. No comprehensive database exists to track the flow of European technology into the Israeli military and AI ecosystem. As a result, the researcher had to act as a forensic aggregator to overcome the shroud of secrecy maintained by both European states and private corporations. These entities frequently use national security and commercial confidentiality to hide their contracts from the public, effectively turning the digital supply chain into a black box.

To bridge this information gap, the researcher built upon the foundational work of organizations such as Amnesty International, Who Profits, AlgorithmWatch, and the United Nations Special Rapporteur on the Occupied Palestinian Territories. This paper consolidates fragmented pieces of evidence found in military trade journals, corporate press releases, and non-governmental organization field reports to create a unified registry of support to genocide.

For the purposes of this paper, corporate involvement is assessed through three analytical categories of contribution. Material contribution involves the supply of physical parts or components for weapons platforms. Financial contribution tracks the flow of R&D subsidies, public grants, or direct investment into military-linked firms. Enabling contribution identifies the provision of essential "dual-use" services, such as cloud infrastructure and the data processing capacity required for algorithmic targeting.

This paper's classification of material, financial, and enabling contribution follows the framework developed by the UN Guiding Principles on Business and Human Rights, which assess a company's connection to an adverse human rights impact through its own activities, products, or services, or through its business relationships. This is an analytical and human-rights-due-diligence framework, not a determination of criminal or civil legal liability, which only a court of competent jurisdiction can make.

The researcher adopts a framework rooted in Palestinian-centered epistemology rather than the techno-optimism that dominates mainstream Western and Israeli reporting. Where conventional coverage focuses on the sophistication and technical precision of AI systems, this paper shifts the lens toward accountability, treating the supply chains not as innovation but as infrastructure that renders Palestinian life machine-readable and targetable, erasing not only individual lives but Palestinians' collective existence.

This framework is designed to be replicable. The intersection of public subsidy records, corporate disclosures, and field-based human rights documentation produces a methodology that other researchers can apply to map the corporate and state structures enabling automated warfare across different geopolitical contexts. The template is scalable and testable, filling a persistent gap in conventional oversight, where these data streams are typically siloed.

Three primary groups of companies serve as the focus for mapping this ecosystem. One group

9 Elbit Systems, "Elbit Systems Reports Third Quarter 2025 Results", 20 November 2025, available at https://www.elbitsystems.com/news/elbit-systems-reports-third-quarter-2025-results.

consists of European-based corporations operating in the security, technology, AI, and military sectors, including their international subsidiaries. Another group includes Israeli companies in these same fields that receive funding from EU programs or maintain active research collaborations and joint ventures with European firms. The final group involves global technology companies that operate critical cloud infrastructure, data centers, or AI services within EU territory. A strict geographic focus remains on the EU and its member states.

The timeframe for analyzing operational data and corporate revenue surges spans from October 2023 to March 2026. A window of this length captures the transition from an economy of occupation to an economy of genocide, as defined by recent UN reports.[10] It also allows for the tracking of sudden spikes in defense-related profits in correlation with specific military operations in Gaza. The scope for tracing R&D subsidies extends back to 2021. A longer window of this type accounts for the multi-year development cycles required for AI and defense technologies to move from a funded project to active deployment.

Specific inclusion criteria guided the selection of these companies. First, a firm must maintain a headquarters or infrastructure in the EU or participate in research collaborations with European partners. Second, a firm must have received EU-level R&D funding for security or AI projects at any point during the five-year development window. Third, the technology must be documentarily linked to the Israeli defense apparatus in Gaza through primary sources or investigative reports. Companies providing purely non-security-related infrastructure were excluded to keep the research focused exclusively on the technical and financial aspects most directly connected to military targeting and operational systems.

The research process followed a multi-layered verification protocol to establish high-confidence linkages. Baseline data collection began with an audit of corporate annual reports and investor disclosures to identify defense-sector revenue surges often omitted from public-facing marketing. Analysis of EU funding portals, specifically the European Defence Fund (EDF) and Horizon Europe, provided the second layer of verification regarding public grants for surveillance and AI development. The evidentiary threshold required successful triangulation between these financial records and the operational reality documented in human rights reports or investigative journalism.

Indirect involvement was assessed through the presence of critical components or digital infrastructure essential to the functioning of larger autonomous systems. Inferences regarding military application were made by matching specific technical capabilities, such as high-frequency sensor resolutions or cloud processing speeds, with the known requirements of Israeli defense operations in Gaza. Any entity lacking a direct documentary link or a clear technical necessity for military use was not included in the registry.

The resulting registry in Annex I classifies each entity according to the three categories of contribution defined above. Each company entry identifies whether its involvement constitutes material contribution, financial contribution, enabling contribution, or a combination of these categories. This classification is designed to serve as an actionable tool. Litigators pursuing corporate accountability can isolate entities by contribution type. Parliamentary committees reviewing export licenses can identify which category of support persists despite declared embargoes. Divestment campaigns can prioritize targets based on the directness of a company's contribution to the kill chain. The methodology also provides a specialized architecture for tracking the migration of civilian AI into systems used for surveillance, mass destruction, and targeted killing. Future investigations can adapt this specific layering of subsidy records and operational data to audit other high-risk supply chains where corporate accountability remains hidden.

10 Albanese, "From Economy of Occupation to Economy of Genocide".

European Corporate Ties to the Military Web in Gaza

The integration of European technology into the Israeli war effort, and that of Israeli military technology in European industry, is the result of structured corporate relationships rather than chance. This network ranges from direct suppliers of lethal components to strategic partners in R&D. These corporate ties often operate in total opposition to the diplomatic stances of the countries where these companies are headquartered. Israeli military firms have effectively created backdoors into the European economy and public treasury by establishing local subsidiaries and deep R&D partnerships.

The 2025 report by the UN Special Rapporteur, Francesca Albanese, *From Economy of Occupation to Economy of Genocide*, documents a fundamental shift in how this infrastructure operates. The report's findings reveal a deadly transformation, where long-standing systems of colonial control have been fully mobilized to carry out mass violence and immense destruction. This economy of genocide relies on a global web of corporate entities that contribute to the essential financial and technical underpinnings for the military campaign.[11] Under this model, European corporate nodes in the tech and military sectors operate as a key part of the economic backbone of the genocide. These firms ensure the efficiency required for mass killings and the systematic destruction of life in Gaza through the provision of drone components, targeting algorithms, and high-frequency hardware.

Corporate frameworks frequently rely on the "dual-use" label as a legal fiction to bypass stringent export controls and ethical oversight. Characterizing high-capacity cloud servers, data processing software, or advanced sensor arrays as purely civilian technology ignores the seamless integration of these tools into modern autonomous warfare. The resulting evidence challenges the perceived neutrality by demonstrating how AI for civilian purposes acts as the foundational layer for target identification and surveillance. Moving past these official designations exposes a reality where the boundary between commercial innovation and military application has effectively collapsed.

Below are cases from four EU member states that illustrate how this industrial integration facilitates these operations through specific corporate structures and state-subsidized projects.

The Greek Gateway to EU Public Funds

In May 2023, Israel Aerospace Industries (IAI) acquired 94.5% of Intracom Defense, a Greek firm, six months before the war on Gaza began.[12] This acquisition allowed the parent company, which manufactures the drones used for the automated domicide of Gaza, to bypass rules that limit EU defense funding to European entities. The IAI gained a direct conduit to the EDF through the use of this Greek subsidiary, a long-established Greek defense manufacturer that IAI acquired specifically to obtain this access.[13]

Evidence of this failure surfaced in late 2024, when Intracom was selected to lead the ACTUS (Advanced Capabilities & Certification for Tactical UAV Systems) drone program.[14] The total program budget stands at €59 million (around US$69 million), of which the European Commission finalized an award of €42 million (around US$49 million) in EU tax money for this project well after the genocide in Gaza had begun.[15] Defense ministries from countries that have signaled support for Palestinian rights, including

11 Albanese, "From Economy of Occupation to Economy of Genocide".

12 Israel Aerospace Industries, "IAI has Acquired Greek Defense Company Intracom Defense", 17 May 2023, available at https://www.iai.co.il/iai-has-acquired-greek-defense-company-intracom-defense.

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

14 Intracom Defense, "Intracom Defense Launches the ACTUS Project", 3 February 2025, available at https://www.intracomdefense.com/intracom-defense-launches-the-actus-project/.

15 Intracom Defense, "National & European Funded Programs", available at https://www.intracomdefense.com/national-european-funded-programs/, accessed 24 August 2026.

Belgium and Norway, are co-funding this project.[16] This creates a loop in which European public funds advance the R&D of a company whose parent firm is currently deploying those same drone capabilities against Palestinian families in Gaza.

The ACTUS case represents financial and enabling contributions operating simultaneously. EU institutions are not passively tolerating this arrangement. They are actively selecting an IAI subsidiary as the lead coordinator for a project that develops the next generation of armed drone technology. The involvement is structural, as it is embedded in the grant architecture itself.

The Spanish Technology Bridge and Diplomatic Dissonance

The Spanish government moved toward an unprecedented level of political commitment in 2025 through its package of nine measures to stop the genocide in Gaza.[17] These actions included a total arms embargo and the denial of entry for individuals linked to war crimes. While Spain has canceled hundreds of millions in direct contracts with Israeli firms such as Rafael and Elbit Systems, the "exception clauses" within the 2025 embargo law allow certain high-tech collaborations to persist for the sake of national interest.[18]

The industrial reality reveals a significant accountability gap despite these measures. Spain's flagship defense firm, Indra Sistemas, remains a strategic partner to IAI.[19] These entities collaborate on the Heron 1 and Heron TP drone systems, which serve as the Israel Defense Forces (IDF)'s primary platforms for targeting and missile strikes in Gaza. Indra's contribution is not peripheral. The company provides the radar, data fusion, and command-and-control architecture that allows the Israeli military to integrate surveillance feeds from drones, satellites, and ground sensors into a single interface for target selection. Indra also leads over 70 EU-funded defense projects and was awarded €24 million (around US$28 million) for AI infrastructure on the Ayalon 20 highway in Tel Aviv, deepening its operational presence in Israel.[20]

In November 2025, Spanish authorities used the "national interest" loophole to permit the transfer of Israeli-made technology to Airbus production lines in Madrid and Seville.[21] Officials justified this move by citing the need to protect 14,000 Spanish jobs and preserve the viability of major European aerospace projects such as the SIRTAP drone, a joint development project that integrates IAI technology under a European airframe.[22] Spanish-developed sensors and software continue to provide the essential architecture for the very systems that make Palestinian sovereignty impossible. The Indra partnership and the Airbus exemption demonstrate that, while an embargo can stop the flow of conventional military hardware, it struggles to sever the deep digital arteries that connect European R&D to the Israeli kill chain.

French Engineering and the Dual-Use Deception

The flow of critical components also persists in France, which moved toward recognition of Palestine in 2025. Investigations by the media outlet Disclose revealed that French firms Sermat, Safran, and Thales continued to supply sensors and motors

16 Investigate Europe, "European Defence Fund".

17 La Moncloa, "President of the Government of Spain announces measures on Gaza", 8 September 2025, available at https://www.lamoncloa.gob.es/lang/en/presidente/news/paginas/2025/20250908-gaza-measures.aspx.

18 International Middle East Media Center, "Spain cancels major arms deal with Israel", 16 September 2025, available at https://imemc.org/article/spain-cancels-major-arms-deal-with-israel/.

19 Diario Socialista, "Denuncian a Indra en su Junta de Accionistas por sus vínculos con el negocio de la guerra y el genocidio en Gaza", 26 June 2025, available at https://diariosocialista.net/2025/06/26/denuncian-a-indra-en-su-junta-de-accionistas-por-sus-vinculos-con-el-negocio-de-la-guerra-y-el-genocidio-en-gaza/.

20 Indra, "Indra implements an advanced dynamic tolling system with artificial intelligence worth 24 million euros in Israel", 12 May 2022, available at https://www.indragroup.com/en/news/indra-implements-advanced-dynamic-tolling-system-artificial-intelligence-worth-24-million.

21 Reuters, "Spain exempts Airbus from Israeli tech ban", 30 December 2025, available at https://www.reuters.com/business/aerospace-defense/spain-exempts-airbus-israeli-tech-ban-2025-12-30/.

22 Al-Monitor, "Spain exempts Airbus from Israeli tech ban", 30 December 2025, available at https://www.al-monitor.com/originals/2025/12/spain-exempts-airbus-israeli-tech-ban (Al-Monitor, "Spain exempts Airbus").

essential for Israeli drones throughout the genocide.[23] French-made alternators and actuators were shipped as recently as late 2025 to equip Hermes 900 unmanned aerial vehicles (UAVs).[24] According to the investigation, over two years, Sermat delivered 29 alternators and 171 actuators to Elbit Systems, with over three-quarters of the actuators shipped by air between 2024 and October 2025. The total documented value of these deliveries is €843,300 (around US$980,000). A further shipment of eight alternators was scheduled for delivery via UPS to Elbit's facility in Karmiel on 20 October 2025.[25]

Authorities often classify these components as "civilian" to bypass export bans, yet their function is purely military.[26] French authorities do not classify Sermat's actuators as military or dual-use equipment, meaning they require no export authorization and fall entirely outside the embargo framework. Sermat's actuators are the electric motors that provide stabilization and precise control for the drone's high-resolution cameras. These sensors are the eyes required by AI targeting systems such as Lavender to identify targets at a massive scale.[27] The alternators provided by Sermat allow these drones to maintain the 30-hour surveillance loops used to track Palestinians to their homes before a strike is ordered.[28]

The operational chain from the French factory floor to Gaza airstrikes is direct. The Hermes 900, equipped with French-made components, has been documented conducting strikes on residential areas throughout the current military campaign.[29] Safran's Euroflir 410 sensors, which provide high-precision targeting and the classification of individuals on surveillance aircraft, have been identified on drones operating over Gaza.[30] France approved record-high export licenses in the ML5 and ML15 categories for targeting and imaging technology in 2024, even as diplomatic statements expressed concern over civilian casualties.[31] This industrial support constitutes a material contribution to genocide: French engineering is not adjacent to automated target acquisition; it is a functioning component of it.

The German Industrial Backbone

Germany occupies a singular position in this network. It is the EU's largest exporter of military and dual-use technology to Israel, with annual electronics and information technology (IT) exports alone exceeding US$870 million.[32] Three German-headquartered companies in the registry show distinct modes of involvement that persist despite Berlin's stated commitment to international humanitarian law.

SAP SE serves as a key digital backbone of the Israeli Ministry of Defense (IMoD). The company's S/4HANA Defense and Security platform manages the IDF's logistics, supply chain, munitions tracking, and personnel administration. Since October 2023, SAP has accelerated the transition of these systems from legacy on-premise infrastructure to a sovereign

23 Ariane Lavrilleux and Elie Guckert, "Arms sales: Delivery of French equipment to Israel imminent", Disclose, 25 October 2025, available at https://disclose.ngo/en/article/arms-sales-delivery-of-french-equipment-in-israel-imminent (Disclose, "Arms sales").

24 Disclose, "Arms sales".

25 Disclose, "Arms sales".

26 Disclose, "Arms sales".

27 GRIP, Military and industrial ties between the European Union and Israel: A mapping of the arms trade and defense cooperation in the context of the Gaza conflict, April 2025, available at https://www.grip.org/wp-content/uploads/2025/04/EC-2025-02-05-25-MI-IA-Israel-Gaza-version-finale-EN.pdf.

28 Disclose, "Arms sales".

29 European Security & Defence, "The Heron UAV's impact on 'Operation Iron Swords'", 14 February 2024, available at https://euro-sd.com/2024/02/sponsored-content/36269/heron-uav-impact-iron-swords/.

30 L'Humanité, "Safran, Thales, STMicroelectronics… Les syndicats dénoncent la complicité de l'industrie française d'armement dans le génocide à Gaza", 19 June 2024, available at https://www.humanite.fr/social-et-economie/armement/safran-thales-stmicroelectronics-les-syndicats-denoncent-la-complicite-de-lindustrie-francaise-darmement-dans-le-genocide-a-gaza.

31 Middle East Eye, "Israeli orders for French arms experienced 'a record year' in 2024", 5 September 2025, available at https://www.middleeasteye.net/news/israeli-orders-french-arms-experienced-record-year-2024.

32 Tamsin Paternoster and Christoph Debets, "German arms exports to Israel increase, contradicting government reports", Euronews, 24 October 2024, available at https://www.euronews.com/my-europe/2024/10/24/german-arms-exports-to-israel-increase-despite-export-ban-rumours; Isabel Schlerkmann and Jan-Phillip Graf, "The Other Side of Trade: German Dual-Use Exports to Israel", Verfassungsblog, 12 December 2024, available at https://verfassungsblog.de/the-other-side-of-trade/.

cloud framework, providing the Israeli military with high-speed AI processing capacity for real-time operational planning.[33] SAP acts as a Tier-1 strategic contractor, with its German enterprise AI embedded directly into the IDF's command structure through local partners such as Malam Team, an Israeli IT firm and official Ministry of Defense supplier.[34]

This is enablement at its most embedded: SAP's software does not fire weapons, but it manages the supply chain that ensures those weapons are always available. By forecasting munition consumption rates and automating the replenishment of fuel and shells, SAP's platform maintains the operational tempo that sustains the bombardment. The company also issued between US$4 million and US$7 million (around €3.4-6 million) in internal "war grants" to approximately 1,000 Israeli employees to ensure operational capacity and business continuity during the active bombardment phase.[35]

Hensoldt, a German electronics and defense firm, in which the German federal government and Leonardo, the Italian defense group, each hold a 25.1% blocking minority stake, operates as a strategic arm of German national security policy.[36] The company specializes in radar technology, electronic warfare, and AI-driven sensor fusion. In 2023 and 2024, Germany approved a massive increase in defense exports to Israel.[37] While exports classified as "war weapons" saw temporary pauses, electronic sensor suites, which constitute Hensoldt's core business, were reclassified as "other military equipment." In fact, Germany testified before the International Court of Justice that 98% of the licenses granted since October 2023 fell into this "other" category, a distinction that allowed German exports to remain at record levels throughout the war.[38] Hensoldt provides the Active Electronically Scanned Array (AESA) radars and AI sensor suites used for identifying and tracking low-altitude targets, including drones, over Gaza.[39] This represents both material and financial involvement: the components are physically integrated into targeting infrastructure, and the company benefits from EDF grants to develop the next generation of these systems.

Rohde & Schwarz, a privately held German firm specializing in electronic monitoring and signals intelligence, completes the German cluster. While specific arms contracts remain undisclosed, the company's equipment is widely integrated into Israeli defense frameworks through channels facilitated by the European Leadership Network (ELNET) and its Security and Defense Initiative.[40] In late 2025, Rohde & Schwarz's Israeli subsidiary launched the ARDRONIS Effect, an AI-powered communications jammer designed specifically for the Israeli market.[41] The company described

33 Israel Defense, "SAP AG and IDF Sign $10M Deal", 20 February 2015, available at https://www.israeldefense.co.il/en/node/20206.

34 Who Profits, "Malam Team", available at https://www.whoprofits.org/companies/company/4217, accessed 24 August 2026.

35 Globes, "SAP provides war grants to Israeli employees in combat zones", 1 November 2023, available at https://en.globes.co.il/en/article-sap-provides-war-grants-to-israeli-employees-in-combat-zones-1001461536.

36 Leonardo, "Leonardo acquires 25.1% of HENSOLDT AG for approx. 606 million euros", 24 April 2021, available at https://www.leonardo.com/en/press-release-detail/-/detail/24-04-2021-leonardo-acquista-il-25-1-percento-di-hensoldt-ag-per-ca.-606-milioni-di-euro, accessed 17 January 2026.

37 Forensic Architecture, "German Arms Exports to Israel: A Detailed Investigation", 2024, available at https://forensic-architecture.org/investigation/german-arms-exports-to-israel-supported, accessed 17 January 2026.

38 Adil Ahmad Haque, "The Fall and Rise of German Arms Exports to Israel: Questions for the International Court of Justice", Just Security, 13 June 2025, available at https://www.justsecurity.org/114479/german-arms-exports-israel-icj/.

39 Facing Finance, "Rheinmetall und Co: Unregulierte Expansion und Autonomie", 23 May 2024, available at https://www.facing-finance.org/2024/05/rheinmetall-und-co-unregulierte-expansion-und-autonomie/ (Facing Finance, "Unregulierte Expansion"); Hensoldt, "PrecISR: Airborne multi-mission radar family", available at https://www.hensoldt.net/products/precisr-airborne-multi-mission-radar-family, accessed 24 August 2026.

40 ELNET, "Launch of ESDI – ELNET Security & Defense Initiative", 11 July 2024, available at https://elnetwork.eu/country/israel/launch-esdi-elnet-security-defense-ini/.

41 Rohde & Schwarz, "Mitigating emerging and future threats: Rohde & Schwarz unveils next-generation multi-band jammer for counter-drone missions", 3 April 2025, available at https://www.rohde-schwarz.com/us/about/news-press/all-news/mitigating-emerging-and-future-threats-rohde-schwarz-unveils-next-generation-multi-band-jammer-for-counter-drone-missions-press-release-detailpage_229356-1552768.html.

it as "field-proven" in the dense urban areas of Gaza.[42] The European Centre for Constitutional and Human Rights filed a legal action in November 2025 challenging the legality of German arms exports to Israel, arguing that the continued flow of military technology during documented atrocities violates the EU Common Position on Arms Exports.[43] The German case demonstrates that, even where the political will to restrict exports nominally exists, the industrial and regulatory architecture is designed to maintain the flow.[44]

Subsidizing the Military Operations in Gaza Through Research and Development Funding

The EU's role has shifted from passive oversight to the active facilitation of the technologies currently deployed in Gaza. The EDF and Horizon Europe have become key mechanisms for this institutional crisis. Findings from the UN Special Rapporteur's report identify this systemic failure as the result of a fundamental global governance gap that grants corporate entities immense power without justiciable accountability. This gap fosters an asymmetry in which military campaigns, including those causing genocide, are treated as ordinary economic activity, shielded by the absence of state-level oversight. Israeli military firms and their European partners exploit this lack of regulation through a complex web of parent companies and subsidiaries to obscure their involvement in atrocity crimes. This intentional complexity allows firms to bypass domestic export restrictions and maintain a steady flow of public funding through EU research grants.[45]

This dynamic is not limited to a single grant. Annex II documents nine separate EU-funded R&D projects, spanning the EDF and Horizon Europe, through which European institutions channeled research funding to Israeli defense, intelligence, and drone entities between 2021 and 2026, with a combined traced value of over €148 million (around US$ 172 million).

The Israeli company Xtend provides a clear illustration of this governance gap, having received a €50,000 (around US$58,000) Horizon Europe grant to optimize its Skylord drone system.[46] While the EU awarded this funding for a civilian feasibility study on drone navigation, the reality on the ground is different. The IDF now openly uses thousands of these Skylord drones for urban warfare missions and close-quarters combat in Gaza.[47] Xtend's €50,000 (around US$58,000) grant is a small sum, but it is illustrative of a much larger pattern: IAI itself, the state-owned parent of Intracom Defense, separately participates in eight Horizon Europe projects that have received over €92 million (around US$ 107 million) in EU funding to date.[48]

This R&D loop is anchored by Europe's own defense giants, companies that dominate EU funding while simultaneously supplying the Israeli military's heaviest hardware. Leonardo ranks as the second-largest recipient of EDF grants at

42 Digit, "Israel and US companies are using Gaza as a tech test lab for AI – Germany may soon benefit", 24 July 2025, available at https://digit.site36.net/2025/07/24/israel-and-us-companies-are-using-gaza-as-a-tech-test-lab-for-ai-germany-may-soon-benefit/.

43 ECCHR, "No German weapons to Israel", available at https://www.ecchr.eu/en/case/no-german-weapons-to-israel/, accessed 24 August 2026.

44 NPR, "Germany bans its military exports for Israel to use in Gaza", 8 August 2025, available at https://www.npr.org/2025/08/08/nx-s1-5496240/germany-israel-gaza-military-exports-weapons.

45 Albanese, "From Economy of Occupation to Economy of Genocide".

46 Euronews, "EU funding drone technology used by Israel in Gaza war, claims monitor", 23 March 2024, available at https://www.euronews.com/2024/03/23/eu-funding-drone-technology-used-by-israel-in-gaza-war-claims-monitor.

47 Al Mayadeen, "How EU funding continues to support Israeli military technology", 25 March 2024, available at https://english.almayadeen.net/news/Economy/how-eu-funding-continues-to-support-israeli-military-technol.

48 European Parliament, "Parliamentary question: On EU funding to Israel Aerospace Industries, Israel's main defence supplier", E-002908/2024, available at https://www.europarl.europa.eu/doceo/document/E-10-2024-002908_EN.html, accessed 21 August 2026.

€114 million (around US$132 million) and is a strategic partner in projects such as TIRESYAS, which develops the next generation of AI-driven radar using AI algorithms for automated target tracking.[49] Leonardo receives millions from the EU to engineer the future of "autonomous defense." At the same time, the company continues to supply structural components for the combat aircraft and weapons platforms used in Gaza.[50] Workers at Leonardo's Italian manufacturing plants have publicly documented these production lines, and a 2025 petition by arms workers at the company's facilities demanded an end to all contracts and collaboration with Israel.[51] The company's dual role, collecting EU research grants while supplying parts of the airframes that deliver ordnance onto Gaza's residential blocks, collapses the distinction between civilian innovation and military application.

The industrial ties extend beyond R&D into the physical machinery of ground operations. The Eitan Armored Personnel Carrier, deployed extensively during the 2024 and 2025 raids in the West Bank and Gaza, is powered by engines from Rolls-Royce Solutions, a German-headquartered subsidiary of the British Rolls-Royce Holdings plc. In April 2025, a new US$180 million contract (around €155 million) was approved for these engines.[52] European engineering is directly supporting Israeli ground invasions. Physical hardware such as these engines is not developed in isolation from Europe's broader R&D ecosystem. RADA Electronic Industries, an Israeli radar company whose radar technology underpins the Eitan's Iron Fist protection system, was acquired in 2022 by Leonardo DRS, folding it into the same Leonardo group that leads TIRESYAS, an EU-funded project explicitly developing AI-driven radar systems.[53] The financial architecture is circular, wherein EU grants subsidize the research that improves the sensors, while industrial contracts supply the vehicles on which those sensors are mounted. The result is a European-funded ecosystem in which R&D and manufacturing reinforce each other in service of the same military operations.

The most structurally damning element of this ecosystem is the role of Frontex, the EU's own border agency. Frontex has awarded contracts worth over €100 million (around US$116 million) to companies such as Elbit Systems and IAI for maritime surveillance used to detect migrant and refugee boats along the Mediterranean,[54] intelligence that Frontex funneled to Libyan and Tunisian forces for interception rather than systematically alerting nearby rescue vessels.[55] The commercial logic that connects these facts is the business model itself. Israeli defense firms explicitly market their products to European buyers as "combat-proven" and "field-tested," language that refers directly to their deployment against Palestinian civilians. Elbit Systems' marketing materials for the Hermes 900 drone, for instance, emphasize its operational record in Gaza as a credential for European procurement.[56] The cycle operates as

49 Science Business, "Thales, Leonardo, Airbus lead rankings for European Defence Fund grants, Science Business finds", 30 April 2024, available at https://sciencebusiness.net/news/fnw/thales-leonardo-airbus-lead-rankings-european-defence-fund-grants-sciencebusiness-finds.

50 AFSC Investigate, "Leonardo SpA: Company Profile", available at https://investigate.info/company/leonardo, accessed 24 August 2026.

51 New Internationalist, "Italian arms factory workers say no to war", 12 March 2026, available at https://newint.org/arms/2026/italian-arms-factory-workers-say-no-war.

52 Who Profits, "Rolls-Royce Holdings", available at https://www.whoprofits.org/companies/company/7397?rolls-royce, accessed 24 August 2026 (Who Profits, "Rolls-Royce").

53 Leonardo DRS, "Leonardo DRS and RADA Agree to All-Stock Merger", 21 June 2022, available at https://www.leonardodrs.com/news/press-releases/leonardo-drs-and-rada-agree-to-all-stock-merger-combining-top-defense-technology-companies-into-leader-in-advanced-sensing-and-force-protection/; European Union, "TIRESYAS – Defence Industry and Space", European Commission, available at https://defence-industry-space.ec.europa.eu/system/files/2023-06/TIRESYAS%20-%20Factsheet_EDF22.pdf.

54 Statewatch, "Border surveillance, drones and militarisation of the Mediterranean", 17 May 2021, available at https://www.statewatch.org/analyses/2021/border-surveillance-drones-and-militarisation-of-the-mediterranean/.

55 Human Rights Watch, "Frontex: Act to Save Lives at Sea", 24 October 2024, available at https://www.hrw.org/news/2024/10/24/frontex-act-save-lives-sea.

56 Business & Human Rights Resource Centre, "Frontex's contracted companies reportedly operating surveillance equipment to monitor migrants & refugees crossing the Mediterranean utilized by the Israeli military in its assaults on Gaza, incl. co. responses", 20 March 2024, available at https://www.business-humanrights.org/en/latest-news/frontexs-contracted-companies-reportedly-operating-surveillance-equipment-to-monitor-migrants--refugees-crossing-the-mediterranean-utilized-by-the-israeli-military-in-its-assaults-on-gaza-incl-co-responses/.

follows: EU research grants fund the development of surveillance and targeting technology. That technology is deployed in Gaza, where it is used against a civilian population under conditions that multiple UN bodies have characterized as genocidal. The resulting operational data and combat record are then packaged as selling points to win further EU contracts for border surveillance, critical infrastructure protection, and maritime monitoring.

European Soil as the Digital Architecture of AI Warfare

Over 11,500 terabytes of Israeli military data have been processed through data centers located in Ireland, Germany, and the Netherlands.[57] Microsoft's Azure cloud infrastructure alone has handled approximately one million intercepted Palestinian phone calls per hour on behalf of the Israeli military.[58] These figures constitute the digital substrate upon which the AI-powered targeting systems described in this paper operate. The algorithms that select human targets in Gaza require immense computational power. That power sits in significant parts on European soil.

The backbone of this digital architecture is Project Nimbus, a US$1.2 billion (around €1 billion) contract between the Israeli government and two American technology giants, Google and Amazon.[59] While the contract was signed between Israeli and American entities, the physical infrastructure that executes it is distributed in large parts across European territory. Amazon Web Services operates major data center clusters in Dublin, Frankfurt, and Amsterdam. Google Cloud maintains equivalent facilities in the same cities. Microsoft Azure, which provides additional cloud capacity to the Israeli military, hosts its European operations primarily through hubs in Ireland and the Netherlands.[60] [61] [62] These facilities provide the high-frequency compute power required to process surveillance feeds in real time, run pattern-recognition algorithms against intercepted communications, and generate the targeting recommendations that precede airstrikes.

Leaked internal documents and investigative reporting have revealed the scale of what these servers process. The Israeli military utilized "near-limitless" storage in Ireland and the Netherlands to maintain a massive repository of intercepted Palestinian communications.[63] The Rolling Stone surveillance system, which tracks Palestinian movements across Gaza in real time, operates through the same cloud architecture.[64] In October 2025, *The Guardian* reported that Israel had pressured Google and Amazon to use a secret coded system referred to internally as a "wink" to sidestep legal orders that might have restricted data processing in European jurisdictions.[65]

This infrastructure directly enables the AI systems documented throughout this paper. The Lavender algorithm, which has generated tens of thousands of targeting recommendations in Gaza, processes vast quantities of surveillance data to identify individuals for assassination. The Gospel system automates target selection for airstrikes on buildings and infrastructure. Where's Daddy? monitors individuals until they return to their family homes before authorizing a strike. Each of these systems depends on cloud computing capacity that far exceeds what domestic Israeli infrastructure can provide. Project Nimbus was designed precisely to

57 Harry Davies, "Activists in Netherlands protest on roof of Microsoft site storing Israeli military data", *The Guardian*, 10 August 2025, available at https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data (Davies, "Activists in Netherlands").

58 Harry Davies and Yuval Abraham, "A million calls an hour: Israel relying on Microsoft cloud for expansive surveillance of Palestinians", The Guardian, 6 August 2025, available at https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud.

59 Yuval Abraham, "'No restrictions' and a secret 'wink': Inside Israel's deal with Google, Amazon", +972 Magazine, 29 October 2025, available at https://www.972mag.com/project-nimbus-contract-google-amazon-israel/ (Abraham, "No restrictions and a secret wink"); Noa Yachot, "'Data is control': what we learned from a year investigating the Israeli military's ties to big tech", The Guardian, 30 December 2025, available at https://www.theguardian.com/world/2025/dec/30/israeli-military-big-tech.

60 Davies and Abraham, "A million calls an hour".

61 Lisa O'Carroll, "Irish authorities asked to investigate Microsoft over alleged unlawful data processing by IDF", The Guardian, 4 December 2025, available at https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf (O'Carroll, "Irish authorities").

62 O'Carroll, "Irish authorities".

63 Davies and Abraham, "A million calls an hour".

64 Abraham, "No restrictions and a secret wink".

65 O'Carroll, "Irish authorities".

fill this gap by leveraging the high-density server clusters hosted on European soil.

This arrangement exposes a fundamental contradiction at the heart of European technology regulation. The 2025 EU AI Act prohibits AI practices involving unacceptable risk, including predictive policing and mass biometric surveillance.[66] However, the Act contains a broad national security exemption that excludes AI systems developed or used exclusively for military purposes from its scope.[67] The result is a legal architecture that bans these technologies when deployed against European citizens but permits European infrastructure to host the identical practices when the targets are Palestinian. A continent that regulates facial recognition in its shopping centers provides the server capacity for a system that identifies Palestinians for execution in their homes.

The General Data Protection Regulation (GDPR) compounds this contradiction. The interception and processing of communications from an entire civilian population (millions of Palestinians, whose calls, messages, and movements are swept into European-hosted databases) raises fundamental questions about lawfulness, purpose limitation, and data minimization under Articles 5 and 6 of the GDPR.[68] In December 2025, the Irish Council for Civil Liberties (ICCL) lodged a formal complaint with Ireland's Data Protection Commission, demanding an investigation into whether Microsoft's Irish data centers had unlawfully processed surveillance data on behalf of the Israeli military.[69] Activists in the Netherlands staged a rooftop protest at a Microsoft data center in Eemshaven in August 2025, drawing public attention to the same issue.[70]

Under the framework of contribution to genocide adopted in this paper, the hosting of military targeting infrastructure on European soil constitutes enablement in its most direct form. These data centers do not manufacture weapons. They do not fire missiles. But without the computational power they provide, the AI systems that automate the identification, tracking, and killing of Palestinians would be nearly useless. Europe's role in this chain is architectural.

The Failure of Legal Standards and Corporate Responsibility Mandates

The support network described in this research carries severe ramifications under international humanitarian law. These laws establish the minimum standards of humane conduct during armed conflict and prohibit the targeting of civilians or the use of disproportionate force.

International law imposes direct obligations on both states and corporate actors operating within their jurisdiction. Common Article 1 to the four Geneva Conventions of 1949 obliges all High Contracting Parties not only to respect the Conventions themselves, but "to ensure respect" for them "in all circumstances."[71] The ICRC's Updated Commentary interprets this obligation as extending to third states' dealings with private actors under their jurisdiction: where a state has knowledge, or should have knowledge, that arms, technology, or services transferred from its territory carry a clear risk of contributing to violations of IHL, it must take feasible measures to prevent that outcome.[72] The continued licensing of AI-enabled targeting components to a party credibly alleged to be committing serious violations of IHL — and, per the International Court of Justice's provisional measures order, facing a plausible risk of genocide — places the European states hosting this research

66 European Union, "Artificial Intelligence Act, Article 5: Prohibited AI Practices", available at https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng, accessed 24 August 2026.

67 European Union, "Artificial Intelligence Act, Article 5: ProhibiEuropean Union, "Artificial Intelligence Act, Recital 24", AI Act Service Desk, European Commission, available at https://ai-act-service-desk.ec.europa.eu/en/ai-act/recital-24, accessed 24 August 2026.

68 General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, accessed 24 August 2026.

69 O'Carroll, "Irish authorities".

70 Davies, "Activists in Netherlands".

71 Article 1 (common to all four 1949 Geneva Conventions).

72 International Committee of the Red Cross (ICRC), Commentary on the First Geneva Convention, 2016, Article 1, available at https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-1/commentary/2016.

and industrial cooperation squarely within the scope of this obligation.[73]

Corporate actors, including individual corporate leaders, can also bear responsibility under international law. Article 25(3)(c) of the Rome Statute establishes individual criminal responsibility for any person who, "for the purpose of facilitating the commission" of a crime within the Court's jurisdiction, "aids, abets or otherwise assists in its commission."[74] Tribunal jurisprudence has clarified that this standard does not require the aider to share the principal perpetrator's genocidal or persecutory intent; knowledge that one's assistance has a substantial effect on the commission of the crime is sufficient.[75] This is not a novel theory. It is the same legal architecture that, at Nuremberg, convicted the directors of IG Farben for knowingly supplying material used in the extermination of concentration camp prisoners — establishing that corporate officials cannot outsource legal responsibility to the state actors who carry out the killing.[76]

Contemporary courts have shown renewed willingness to apply this doctrine to corporations operating in today's conflict economies. In April 2026, a Paris court convicted Lafarge and four former executives on the related charge of financing terrorism, for precisely this kind of knowing, profit-driven engagement with an actor it knew to be committing atrocities.[77]

European firms move from neutral suppliers to technical facilitators when they provide the specialized AI technology that helps power Israel's genocidal campaign. This hardware includes high-resolution sensors for drones and the data processing units that run targeting algorithms such as Lavender and The Gospel.[78] These digital tools facilitate grave human rights violations by automating the selection of targets and creating a permanent infrastructure for mass surveillance, where every movement is tracked in real time.

Under the UN Guiding Principles on Business and Human Rights (UNGPs), companies have a clear mandate to respect these international standards.[79] Specifically, Guiding Principle 17 requires these enterprises to carry out human rights due diligence to identify and mitigate their adverse impacts. In situations of active armed conflict and genocide, international standards demand a heightened human-rights-due-diligence process.[80] This rigorous assessment requires companies to identify how their AI-enabled products might be used to automate killings or conduct mass surveillance in direct violation of IHL. Guiding Principle 13 further clarifies that businesses must seek to prevent adverse impacts directly linked to their operations, products, or services through their business relationships. Their continued supply of these digital tools during an active genocide investigation constitutes a total failure of this ethical and operational mandate.

The digital infrastructure documented in the preceding section deepens this legal exposure. Companies that host military targeting data on European servers cannot claim ignorance of its end use when investigative reporting has publicly documented the nature of these operations. The heightened due diligence standard required by the United Nations Guiding Principles on Business and Human Rights (UNGPs) in conflict situations applies

73 International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel)*, Order on Provisional Measures, 26 January 2024, available at https://www.icj-cij.org/case/192.

74 Rome Statute of the International Criminal Court, 17 July 1998, Article 25(3)(c), available at https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf.

75 Prosecutor v. Furundžija, Case No. IT-95-17/1-T, Trial Chamber Judgment, 10 December 1998, paras 235, 249, International Criminal Tribunal for the former Yugoslavia.

76 United States v. Carl Krauch et al. (The IG Farben Case), in *Trials of War Criminals Before the Nuernberg Military Tribunals*, Vol. VIII (Washington, DC: US Government Printing Office, 1948).

77 European Center for Constitutional and Human Rights (ECCHR), "Lafarge in Syria: Complicity in human rights violations?", case update, available at https://www.ecchr.eu/en/case/lafarge-in-syria-accusations-of-complicity-in-grave-human-rights-violations/, accessed 24 August 2026.

78 Abraham, "'Lavender': The AI machine".

79 Office of the High Commissioner for Human Rights (OHCHR), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011, available at https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

80 Institute for Human Rights and Business (IHRB), "Businesses Must Respond to Human Rights Abuses in Gaza and Beyond", 11 April 2024, available at https://www.ihrb.org/latest/businesses-must-respond-to-human-rights-abuses-in-gaza-and-beyond (IHRB, "Businesses Must Respond").

with equal force to cloud service providers whose infrastructure processes surveillance data and targeting algorithms. Enabling contribution through digital infrastructure is no less consequential than the material supply of physical weapons components.

Industrial cooperation also exposes a collapse of the EU Common Position on Arms Exports (2008/944/CFSP).[81] This legally binding treaty mandates that member states deny export licenses if there is a "clear risk" that the military technology might be used to commit serious violations of IHL. Nations such as Spain and Italy have claimed to implement "pauses" on exports.[82] The persistent use of the dual-use R&D loophole still allows components and software to flow uninterrupted. The exemption granted for the SIRTAP drone in early 2026 suggests that member states are treating these legal instruments as optional. This represents a structural failure of the European legal framework designed to prevent contribution to international crimes.

The EU–Israel Association Agreement, which governs the broader framework of trade and cooperation between the two parties, contains an essential elements clause under Article 2 that conditions the entire relationship on respect for human rights and democratic principles. The European Parliament has repeatedly called for a review of this agreement in light of the situation in Gaza, and the European Commission initiated a formal review process in 2025.[83] This clause provides the most direct legal mechanism available to EU institutions to suspend the research funding and industrial cooperation documented in this paper.

81 IHRB, "Businesses Must Respond".

82 Anadolu Agency, "Italy's suspension of arms exports to Israel consistent with its constitution, obligations: Expert", 15 July 2024, available at https://www.aa.com.tr/en/europe/italys-suspension-of-arms-exports-to-israel-consistent-with-its-constitution-obligations-expert/3603548; Al Jazeera, "Spain's parliament formally approves Israel arms embargo", 8 October 2025, available at https://www.aljazeera.com/news/2025/10/8/spains-parliament-formally-approves-israel-arms-embargo.

83 European Parliament Research Service, "Review of the EU-Israel Association Agreement", 12 June 2025, available at https://epthinktank.eu/2025/06/12/review-of-the-eu-israel-association-agreement/; European Commission, "COM(2025) 890 final: Proposal for partial suspension of the EU-Israel Association Agreement", available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0890, accessed 17 January 2026.

Recommendations

For EU and national policymakers

- The European Commission must complete the Article 2 review of the EU–Israel Association Agreement and proceed to suspension. The review has already found indications of breach. Suspension provides the legal basis to terminate Horizon Europe participation, EDF grants, and cloud infrastructure agreements.
- National governments must audit all military data hosted on European cloud infrastructure and suspend processing agreements linked to operations under active International Court of Justice review.
- The EU must terminate all Horizon Europe and EDF grants to entities involved in the occupying power's military-industrial complex, including subsidiaries using European corporate structures to access funding.
- Member states should adopt the Spanish model: prohibit the export, transit, and import of all weapons, software licenses, and dual-use components regardless of when contracts were signed.

For companies

- Publish a transparent registry of every end-user certificate issued for high-risk technology and AI software. This paper's registry provides the baseline. Companies must now produce documentation to refute or confirm the linkages identified here.
- Cease all partnerships and joint ventures with Israeli defense firms immediately. Maintaining business relations with entities such as Elbit Systems or IAI constitutes a knowing and material contribution to an unlawful military occupation and the machinery of genocide under current UN findings.
- Undertake heightened human rights due diligence for all AI and dual-use exports. Failure to identify how technology enables civilian targeting constitutes a breach of the corporate responsibility to respect human rights.
- Where risk of contribution cannot be managed,

terminate operations entirely. Under UN Guiding Principle 23, the threshold has been met.

Conclusion

On 20 March 2025, an Israeli airstrike hit the Abu Dagga family home in Abasan al-Kabira, near Khan Younis, while they gathered on a Ramadan night. At least 16 people were killed, mostly women and children. A father and his seven children died alongside them. Only a 25-day-old baby, Ella, survived, pulled from the rubble by first responders who followed her cries.[84] The operational pattern matches what investigative reporting has documented, in which AI systems such as Lavender generate tens of thousands of targeting recommendations, and the "Where's Daddy?" protocol delays strikes until individuals return to their family homes at night, when entire multi-generational families are gathered under one roof.[85] The drone that carried out such a strike relies on sensors and stabilization systems with European-made components. The AI that processes the targeting data runs on cloud infrastructure hosted in European data centers. The EU research grants that helped develop the underlying technology are documented in the annexes of this paper.

European governments and the corporations listed in this report did not stumble into their facilitation of genocide. European institutions funded the research; the companies documented in this paper supplied the components, funded the research, and hosted the servers that help sustain the automated killing of Palestinians in Gaza.

This paper has traced that machinery from EU grant portals in Brussels, through corporate subsidiaries in Athens, Madrid, Paris, and Berlin, to the targeting systems operating over Gaza. Twenty-four companies across eight countries, nine EU-funded projects, and over €148 million (around US$172 million) in traced funding connect European institutions to the infrastructure of this violence.

The registry produced by this research consolidates these fragmented data streams into a single tool that classifies each entity by the nature of its involvement, whether material, financial, or enabling, and links EU funding to operational deployment through a unified evidentiary framework. Litigators can use it to establish corporate liability chains. Parliamentary committees can use it to audit the export licenses and research grants that sustain these relationships. Divestment campaigns can use it to identify and prioritize targets.

With the evidence assembled in this paper, the question is no longer whether Europe is implicated, but whether it will act to sever these ties or continue to serve as the structural engine of a documented genocide in Gaza.

84 Associated Press, "Month-old girl pulled from rubble in Gaza after airstrike killed her parents", 20 March 2025, available at https://www.pbs.org/newshour/world/month-old-girl-pulled-from-rubble-in-gaza-after-airstrike-killed-her-parents.

85 Abraham, "'Lavender': The AI machine"; Office of the High Commissioner for Human Rights (OHCHR), "Israel has committed genocide in the Gaza Strip, UN Commission finds", 18 September 2025, available at https://www.ohchr.org/en/press-releases/2025/09/israel-has-committed-genocide-gaza-strip-un-commission-finds.

Annex I: Registry of Contribution to Genocide

This registry provides a non-exhaustive mapping of European-, Israeli-, and US-headquartered companies whose hardware, software, cloud infrastructure, and technical components are integrated into the military operations in Gaza through European-funded research, joint ventures, procurement contracts, or the hosting of military data on European soil.

How to use this registry: Each entity is classified by contribution type (Material, Financial, Enabling, or a combination) and by evidentiary status, indicating whether the link is confirmed through corporate disclosure, investigative journalism, EU grant records, or circumstantial inference based on technical capability matching. Litigators pursuing corporate accountability can filter by contribution type to establish liability chains. Parliamentary committees can cross-reference the funding sources and evidentiary status to audit export licenses and research grants. Divestment campaigns can prioritize targets based on the directness and level of documentation of each company's contribution.

Contribution type key: **Material** = supply of physical components for weapons platforms. **Financial** = receipt of R&D subsidies or public grants sustaining military-linked operations. **Enabling** = provision of essential dual-use services (cloud infrastructure, software licensing, data processing). **Multiple** = operates across all three categories.

Company	Country	Sector	Operational Status and Identity	Primary Funding Source	Estimated Amount (2023–2026)	Context of Funding	Military Contract and Gaza Impact	Contribution Type	Evidentiary Status
1. Intracom Defense	Greece	AI / Drones	Israeli-owned: 95%, lead on ACTUS program.	EDF	€14 million+	Awarded for 15 defense projects (ACTUS, Triton) post-IAI purchase. Lead coordinator for ACTUS.	Backdoor for IAI state drones into the EU; AI tracking system ACTUS used in Gaza operations.	Financial / Enabling	Corporate disclosure (IAI acquisition) / EU grant records / Investigate Europe
2. Thales Group	France	Aerospace / AI	State-linked, major IMoD partner for decades.	Horizon Europe / National Contracts	€1 billion+	Involved in dozens of Horizon Europe projects. France approved hundreds of millions in dual-use export licenses.	AI-integrated sensors and transponders used in unmanned aerial vehicle (UAV) fleets deployed in Gaza	Material / Financial	Investigative journalism (Disclose) / Export license records / Corporate filings
3. OIP Sensor Systems	Belgium	Electro-Optics	Wholly owned by Elbit Systems. Primary manufacturing hub in Western Europe.	Corporate Revenue (Elbit Systems)	Part of US$6.8 billion (Elbit Total)	Funnels EU sales back to Elbit Systems parent company, which saw a 27% revenue spike in 2024.	Thermal imaging and AI-ready optronics used for automated target identification in Gaza.	Material	Corporate disclosure (Elbit Systems subsidiary) / AFSC Investigate / Who Profits

4. Leonardo S.p.A.	Italy	Defense & AI	30% owned by Italian government. Vast subsidiary network in UK and US.	National export licenses stumble	US$3 billion	Despite a partial embargo, Italy continued honoring pre-existing high-tech contracts for naval and air components.	Components for combat aircraft and naval artillery used in Gaza. Named in the UN Special Rapporteur report.	Material / Financial	UN Special Rapporteur (A/HRC/59/23) / AFSC Investigate / Leonardo workers' petition / Civil society lawsuit
5. BATS	Belgium	Radar / AI	Fully owned by ELTA / IAI Specializes in "smart border" technologies, coastal surveillance.	EDF	€42 million	Lead partner in the ACTUS project (AI-driven armed drones) funded by the EDF.	IAI's CEO stated systems are heavily employed in Gaza. BATS "Europeanizes" IAI technology for EU funding.	Financial / Enabling	Corporate disclosure (IAI / ELTA ownership) / EDF grant records / IAI public statements
6. SAP SE	Germany	Software / AI	Primary "digital backbone" for IMoD. S/4HANA Defense & Security platform.	Funded via the IMoD Digital Transformation budget. Tier-1 strategic contractor	US$25 million–US$45 million Estimated	Core component of Germany's US$870 million+ annual electronics and IT exports to Israel. Issued US$4 million–US$7 million in war grants to Israeli staff.	AI-powered predictive analytics manage the IDF supply chain. Forecast munition burn rates and automate replenishment.	Enabling	Corporate disclosure (SAP-IDF contract) / Globes / Times of Israel / Verfassungsblog
7. Hensoldt	Germany	Electronics	25.1% owned by German government, 25.1% Leonardo. Strategic arm of German national security policy.	Export Licenses / EDF	€85 million–€120 million Projected	Electronic sensor suites reclassified as "other military equipment," allowing record exports during the war.	Active Electronically Scanned Array (AESA) radars and AI sensor suites used for identifying and tracking low-altitude targets and drones.	Material / Financial	German export license data (Bundestag disclosures) / Forensic Architecture report / Euronews
8. Aimpoint AB	Sweden	Optics	Private manufacturer.	National Export Licenses / Private Sales	€1.5 million (EU innovation grant)	Swedish export data showed a 61% spike in optical and technical equipment to Israel in 2024.	Red Dot sights (CompM5/M4) documented in use by IDF ground forces in Gaza.	Material	Swedish export records / AFSC Investigate / Field documentation

9. Airbus Defense and Space	Germany / Spain / France	Aerospace / AI	Publicly traded with major government shares. Operates across multiple EU jurisdictions.	EU Research / Exports	€300 million+ (Cumulative EU grants)	Lead partner for the SIRTAP drone. Co-developed with IAI technology under essential security exemptions.	AI-assisted satellite imagery and components for the Heron TP drone used in Gaza.	Material / Financial	Reuters / Jerusalem Post / EU grant records / Spanish embargo exemption documentation
10. Cellebrite	Israel / EU operations	Digital intelligence	Headquartered in Israel, major EU offices. Classifies tools as "civilian services." Supplies 25 of 27 EU states.	EU Service Contracts / Law Enforcement Procurement	US$11 million IMoD contracts (2016–2025)	European funds indirectly sustain R&D deployed in combat zones.	AI-powered Universal Forensic Extraction Device tools used to extract data from devices seized from Palestinians arrested in Gaza for intelligence gathering.	Enabling	AFSC Investigate / Corporate filings / Investigative journalism
11. Hexagon AB	Sweden	Geospatial Intelligence	Parent of Leica Geosystems. High-precision 3D modeling and situational awareness.	Horizon Europe / Horizon 2020 / Public Equity	€12 million+ (Cumulative EU)	EU grants facilitate high-resolution 3D data management classified as civilian research.	Leica scanners and Luciad software form the foundation for Unit 9900 tunnel mapping and the Gospel AI targeting system.	Enabling	EU grant records / Investigative journalism / Circumstantial inference (technical capability match)
12. Rohde & Schwarz	Germany	Defense electronics	Private, family-owned. Specialized in electronic monitoring and Signals Intelligence (SIGINT).	German Export Licenses / Defense Contracts	Undisclosed (€3.16 billion group revenue 2025)	Facilitated by the European Leadership Network (ELNET) Security and Defense Initiative (ESDI), connecting German firms with the Israeli defense market.	Surveillance technology integrated into Israeli defense frameworks. Launched the ARDRONIS Effect AI jammer for the Israeli market.	Material / Enabling	European Leadership Network (ELNET) Security and Defense Initiative (ESDI) launch records / Rohde & Schwarz press releases / Investigative journalism (digit.site36)

13. Safran	France	Aviation / AI Sensors	French defense leader. Collaborates with Greek and Israeli firms on EU-funded drone research.	National export licenses & EU Grants (EDF)	€27.1 million / €42 million (EU projects)	France approved record licenses for targeting and imaging technology. Coordinates the ACTUS project with IAI-owned Intracom.	Euroflir 410 sensors used for high-precision targeting and classification on surveillance aircraft and drones.	Material / Financial	Investigative journalism (Disclose) / EDF grant records / French export license data
14. Dassault Systèmes	France	Software / Simulation	Engineering software firm.	Institutional Licensing IMoD	Undisclosed	Israeli IMoD Digital Twin revenue.	3DEXPERIENCE software used by IAI and Elbit Systems to design drones and armored vehicles.	Enabling	Circumstantial inference (technical capability match) / Corporate product documentation
15. Elbit Systems	Israel	Defense / AI	Primary IDF supplier: approximately 85% of land equipment and the majority of the tactical drone fleet.	Horizon Europe / EDF / National Tenders	€2.5 million+ (EU); US$2 billion+ (National)	Active in Horizon Europe for civilian security. National contracts focus on field-tested AI suites.	CEO linked profit increases to Gaza operations. Hermes 900 serves as the primary aerial platform and is marketed as combat-proven. Micro-suicide drone swarms were deployed.	Multiple	Corporate disclosure (earnings reports) / Who Profits / EU grant records / Field documentation
16. Xtend	Israel	Drones	"Human-guided autonomous" drones. XOS system allows VR/AR control.	Horizon Europe / IDF Tenders	€50,000 (EU) + multi-million IDF tender	The CEO stated the company redirected all activities to support the IDF 100%.	AI algorithms track people and vehicles in Gaza with high precision.	Material / Financial	Corporate statements (CEO interviews) / EU grant records / Investigative journalism
17. Indra Sistemas	Spain	Defense / Technology	28% state-owned. €206 million profit (2023) driven by Defense & Security division.	Spanish Government / EDF	€1.1 billion+ (Consortium Total)	Leads 70+ EU defense projects. Awarded €24 million for AI infrastructure in Tel Aviv.	Strategic partner for IAI Heron 1 and Heron TP drones used for targeting in Gaza. Collaborates with Elbit Systems on the SILAM rocket program.	Material / Financial	Corporate filings / EU grant records / Investigative journalism (Diario Socialista)

18. Rafael Advanced Defense Systems	Israel	Defense / AI	State-owned. Prime IDF contractor.	Spanish Ministry of Defense / Horizon Europe	€280 million+ (Spanish contracts)	Awarded €442,750 from Horizon Europe (2023). Despite an embargo, Spain continued maintenance contracts.	Producer of Spike missiles and Spice bombs. Litening five targeting pods used by the Israeli Air Force in Gaza.	Material / Financial	Corporate disclosure / EU grant records / Army Recognition / Spanish procurement records
19. Robotican	Israel	Robotics / Drones	Autonomous indoor robotics. Developer of Rooster hybrid drone.	NATO / European Special Forces Contracts	€5 million–€10 million (EU Sales)	Secured a NATO Stock Number in 2024. Sold 50+ robotic systems to NATO armies and Israel.	Rooster drone serves as a primary IDF tool for underground scouting in Gaza. Maps buildings autonomously using AI.	Material	Corporate press releases / EDR Magazine / NATO procurement records
20. SAES	Spain	Underwater Electronics	Jointly owned by Indra (51%) and Navantia (49%). Thales as key tech partner.	EDF / Horizon Europe	€10 million+ (Consortium)	EU defense funding for mine counter-measures and autonomous underwater vehicles.	Sensors used by the Israeli Navy to monitor the Gaza coastline and enforce the naval blockade restricting humanitarian access.	Material / Enabling	EU grant records / Corporate structure filings / Investigative journalism
21. Sermat	France	Aerospace components	Headquartered in Nanterre, France. Specializes in electromechanisms for the aerospace, armament, and space sectors.	National export licenses (components classified as non-military, requiring no export authorization)	€843,300 (documented deliveries over two years)	French authorities have long ignored Sermat's actuators because they are not classified as military or dual-use equipment, requiring no export authorization.	Over two years, Sermat delivered 29 alternators and 171 actuators to Elbit Systems. Alternators are designed for the Hermes 900 and Hermes 450 drones deployed in Gaza strikes. Actuators provide stabilization and precise control for drone surveillance cameras. A further shipment of eight alternators via UPS was scheduled for delivery to Elbit Systems in Karmiel on 20 October 2025.	Material	Investigative journalism (Disclose, October 2025)

22. Amazon Web Services (AWS)	US (EU infrastructure: Ireland, Netherlands, Germany)	Cloud infrastructure	Operates major data center clusters in Dublin, Frankfurt, and Amsterdam. Partner in Project Nimbus (US$1.2 billion contract with Israeli government).	Project Nimbus contract (US–Israel); EU data center revenue	Part of US$1.2 billion (Nimbus, joint with Google)	European data centers process and store Israeli military data, including surveillance feeds and intercepted communications. Israel pressured Amazon to use a coded "wink" system to sidestep legal orders in European jurisdictions.	Cloud infrastructure provides compute power for AI targeting systems, including Lavender and The Gospel system. Over 11,500 terabytes of military data processed through European-hosted servers.	Enabling	Investigative journalism (The Guardian, +972 Magazine) / Leaked internal documents
23. Google Cloud	US (EU infrastructure: Ireland, Netherlands, Germany)	Cloud infrastructure	Operates data centers in Dublin, Ireland, Eemshaven, Netherlands, and Frankfurt, Germany. Partner in Project Nimbus. Negotiated deeper relationship with IMoD during the war.	Project Nimbus contract (US–Israel); EU data center revenue	Part of US$1.2 billion (Nimbus, joint with Amazon)	Google described its work as civilian, but leaked contracts show a phase 2 to build out IMoD cloud architecture. Internal employees stated the company has limited ability to monitor sovereign nations' use of its cloud.	Cloud infrastructure enables computational processing for military AI systems. IMoD contract expands cloud architecture for additional military units.	Enabling	Investigative journalism (TIME, The Guardian, +972 Magazine) / Leaked contract documents
24. Microsoft Azure	US (EU infrastructure: Ireland, Netherlands)	Cloud infrastructure	Operates major data center hubs in Ireland and the Netherlands. Provides Azure cloud capacity to Israeli military. Largest Microsoft data center outside the US is in Israel.	Israeli Military Contracts / EU Data Center Revenue	Undisclosed (separate from Project Nimbus)	Azure cloud processed approximately one million intercepted Palestinian phone calls per hour. The Irish Council for Civil Liberties (ICCL) lodged a formal complaint with Ireland's Data Protection Commission in December 2025.	Hosts the Rolling Stone surveillance system monitoring Palestinian movements. Provides near-limitless storage for intercepted communications. Eemshaven data center targeted by activist protest in August 2025.	Enabling	Investigative journalism (The Guardian) / Irish Council for Civil Liberties (ICCL) formal complaint / Activist documentation

Annex II: EU-Funded R&D Projects

The table below details specific R&D projects funded through the EDF and Horizon Europe. These projects facilitate the transfer of AI and autonomous technologies that, while classified as research, provide essential technical components for operational systems.

No.	Project Name	Primary EU Fund	Key Partners (Israeli and EU)	Technology and AI Focus	Dual-Use Risk and Gaza Context
1	ACTUS	Horizon Europe	Intracom Defense (IAI subsidiary) / Airbus / Safran	AI for drone weapon integration and target tracking.	€14 million awarded to an IAI-owned Intracom subsidiary. Technology is used to optimize Heron drones currently conducting airstrikes in Gaza.
2	EU-GLOCTER	Horizon Europe	Reichman University, International Institute for Counter-Terrorism (ICT) / Dublin City University	AI for counter-terrorism simulations and doctoral research on global terror threats.	€2.6 million total. Partners include the Interdisciplinary Center (ICT) at Reichman University, staffed by senior veterans of Israeli intelligence and security establishments. These entities provide war games and operational simulations used to refine urban combat doctrines deployed in Gaza.
3	ResponDrone	Horizon Europe	IMoD / IAI	Drone fleet management and 3D mapping.	€8 million total. The Israeli IMoD received direct funding for situational awareness technology used to coordinate drone swarms and map urban zones in Gaza.
4	UnderSec	Horizon Europe	Israel IMoD / Thales / Leonardo	AI multimodal sensors for maritime surveillance.	€6 million total. Started in October 2023. Provides sensors for maritime situational awareness during coastal blockade operations in Gaza.
5	ROXANNE	Horizon Europe	Israel Ministry of Public Security / Interpol / Technion	AI for identifying persons of interest via voice, text, and facial data extraction.	The Israeli Ministry overseeing police and prisons received direct funding to develop these tools. The machine learning techniques for network analysis and target identification are functionally similar to the logic used by the Lavender system to generate strike lists in Gaza.
6	COPAC	Horizon Europe	Elbit Systems / Hebrew University	Engineered quantum dots for ultra-fast computing.	€1 million+ to Elbit Systems and Hebrew University. Research targets breaking and intercepting present-day security systems, key for signals intelligence (SIGINT) operations in Gaza.
7	AUTOFLY	Horizon Europe	Sightec (Israel) / IAI	GPS-independent AI navigation for drones.	€2.5 million total. Critical for drone operations in jammed environments or tunnel networks in Gaza where GPS is unavailable.
8	MARTE	EDF, Grant No. 101168103	Intracom Defense (IAI) / Leonardo	Main battle tank (MBT) AI for automated response.	€15 million+ (consortium). The project integrates lessons learned from current conflicts into its AI logic for urban combat, specifically involving IAI hardware and armored doctrines used in Gaza.
9	TRITON	EDF, Grant No. 101168341	Intracom Defense (IAI) / UBITECH	AI to automate penetration testing and secure tactical military wireless networks.	€15 million+ (consortium share). Awarded in December 2024 to a subsidiary of IAI. Develops AI-driven cybersecurity for tactical networks required to operate IAI drones (for example, Heron MK II) deployed in Gaza.

About the Arab Reform Initiative

The Arab Reform Initiative is an independent Arab think tank working with expert partners in the Middle East and North Africa and beyond to articulate a home-grown agenda for democratic change and social justice. It conducts research and policy analysis and provides a platform for inspirational voices based on the principles of diversity, impartiality, and gender equality.

About the Tech & Society Program

ARI's Tech & Society Program explores how the accelerating deployment of technologies is affecting political life, economic activities, and the environment in MENA. Grounded in ARI's approach which centers political participation and social justice, the program seeks to strengthen public scrutiny, democratic oversight, and civic participation in the deployment of these technologies. For us, the whole tech ecosystem – not just the end-user interfaces – needs to be scrutinized and debated in order to push for safer and more just societies as we move towards an ever-more digitized future.

contact@arab-reform.net
Paris - Beirut - Tunis