



Università  
Ca' Foscari  
Venezia

Corso di Laurea  
magistrale  
in Innovation and  
Marketing

Tesi di Laurea

**“Strategic Innovation in the Defence Sector: A Comparative  
Perspective on Israel and Italy within the European Dual-Use  
Framework”**

**Relatrice/Relatore**

Ch. Prof. Carlo Bagnoli

**Laureando**

Matteo Crozzoli

Matricola 880773

**Anno Accademico**

2024 / 2025

## Index

Chapter 1: Technology Innovations and Defence Forces .....	4
1.1: The disruptive evolution of the world geopolitical context.....	4
1.2 The importance of technology innovation in defence activities .....	7
1.2.1: New defence priorities spur new technology needs .....	9
1.2.2 Successful defence technology disruptors employ five techniques. ....	13
1.2.3 Deep tech as the fourth wave of innovation .....	15
1.3 Dual-use technologies shape the modern battlefield .....	26
1.3.1 Five Market Opportunities for Defence Technology Startups .....	31
Chapter 2: Technology Innovations and Israeli Defence Forces .....	41
2.1: The disruptive evolution of middle east geopolitical context .....	41
2.1.1: Regional Power Shift.....	41
2.1.2: Non-State Actors & Hybrid Threats.....	42
2.1.3 Cyber and Information Warfare .....	42
2.1.4: The Gaza War .....	43
2.1.5: The conservation of the technological superiority .....	44
2.2: Innovation challenges for the Israeli Defence Forces.....	47
2.2.1: Institutional Reform: AI & Autonomy Administration .....	47
2.2.2 Directed-Energy & Air Defence (Iron Beam).....	48
2.2.3 Unmanned Ground Systems & Urban Operations .....	48
2.2.4 Cybersecurity & C2 Resilience .....	49
2.3 Technology Innovations and Israeli Defence Forces .....	50
2.3.1 Deep Tech as a source of innovation for the IDF.....	50
2.3.2: The deep tech innovation ecosystem in Israel.....	60
2.3.3: Israeli Innovation Funding Trends.....	63
2.3.4: Incubators and accelerators .....	68
2.3.5 The Talpiot Program.....	87
2.3.6: The Unit 8200 .....	94
2.4: Conclusion.....	98
Chapter 3: Technology Innovation and Italian Defence Forces .....	100
3.1: The disruptive evolution of European geopolitical context .....	100
3.1.1 The Italian case .....	103
3.2: The innovation framework adopted by Italian Defence Forces .....	105

3.2.1: Strategic Analysis: Strengths and Limitations .....	108
3.2.2 Exein and Ephos case .....	109
3.2.2: Dual Use technology in the Italian Innovation Framework .....	111
3.2.3: Dual-Use Technology in Practice: Connecting Exein and Ephos to Italy's Defence Innovation and Spending Objectives .....	113
3.2.4: Italy–Israel Dual-Use Technology Cooperation: A Strategic Bridge for Innovation .....	115
3.3: How to build a Italian start-up ecosystem .....	118
3.3.1: Legal and Institutional Foundations .....	118
3.3.2: Funding Infrastructure and Dual-Use Finance .....	119
3.3.3: Funding Infrastructure and Dual-Use Finance .....	120
3.3.4: Human Capital, Talent and Mobility .....	121
3.3.5: Governance, Metrics and Strategic Alignment .....	121
3.3.6: Internationalization and Scaling.....	122
3.3.7: Case Studies Deep Dive .....	122
Chapter 4: General Conclusion .....	125
Bibliography: .....	133

# Chapter 1: Technology Innovations and Defence Forces

## 1.1: The disruptive evolution of the world geopolitical context.

The world's geopolitical landscape is undergoing a profound and disruptive evolution, driven by a convergence of longstanding power rivalries, emerging technologies, transnational challenges, and shifting ideological currents (Romansanta, Ahmadova, Wareham, & Priego, 2022). In the aftermath of the Cold War, many observers proclaimed the dawn of a liberal, U.S.-led unipolar moment; yet over the past two decades, that promise has given way to a far more contested and fragmented order. The rise of China as a comprehensive strategic competitor has rebalanced Asia's power dynamics, while an increasingly assertive Russia has sought to reclaim influence in its near abroad (Romme, 2022). At the same time, regional powers such as India, Turkey, Iran and Saudi Arabia are leveraging economic growth and regional ambitions to carve out autonomous spheres of influence, often pursuing policies at odds with both Washington and Beijing.

Technological change constitutes a second major axis of disruption (Peña & Jenik, 2023). Competition over critical emerging technologies, quantum computing, biotechnology and next-generation telecommunications, has intensified strategic mistrust and prompted a shift from globalized innovation networks toward "friend-shoring" and tighter export controls. Cyberspace itself has become a new domain of great-power rivalry, with state-sponsored hacking, disinformation campaigns, and digital surveillance extending traditional geopolitical contests into

the virtual realm. Meanwhile, social media platforms have empowered non-state actors, from extremist groups to transnational corporations, to shape narratives, mobilize support, and influence elections in ways that evade conventional diplomatic or military countermeasures.

Artificial intelligence has rapidly emerged as the latest, and perhaps most consequential, frontier of geopolitical competition (Carnegie Endowment for International Peace, 2024; Clark, 2023). Nations are racing to develop advanced AI systems capable of powering everything from automated defence platforms to predictive governance tools. This has sparked an AI arms race in which ethical norms, safety standards, and export regulations are weaponized alongside algorithms themselves. States with leading AI prowess can bolster their economic competitiveness through productivity gains, dominate future high-tech industries, and wield new forms of surveillance and social control. At the same time, AI-driven disinformation engines amplify propaganda at an unprecedented scale, eroding trust in democratic institutions and complicating efforts at global cooperation. The uneven distribution of AI talent and compute infrastructure also risks deepening the divide between technological “haves” and “have-nots,” prompting lower-resourced countries to either bandwagon with dominant powers or pursue independent, sometimes destabilizing, development paths. In short, artificial intelligence is reshaping not only the tools of power but the very calculus of strategic decision-making, forcing states to rethink doctrines of deterrence, data sovereignty, and human-machine collaboration.

To navigate these technological shifts, governments must overhaul traditional defence procurement processes and policy frameworks, adopting agile, modular approaches that mirror commercial best practices and embrace continuous experimentation (Clark, 2023; RAND Europe, 2024). This includes establishing dedicated AI governance and ethics bodies, such as the U.S. Department of Defence’s Chief Digital and Artificial Intelligence Office and proposed extensions to the EU’s AI Act, to ensure cross-domain coordination, transparency, and accountability in weapons development (Csernatoni, 2024; Reuters, 2024). Moreover, states invest in

workforce transformation by partnering with academia and industry to cultivate AI expertise, integrating machine teaming principles into doctrine and training exercises to maintain decision superiority while upholding meaningful human control over lethal systems (RAND Europe, 2024; Clark, 2023).

Beyond the power struggles of states and corporations, the pressing realities of climate change and pandemic risk are redefining the very parameters of security. Melting Arctic ice is opening new sea lanes and resource-rich territories, stoking competition among Russia, China, and the United States. Water scarcity, desertification, and extreme weather events are fueling internal displacement and cross-border migration, exacerbating social tensions and prompting militarized border responses. The COVID-19 pandemic underscored global supply-chain vulnerabilities, inspiring national strategies to reshore critical industries and stockpile essential medical supplies, measures that, while enhancing resilience, threaten to further fragment the global economy.

At the ideological level, the post-Cold War triumphalism of liberal democracy has given way to a more complex contest between competing governance models. Authoritarian and hybrid regimes have grown more sophisticated in their use of economic incentives, digital surveillance, and propaganda to project stability and economic promise, while liberal democracies struggle with populist backlashes, political polarization, and waning public confidence in multilateral institutions. This contest has played out across battlegrounds such as Africa and Latin America, where infrastructure investments, debt-financing, and security partnerships offered by Beijing and Moscow challenge the traditional development paradigms promoted by Western donors.

The proliferation of non-state actors: terrorist networks, private military companies, global criminal cartels, and international NGOs, further complicates the picture. Today's conflicts often feature a complex mosaic of state and non-state actors, shifting alliances and proxy engagements, from cyber-mercenaries in Eastern Europe to private security contractors in Africa and the Middle East. Global corporations, especially in the extractive, defence, and technology sectors, wield

financial clout and lobbying power that rival many midsize states, influencing policy decisions and strategic alignments in subtle but consequential ways.

In this disruptive environment, conventional tools of diplomacy, deterrence, and alliance-building are being both tested and reinvented. New security architectures; from the Quad in the Indo-Pacific to expanded Arctic forums, seek to bridge like-minded partners around shared challenges, yet they also risk deepening divisions with excluded powers. Economic levers such as sanctions and trade diversification are increasingly weaponized, but their long-term efficacy depends on sustained unity among sanctioning states. Likewise, emerging domains such as outer space and cyberspace demand novel legal frameworks and cooperative norms, even as major powers vie to assert rules of their own making.

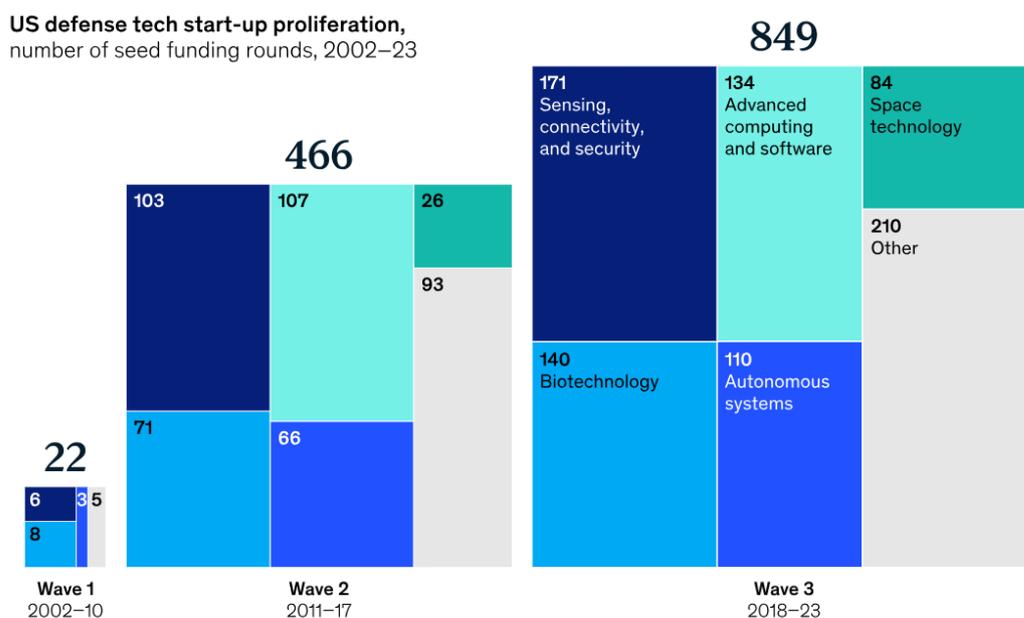
Ultimately, navigating the disruptive evolution of the world's geopolitical context will require a blend of adaptive governance, resilient multilateralism, and pragmatic strategic engagement. States and societies must reconcile the competing demands of national security, economic vitality, and global public goods, whether in climate mitigation, pandemic preparedness, or digital governance, while preserving the flexibility to respond to unforeseen challenges. In an era defined by flux and contestation, success will belong to those actors best able to forge dynamic partnerships, harness technological advances for inclusive growth, and uphold the rule-based principles essential to collective stability.

## 1.2 The importance of technology innovation in defence activities

Countries around the world are modernizing their military capabilities in response to a new era of geopolitical unpredictability and a fast-changing national security environment (Klempner, Rodriguez, & Swartz, 2024). And, as new mission requirements emerge throughout multidomain operations, different tools are in

demand, supplied by a variety of new entrants into the defence business. National security customers are expressing a need for technologies from companies other than the traditional defence industrial base. This dynamic is not new, manifested in three successive waves of defence technology start-ups during the last two decades.

Picture 1: growing of tech start-up in the U.S.



<sup>1</sup>Other includes advanced materials, human machine interfaces, quantum, energy generation or storage, and semiconductors.  
Source: Pitchbook; McKinsey analysis

McKinsey & Company

Sources: McKinsey & Company

In the United States, SpaceX and Palantir were significant startups in the first wave of the early 2000s; both built technologies for government channels other than the Department of Defence (Klempner et al., 2024). A second wave emerged in the mid-to-late 2010s, led by new entrants like as Anduril and ShieldAI, both now unicorns, that used commercially generated technology targeted to defence applications (Klempner et al., 2024). A third wave of disruption is already emerging: a far larger ecosystem of start-ups and atypical businesses that are pushing innovation, garnering major venture capital (VC) money, and seeking ways to scale (Bessemer Venture Partners, 2024).

In many cases in Europe and the United States, these start-ups (along with their commercial hyperscaler counterparts) are well-positioned to meet critical national security needs, supplementing the traditional industrial base, which may lack the capacity to respond to changing demands on its own. However, before large-scale solutions can be safely delivered to national security consumers, hurdles must be overcome. Effective strategies geared to defence customers could make the journey easier, and successful firms in this environment may need to leverage dual-use technology (suited for both military and nonmilitary applications) to drive growth (Klempner et al., 2024).

### 1.2.1: New defence priorities spur new technology needs

For decades, national security agendas were largely concerned with asymmetric and transnational threats like terrorism and cybercrime (Siegel & Krishnan, 2020). However, the uncertain global geopolitical environment can occasionally lead to peer and near-peer competition, as illustrated by national security strategies issued since 2022 in Germany, Japan, the United Kingdom, and the United States.

These tactics may generate demand for new technologies to improve resilience and efficacy, particularly those that support new disaggregated and "joint all-domain" notions.

We have noticed that there is a call for three overlapping sets of capabilities (Carnegie Endowment for International Peace, 2024):

- Disaggregating capabilities: By breaking down capabilities into smaller nodes, force planners may eliminate points of failure and increase the likelihood of successful operations that connect air, land, sea, and space forces. This could increase operational coverage and resilience. Instead of a single high-value satellite, a network of smaller, linked satellites may be preferred, instead of a single human submarine, a coordinated fleet of unmanned underwater vehicles.

- **Effective communication networks:** For such disaggregated assets to work together, real-time intelligence exchange, facilitated by durable and effective communication networks, is critical. Resilient networks can assure fast communication between assets (sensors and effectors) and enable smooth, responsive operations. Resilient network-enabling technologies like 5G, phased-array antennas, artificial intelligence (AI), and high-density computers can help relocate responsive decision-making to the tactical edge, where it can have the biggest mission impact.
- **New Technologies:** Engineering high-bandwidth, robust networks will most likely require retrofitting existing platforms or creating new architectures (for example, AI-powered command-and-control systems that connect customers across services and collating partners in air, land, sea, and space). The density of technology-enabled mission systems is projected to expand in the foreseeable future. In any case, new technologies such as decentralized cloud computing, data management, edge analytics, autonomy-enabling systems, and a wide range of hardware solutions and novel materials are regularly highlighted as capability requirements.

Start-ups, like their commercial hyperscaler counterparts, are well positioned to meet vital national security needs while supplementing the old industrial basis.

In addressing these needs, the traditional defence industrial base can offer various strengths to national security customers, including an understanding of specific missions, deep technical expertise in designing for those missions, long-established security protocols and infrastructure for hosting classified data, business development and customer relationships, acquisition capabilities, program management excellence, and integration opportunities within existing, installed platforms.

These qualities, however, may no longer be sufficient. A new generation of security technology companies has emerged to meet changing needs. This new cohort includes both start-ups and commercial technology hyperscalers, which can provide separate but complementary benefits:

- The defence contractor spends more on high-risk R&D than the norm. It also invests in top-tier software and attracts STEM talent with expertise in digital technologies like AI, quantum computing, and advanced microelectronics.
- Product-oriented business approaches are generally faster, cheaper, and more inventive.
- A concentration on commercially priced, scalable products and services.

The European Union and the United States have expressed an interest in these innovative capabilities. The US Department of Defence has taken steps to gain access to commercial technology through new procurement and budgeting authorities, such as raising the profile of the Defence Innovation Unit and launching the Replicator initiative in 2023 to swiftly field autonomous, attritable systems.<sup>6</sup> NATO has established an innovation accelerator (DIANA) to stimulate engagement with start-ups and other technology companies, as well as the €1 billion NATO Innovation Fund, which will focus on dual-use innovations.

Private capital has also expressed a desire to investigate defence technology prospects, and we have seen that VC investment in such technologies exceeded general increase in venture spending between 2019 and 2023. Meanwhile, established military businesses have strengthened their corporate venture funds to gain access to innovative technologies.

Despite this momentum, many next-generation defence tech firms have struggled to do business at scale with national security organizations.<sup>8</sup> This is likely due to three main challenges:

- Reconciling program-centric and product-centric operational strategies. Customers in the national security sector frequently choose tailored solutions to highly specific challenges over "out of the box" commercial offerings. With restricted access to sensitive information and other sources of knowledge, tech companies may fail to identify the specific nature of these issues. The endeavor to modify an existing solution to the "last mile" of defence may also be incompatible with the commercial-scale economic models preferred by IT corporations.

- Developing go-to-market capabilities for defence markets. New defence technology companies may be limited by their lack of knowledge with the government sales and contracting landscape. Scaling a solution in military markets necessitates a strong government affairs operation and a mastery of the various government procurement procedures. Start-ups, in particular, frequently lack a track record of success on programs of record at defence agencies, which can be a critical condition for securing new business.
- Matching revenue timeframes to investor expectations. Government contracts frequently provide an abnormal return profile to private capital (such as venture capital and growth equity), which has emerged as the principal backer of defence technology start-ups. Private investors typically want returns over three to five years, which can differ from the slower (traditionally seven to ten years) pace of defence programs of record. A start-up may run out of money before consistent revenue from government contracts begins to appear. This mismatch is likely to discourage private investment.

Given their emphasis on short-term results and an aerospace and defence investor base that frequently prioritizes reliable cash flows over risky investments in breakthrough technology, public markets are unlikely to fully fill this gap. Meanwhile, governments in Europe and the United States generally invest less in innovation than their private sector counterparts: for example, the US national security community has recently been spending less than 5% of its total budget on developing innovative technologies, whereas a typical commercial technology firm spends three to four times that amount of revenue each year.

## 1.2.2 Successful defence technology disruptors employ five techniques.

How do we deal with these challenges? Five excellent methods are among the lessons acquired from successful military technology companies.

- Create the infrastructure for scaling from the beginning. Most military tech businesses eventually become hardware companies, and many are now confronted with the same scaling issues as their more established colleagues and competitors, such as maintaining manufacturing speed and quality, durable supply chains, and machining or technical talent. Building scaling infrastructure into the early strategy, beginning with prototyping resources, can have a significant impact on time to market.
- Lower the hurdles by utilizing more established partners. Once a product's viability has been shown, collaborating with an existing industrial defence company could help it enter the market. Established suppliers can contribute established bases, mission experience, and client familiarity to supplement IT businesses' skills. Established suppliers frequently influence access to the aircraft, land systems, and ships into which new mission systems will be incorporated by providing the "socket" into which a disruptor's "lightbulbs" can plug. Recent cooperation announcements between defence tech disruptors and established defence corporations include hardware and software in a variety of technology focus areas, including as 5G, hypersonic aircraft, autonomy for next-generation tactical aircraft, AI, and edge networks. Consider the defence disruptor Helsing, which was able to achieve a program of record in less than three years by collaborating with an existing defence prime (Saab). Helsing's AI and signal processing capabilities enhanced Saab's

hardware-based sensors and self-protection systems. As the two firms grew closer, Saab made a significant investment of €75 million in Helsing's most recent venture round in September 2023, valued at €1.5 billion.

- Go for dual use. Purely may struggle to scale defence-focused startups before investors become dissatisfied with delays. However, companies that discover nonmilitary applications for their technologies might gain size in commercial markets while purchasing time to seek a long-term defence contract. However, pursuing dual-use technologies may necessitate developing a two-speed business model to fit varying timetables and unique international security concerns. Strong demand and solid capital inflows have enabled several dual-use technology companies to grow. Private investors, who have a higher risk tolerance than public markets or government R&D appropriators, are often looking to fund dual-use technology because of its enormous potential returns and broad applicability.
- Vertically integrate to give software and hardware in a single solution. Defence customers prefer integrated hardware and software systems over stand-alone software capabilities that may be used with a variety of hardware. For technology disruptors, selling distinctive software bundled within hardware can be advantageous.
- Customize sales capabilities to the customer. Selling to defence customers might be difficult if a company has not established a government affairs section with the necessary clearances and experience. Tech companies can explore beyond a defence organization's broad requests for bids and communicate with potential customers about specific requirements.

### 1.2.3 Deep tech as the fourth wave of innovation

Deep tech emerges as a disruptive force in the ever-changing technological landscape, capable of tackling global challenges and significantly shaping the future. But what exactly does 'Deep Tech' mean?

Unlike superficial technologies, which are frequently focused on consumer applications or incremental improvements, Deep Tech is founded on groundbreaking scientific discoveries and radical technical advancements. These technologies are the result of years of study and development in complicated fields, including biotechnology, advanced artificial intelligence, photonics, and materials science. One example is the development of new gene therapy medications, which necessitates a thorough understanding of the human genome and disease molecular pathways.

It is fundamental to understand that 'Deep Tech is not a new technology, but a new approach to business innovation' (Bagnoli, C., & Portincaso, M., 2021).

Deep Tech breakthroughs are therefore driven by the desire to provide novel answers to civil society's issues and problems, which leads to seeking the best technology, new or existing, to tackle an "old" problem (Bagnoli, C., & Portincaso, M., 2021).

Deep Tech technologies are notoriously difficult to copy, as they are frequently protected by patents and proprietary knowledge. Consider CRISPR-Cas9 technology for gene editing, which takes specialized skills to deploy. Furthermore, Deep Tech solutions seek to have a long-term impact on society by addressing global issues like climate change and encouraging sustainability. The development of new sources of clean energy, such as nuclear fusion, is an excellent example.

It is critical to note that the development of these technologies necessitates significant time and expenditure. Developing a quantum computer, for example,

necessitates costly infrastructure and highly specialized research groups. Despite the hurdles, Deep Tech companies have huge development potential, with the opportunity to transform entire industries and open new markets. Artificial intelligence used in medical diagnostics can increase diagnosis accuracy and speed, lowering costs and increasing healthcare outcomes.

This approach to invention is defined as the fourth wave of innovation, the most disruptive to date, with the potential to 'influence business and society equivalent to or greater than that made by the emergence of the Internet' (Bagnoli, C., & Portincaso, M., 2021).

Four waves of innovation characterize the economy's evolution, and every wave puts the basis for the next one. The first originated with the First and the Second Industrial Revolutions. It is characterized by fundamental development in the fields of chemical, material, electricity, and communication.

The second one happened after the Second World War; it was characterized by the creation of big laboratories for company research. These laboratories were characterized by multidisciplinary and a focus on basic research (Bagnoli, C., & Portincaso, M., 2021). Great achievements of this period were in the field of the ITC, with the creation of the first personal computer.

On the other hand, the third wave of innovation was characterized by more applied research thanks to the contribution of the new venture capital funds. In contrast, the basic research was progressively entrusted to the state funds. The fact that the wave of innovation was dominated by ICT and biotechnologies in the long period puts some limits to the standard model of venture capital because standard evaluation models created for these two profiles of investment have difficulty to work in the other contexts.

In the two standard cases, we have two opposite situations:

- "Low technology risk and high market risk in the digital sector." It is easy to construct the core technology platform Airbnb, but harder to establish it as a market leader, which is the only sustainable competitive position in the winner-takes-all scenario.

- 'High technological risk and little commercial risk in biotechnology.' It is difficult to synthesize a chemical that stops cellular aging, but those who succeed will have market success (Bagnoli, C., & Portincaso, M., 2021).

Starting from this point, the fourth wave of innovation aims to create an innovative approach suitable for every field (de la Tour, A., et al., 2021). As we said before, innovations in the deep tech field constitute a competitive advantage because they are difficult to copy and necessitate huge investments, advanced skills, and long development periods (Dionisio, E.A., et al., 2023).

The characteristics that characterize the fourth wave of Deep Tech innovation can be described through four basic elements, which are: (Bagnoli, C. & Portincaso, M., 2021)

- problem orientation;
- convergence between disciplinary fields;
- the convergence between technological clusters;
- the Design-Build-Test-Learn cycle.

Companies embracing the Deep Tech strategy ambitiously attempt to discover a solution to the most critical problems facing civilized society, which present technologies are unable to provide an answer to, such as the challenges connected to climate change, health, and renewable energy (Romasanta, A., et al., 2021).

Their primary goal is to solve a real-world problem rather than to develop applications for unique technology solutions. Pivot Bio, for example, has developed a revolutionary method to handle the "old" problem of fixing nitrogen at the roots of plants, renouncing the usage of ammonia, whose manufacturing is highly polluting (Bagnoli, C. & Portincaso, M., 2021). The creation of these technologies follows an inverse process concerning applied research, because 'they are built on the development of fundamental research, striving for a profound understanding of phenomena, driven by considerations of the future uses of the new information created (Bagnoli, C. & Portincaso, M., 2021).

The design thinking technique will be used to identify the problem and determine how to solve it. The challenge "must be, in addition to being human-centered, broad

enough to have a real impact and allow creative solutions to emerge but narrow enough to make it possible to manage it without discouraging the team that is called upon to tackle it (Bagnoli, C. & Portincaso, M., 2021).

Start-ups are frequently preoccupied with the technology solution they have created; similarly, existing businesses risk becoming obsessed with perfecting and adapting their answer, and both risks losing sight of the problem. In this regard, the most important steps are market research and understanding the demands of target customers to build an effective solution and develop a value-based strategy that ensures maximum return and scalability. Furthermore, purpose, through problem focus, fosters talent retention, global momentum, and continual dialogue across diverse teams (de la Tour, A., et al., 2021).

Deep Tech firms are distinguished by the confluence of several technological advancements that lead to the development of disruptive solutions (Romme, A.G.L., et al., 2023). They are based on the convergence of different disciplinary fields: advanced science, which is characterized by the generation of new knowledge without posing the problem of its practical implications; design, which is concerned with the exploitation of existing knowledge to satisfy human needs, transcending the understanding of the underlying phenomena; and engineering, which, by ensuring the technical and economic

Advances in diverse disciplinary fields must occur concurrently. A Deep tech enterprise must, in reality, ask itself three essential questions from the start: what is the problem we are addressing? How can we use modern science to tackle it in a novel and improved way? Will this solution operate outside of the laboratory, and can it be priced competitively? (Bagnoli, C. & Portincaso, M., 2021).

"The convergence of many disciplinary domains makes interdisciplinary teams vital. Regardless of the job (investor, start-up, or established company), all team members must have a 'T' profile, which includes surface experience in numerous fields as well as in-depth expertise in one. Investors may correctly characterize an issue and comprehend the potential scientific remedies, but they typically lack the engineering knowledge to assess its technical feasibility and economic viability, or vice versa.

Start-ups are usually capable of dealing with scientific issues; some may even be able to correctly characterize a problem, but they frequently lack engineering expertise (Bagnoli, C. & Portincaso, M., 2021). The convergence of diverse disciplinary domains and the combining of cross-disciplinary competencies allow to expedite learning and experimentation, reduce risk and complexity, and boost the return on investment in innovations (Paschkewitz, J., et al., 2022).

Another aspect is technological convergence: 97% of Deep Tech organizations use at least two existing or upcoming technologies, with 66% employing more than one. Deep tech's technology clusters include computing and cognition (AI, behavioral and neurological sciences), sensing and motion (IoT and robotics), and matter and energy (nanotechnology and synthetic biology), (Bagnoli C. and Portincaso M., 2021).

The emergence of technological platforms that lower the barriers to experimentation, promotion of innovation, and collaboration is a determining factor that enables and stimulates innovation (Siegel, J. E., & Krishnan, S., 2020). This reduces the cost of supporting new deep-tech enterprises, and company growth lead to a fall in the cost of, for example, liquid handling equipment in wet labs, sequencing and DNA synthesis technologies, and access to the infrastructure needed to build them (Bagnoli, C. & Portincaso, M., 2021). Collaboration is critical in lowering barriers and activating an innovation process; one of the ways that is becoming established is that of open innovation; to identify innovation opportunities and to progress in the process, Cloud platforms are important, which, thanks to the increasing availability of data, gather information and enable democratic monitoring of the innovation cycle (Dimitrova, R., SIF 2022). The expansion of invested capital also helps to foster growth and innovation in deep technology. These rose from \$15 billion in 2016 to more than \$60 billion by 2020 (de la Tour, A., et al., 2021).

The 'engine' that powers the Deep Tech innovation strategy is the Design-Build-Test-Learning (DBTL) engineering cycle. This "cycle" serves as a link between the problem being addressed and the science and technology used to solve it. Each encounter in the DBTL cycle is evaluated based on how it contributes to issue-

solving. Problem orientation becomes even more important, as it is also required for the proper development of the DBTL cycle. The DBTL cycle's strength is unleashed through technological convergence. It allows you to first select the most effective technologies for tackling the problem at hand, but also to use a different technology with each encounter (Bagnoli, C. & Portincaso, M., 2021).

Design is the primary phase of the DBTL cycle; it provides for the creation and description of the intended product attributes. Access to a big pool of data at every low cost speeds up the hypotheses-driven innovation process. Speed, open source, processing skills, and availability of cloud computing are all important considerations at this level. 'All of this makes it easier to design high-performance models for research and development activities including novel materials, chemicals, images, sounds, and architecture. Furthermore, the application of generative design broadens the design methodology beyond the initial discovery phase. Prototypes can be scanned and equipped with sensors that offer real-time performance data, which is then sent back into the design process, allowing the object to co-design itself. In the design phase, these possibilities will benefit from quantum computing applications, which will make it possible to 'process huge amounts of information and execute certain algorithms exponentially faster, promising significant impacts especially in the fields of biopharma, chemistry, materials design, and fluid dynamics (Bagnoli, C. & Portincaso, M., 2021).

The Build & Test phase enables economies of scale, speeding up processes and improving their precision, thanks to the "growing emergence of Cloud computing platforms and synthetic biology materials, and the increasing push for process automation through the use of robots." Large user communities take advantage of developing platforms in a variety of Deep Tech disciplines while also contributing to their growth. This also allows start-ups to leverage easily scaled support services, gaining access to capabilities that would otherwise be too costly in both monetary and time terms, and/or too technologically hard to develop in-house (Bagnoli, C. & Portincaso, M., 2021).

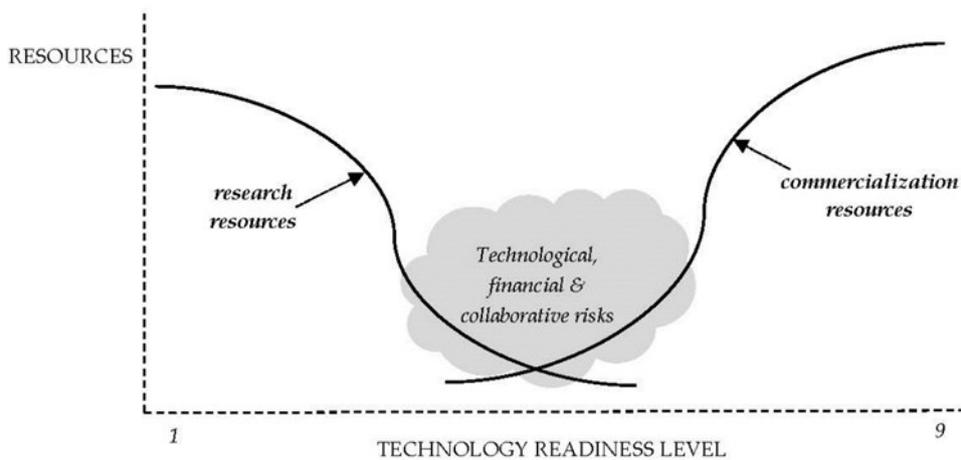
In the learning phase, results are based on the results of the previous DBTL cycle and guide the design phase of the current DBTL cycle, speeding up refining the intended goals. 'The massive amount of data created during the Build & Test phase can be used to feed AI and machine learning algorithms, reducing the learning time from weeks or months to days or minutes. The algorithms automatically learn which types of products are appropriate and which are not, revising the assumptions established during the design phase and initiating a new feedback loop. In materials science, for example, the US startup Kebotix blends machine learning algorithms for modeling chemical structures with an autonomous robotics laboratory that synthesizes, tests, and returns results to the algorithms (Bagnoli, C. & Portincaso, M., 2021).

The disruptive innovations that distinguish deep tech start-ups carry a slew of hurdles and impediments that these businesses must overcome to grow and realize their full potential. The problems and high risks that these realities face can be linked back to the significant risk of failure of advanced technologies, the substantial investments necessary, and the lengthy time-to-market. Governments should streamline bureaucratic and legal impediments (Schuh, G. & Latz, T., 2022).

Deep tech realities have a very high failure rate compared to other activities, and their level of complexity implies that they confront a long and deep valley of death during the development and subsequent commercialization phase. This concept is related to the difficulties of obtaining appropriate money for these realities.

The 'valley of death', depicted in Picture 2, considers two variables: the time to market required for the technology to be commercialized, indicated by the Technology Readiness Level (TRL), and the resources required from the development phase to commercialization.

The TRL measures the degree of maturity of the development of a given technology; it can take a minimum value of 1 up to a maximum value of 9, which proves the technological success tested in an operational environment, as can be seen from Figure 1, the valley typically extends from TRL 2 or 3 to TRL 7 or 8 (Romme, A.G.L., et al., 2023).



Picture 2: Valley of Death

Source: Romme, A.G.L., et al., 2023

Many deep tech start-ups are unable to bridge the gap between the initial resources received during the research phase, which are frequently from public money, and the private resources required for industrialization and commercialization at a later stage. As a result, the valley is extraordinarily deep (on the vertical axis due to the large resources needed) and long due to the typical features of these realities (Romme, A.G.L. 2022). This gap can be separated into two distinct valleys, the first referring to technology and hence the difficulties encountered during the research and development phase, and the second to the implementation and commercialization phase in the market. Open-source models serve to decrease these obstacles by speeding development processes and providing access to a database of resources and information from multiple actors, from which these entities can design and test goods and technologies, accelerating the commercialization cycle (Nedayvoda, A., et al., 2020).

Investors perceive these realities as complex and dangerous, and they are frequently misvalued because of an inadequately transparent and clear story. The Vally of Dead is important for getting a perspective on what are the primary issues encountered by deep tech ecosystems (Romme, A.G.L. 2022).

These realities necessitate a rethinking of value chains and business structures so that they can capture the value they create. It is also critical to develop an effective value proposition and model that exploits commercial prospects while overcoming

challenges that impede their capacity to scale. The challenge of reimagining value chains and business models appears daunting, especially for established companies that struggle to abandon certainties, question existing mental models, face the unknown, and build on anomalies and exceptions (Bagnoli, C. & Portincaso, M., 2021). Today's market is much more dynamic and innovation processes are continuous, industry-leading companies struggle to defend their position for a long time, 'in previous decades, 77% of industry-leading companies were still leading five years later; but today this percentage has almost halved to 44%' (Bagnoli, C. & Portincaso, M., 2021).

The deep tech ecosystem requires an entrepreneurial approach focused on innovation and a long-term outlook, which promotes the emergence of direct solutions and is conducive to addressing the risks associated with them to reach its full potential, stimulating the creativity and ambition of the start-ups that operate within it (Kask, J. & Linton, G., 2023).

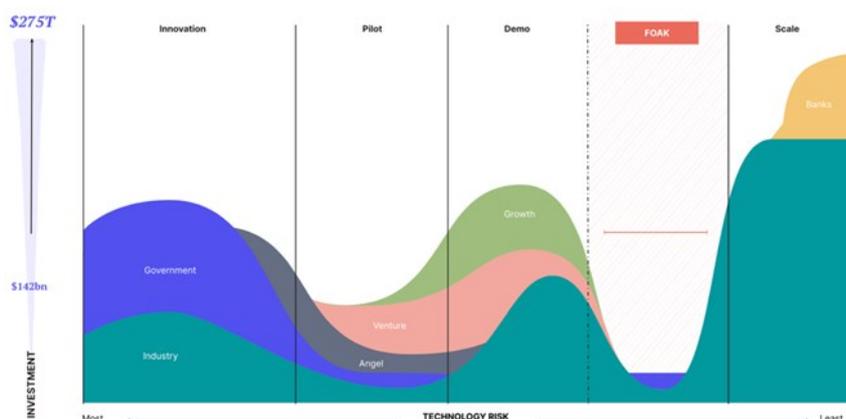
One of the recognized issues is the need to push scientific limits even further. To achieve this, it is important to build a network of partners with complementary skills and resources, to have access to the necessary critical resources and specific know-how required by the sector, stimulating collaboration through technological specializations rather than a focus on geographical areas (Kask, J. & Linton, G., 2023).

The networks created must contain various actors with transversal competencies that allow collaborations between the public sector, such as governments and universities, and the private sector, which includes start-ups and established businesses, for the benefit of scientific development. The transversality of the sectors of inventions and technologies, as well as the collaboration of different actors, provide a very high positive spillover impact (Schuh, G. & Latz, T., 2022).

These issues are compounded by the difficulty of scaling up a minimum viable product (MVP). Developing an MVP is frequently quite complex, as is assuring its scalability, i.e. the engineering required for its "industrial" manufacturing. A

physical Deep Tech product, particularly biological or nanotechnology MVPs, is far more complex and expensive to scale than a digital one. The scale-up phase is also critical to ensuring its viability at market rates. The problems that must be overcome, frequently with no prior experience, include both the technical and economic elements of production (Bagnoli, C. & Portincaso, M., 2021).

The term 'FOAK' (First-of-a-Kind) refers to the phase before the solution's scalability (Picture 3). Initiatives at this stage have typically gone through numerous 'valleys of death', first establishing the functionality of their technology in a laboratory and then in the real world through a pilot project. At the 'FOAK' stage, it must be proved that the solution is successfully scalable and that all commercial, operational, technical, and production risks can be reduced, making it appealing to potential project sponsors (Cohen, G., et al., 2024).

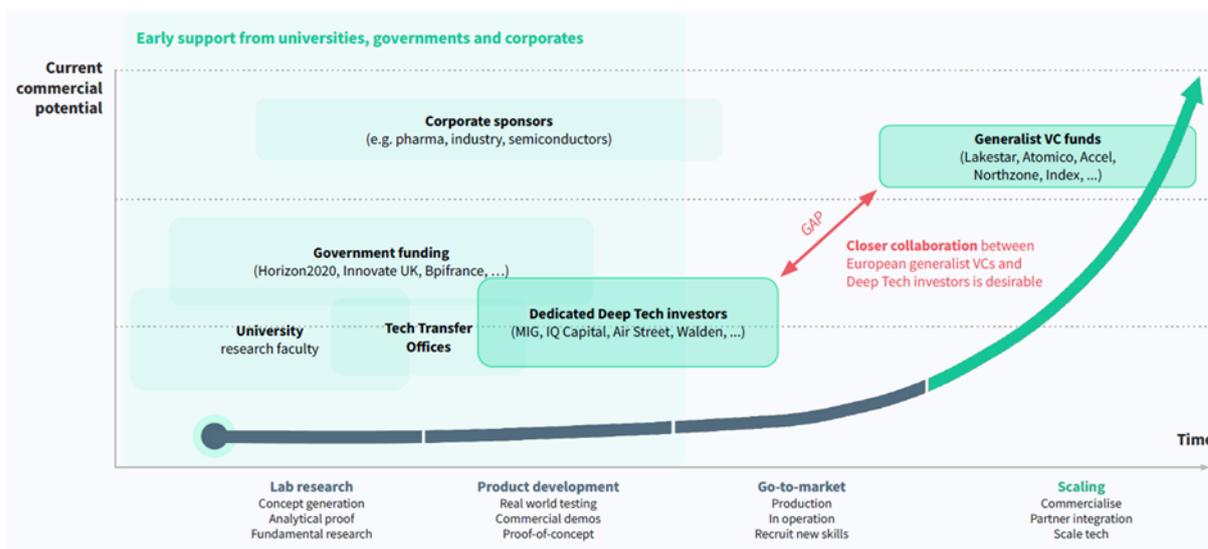


Picture 3: FOAK (Fist-of-a-Kind)

Source: Cohen, G., et al., 2024

One of the most challenging challenges these realities confront is getting adequate money for their development, which is further complicated by the long lead times and unpredictability that characterize the procedures. A fundamental goal is to eliminate the information asymmetry that frequently occurs between deep tech start-ups and venture investors, so that they have the necessary information and experience to evaluate technologies and innovations, simplifying access to money (Kask, J. & Linton, G., 2023).

Deep Tech start-ups are sponsored by different parties at each step of development, and the associated risk varies accordingly, yet significant gaps remain between the stages. Picture 4 demonstrates that there is a gap at the European level between investments that support the development phase and those that take over in the latter stages of scale-up, not completely meeting the needs of the 'go-to-market' phase (Browne, O., 2023).



Picture 4: Stages in the evolution of a deep tech start-up and financing actors

Source: Browne, O., 2023

To better understand Deep tech, let's explore some specific instances. Pivot Bio is transforming sustainable agriculture with a revolutionary solution for nitrogen fixation in plants that eliminates the need for ammonia, a highly polluting fertilizer. Kebotix employs machine learning techniques to predict molecular structures for batteries and new materials, hence speeding up the discovery and development of novel materials.

Despite its potential, the Deep tech industry confronts problems such as lengthy development durations, significant research expenditures, and difficulty in commercialization. Deep Tech start-ups are, indeed, characterized by a longer stage of R&D than the other types of start-ups, therefore, they require a superior investment to succeed (Appendix A). However, despite being perceived as riskier,

Dealroom.co reported that they have the same possibilities of success and failure as the Tech ones (Wijngaarde, Y., 2022).

However, the prospects are equally significant: solving global problems, developing new markets, promoting long-term economic growth, and disrupting established sectors. Deep Tech is already altering industries including healthcare, energy, manufacturing, and the environment by providing creative solutions for disease diagnostics, renewable energy generation, sustainable manufacturing, and environmental monitoring.

It is important to establish an environment favorable to this type of innovation to make Deep Tech develop its full potential. It is necessary to have an environment that fosters R&D, the possibility to build specialized human capital, and, as we said before, access to financing, particularly in the first stages of development (Dionisio, E.A., et al., 2023).

One can see how Deep Tech a driving force of innovation with the potential is to transform our world. It therefore becomes imperative for companies, governments, and investors to be able to grasp its potential to play a key role in shaping a more sustainable and prosperous future.

Deep technologies, such as improved materials are not only important drivers of economic growth, but also essential for national security and global influence. As countries traverse the intricacies of technological innovation, knowing and evaluating the crucial features of deep tech businesses is critical to developing a cohesive and effective national strategy.

### 1.3 Dual-use technologies shape the modern battlefield

Recent developments in the Transatlantic agenda have elevated dual-use technology, which have both civilian and military applications, to a new level of importance

(Alvarez-Aragones, 2024). For example, Russia's full-scale invasion of Ukraine in 2022 drove the European Union and the United States closer to imposing sanctions on the Kremlin (Alvarez-Aragones, 2024). The United States also imposed export limitations on China's access to semiconductors and supercomputing capabilities, involving the Netherlands and Japan. Many EU leaders were concerned about the decision's unilateral nature. However, these occurrences demonstrate that the intersection of trade and technology is a major national security concern in international relations.

Dual use technologies are fundamentally strategic for international markets and a wide array of industries and include advanced semiconductors, artificial intelligence, biotechnologies, and quantum technologies (Alvarez-Aragones, 2024). For example, semiconductors are used in unmanned aerial vehicles (UAV), global positioning systems, radars, and missile guiding systems, among other military applications. With AI, governments can enhance national security decision-making by processing and collating large amounts of data and identifying patterns and trends that the human mind cannot. Quantum computers and technologies, on the other hand, can tackle complex mathematical problems much quicker than conventional computing, raising concerns about whether existing encryption methods are safe enough to safeguard classified government data and information. However, the sometimes ambiguous and inconclusive definition of "dual use" makes it difficult to regulate these technologies (Ding & Dafoe, 2021). For example, if someone lights a cigarette, a civilian object, and then uses it to harm someone, is the cigarette considered a dual-use good? Not really. The context around a technology's military applications, rather than essentialist arguments, determines whether it is dual use. Science, innovation, and strategic investments, among other factors, shape the dual-use potential of technology, making it fluid and dynamic, evolving and changing over time because of scientific revolutions in the military sector.

In "The Logic of Strategic Assets: From Oil to AI," Jeffrey Ding and Allan Dafoe, both from the University of Oxford, give a valuable framework for understanding why some products are deemed strategic by nation-states. First, these dual use

technologies frequently result in high market barriers and economies of scale for the actor who "discovered" the product. Taiwan Semiconductor Manufacturing Company's sophisticated semiconductors could serve as an excellent example. Once Taiwan developed its factories and gained a comparative advantage, no other player could compete with its market share.

Second, as Ding and Dafoe point out, the actor who controls the strategic asset can use its scarcity to its advantage by reducing supply and demanding concessions in exchange. This is not the first time a similar situation has occurred. In October 1973, the Organization of Arab Petroleum Exporting Countries imposed a total oil embargo on the countries that had supported Israel during the Yom Kippur War, resulting in significant stagflation. A recent example is the system of export limitations imposed by the United States, the Netherlands, and Japan to prevent China from gaining access to semiconductors, as each country has a strategic stake in the semiconductor supply chain and benefits from it.

Third, these technologies can be transferred from civilian to military applications, making them dual use. On this, it is timely to recall Robert Jervis' security dilemma, in which country A enhancing its security causes country B to fear for its own, resulting in an arms race and escalation. The dilemma is impossible to avoid when two conditions are met: 1) it is difficult to discern between offensive and defensive weaponry, and 2) the offensive has an edge. According to these two axioms, the security problem is most likely to occur. Revisiting the realist theory behind this concept may help us to understand why dual-use technologies increase the security dilemma. Dual use technologies such as semiconductors diffuse even further the distinction between offensive and defensive; however, the diffusion between civilian and military use adds another layer of uncertainty and mistrust in the picture.

Dual use technology, such as semiconductors, further blur the boundary between offensive and defensive; yet, the spread of civilian and military use adds another layer of uncertainty and mistrust to the picture.

Managing uncertainty and mistrust is one of the primary reasons why nations have typically managed these dual-use technologies through multilateral organizations

such as the Wassenaar Arrangement, a multilateral body that governs dual-use and defence goods (Wassenaar Arrangement, 1996). Countries agreed on international lists and export controls under Wassenaar to limit the spread of certain dual-use technologies. If countries A and B do not agree to ban these dual-use technologies, they will continue to spread and constitute a security risk. In this regard, trust-building processes for disclosing sensitive information between governments have been critical to determining which technologies can lead to military applications and limiting their proliferation.

However, since dual-use technologies add to this level of ambiguity and mistrust, the Wassenaar Arrangement is rapidly being viewed as outmoded. Moscow has been boycotting progress at Wassenaar since 2022. Furthermore, the White House's export prohibitions against China have exceeded the criteria agreed upon in Wassenaar. The United States has also pressed the European Union to take a tougher position against China because it supported Russia's non-lethal equipment parts, which include various dual-use technologies that are part of the Wassenaar agreement.

The examples also occur at a time when competition fueled by dual use technologies is gradually eroding other classic international institutions such as the World Trade Organization and the G20 (Alvarez-Aragones, 2024). As these multilateral organizations fail to address national security concerns, they are being replaced with more restrictive and mini-lateral structures spearheaded by the United States. Examples of this mini-lateral approach include the G7 and the US-EU TTC. Under this new environment of more restricted international cooperation, advances in semiconductors, artificial intelligence, and quantum technologies, among other dual use goods, are pressuring all political blocs to develop strategies for securing these dual-use technologies at the intersection of trade, technology, and security.

In a world where dual use technologies appear to secure supply chains as well as science and innovation, pursuing international projects and spaces appears to become more difficult. The securitization of these technologies and their supply chains is altering the world, bringing a new power dynamic and conceptions of trade

and technology. An important question for policymakers is whether dual-use technologies have influenced a shift in the post-Cold War international order or are simply a symptom of a larger tendency in our global system as we return to "geopolitics."

For years, people believed that defence was not a viable market for businesses. The widespread notion was that the Department of Defences (DODs) was confined to the big primes, which included Boeing, Lockheed Martin, Northrop Grumman, Raytheon, and General Dynamics. However, the future of defence in the United States is undergoing rapid technological transition.

So, what has changed exactly? The DODs now contracts with startups in all technology sectors that affect national security, including horizontal domains (e.g., information and analytics, data and systems) and vertical threat vectors across space, air, land, and sea.

Defence technology encompasses much more than rockets, tanks, and aircraft carriers. Defence technology encompasses all aspects of the Department of Defence and the larger national security infrastructure, including systems infrastructure, communications and intelligence technology, cybersecurity, advanced manufacturing, and innovation used on the battlefield and elsewhere.

This presupposes that the product can be dual-use, government-only, or currently commercial-only but will eventually expand to include government-focused features. Ultimately, this requires a defence-specific product, as well as defence-specific go-to-market and sales staff.

The Department of Defences have new objectives to overcome the classic "valley of death"; the long gap between when a technology is first developed and tested and when funds are available in the budget to produce and buy it. According to US Defence Secretary Lloyd Austin, the Pentagon has the potential to become "a true innovation ecosystem." Defence technology is key to this generational paradigm change, thus, technology companies should carefully explore adding the Department of Defence as a potential new customer.

In 2025, it is obvious that as geopolitical crises across the world worsen, encouraging greater innovation inside the DODs is an essential component of protecting our country and its allies. Collaborating with rising entrepreneurs to develop innovative solutions is a strategic strategy for our country to avoid the deadly predisposition toward all-out war when a dominating power is challenged by an emerging one (also known as the "Thucydides Trap"). Emerging entrepreneurs play an important role in keeping the Western World out of this trap, as innovation has historically been inextricably linked to democracy.

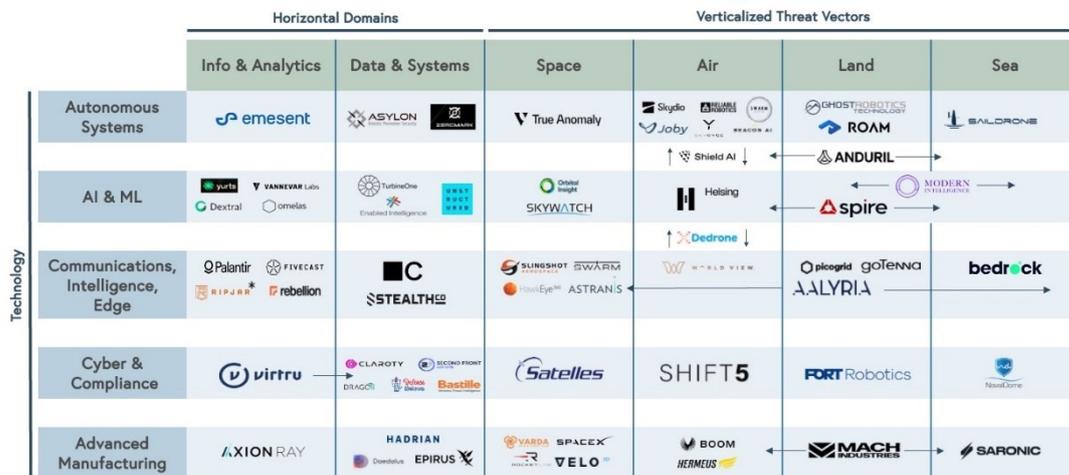
### 1.3.1 Five Market Opportunities for Defence Technology Startups

Many of the established defence industry businesses require no introduction. They include well-known companies like Boeing, General Dynamics, Lockheed Martin, Northrop Grumman, and Raytheon Technologies. Several of these primes have dominated the business for decades, some for nearly a century, and now generate tens to hundreds of billions of dollars in annual income.

However, during the last decade, a slew of groundbreaking startups has emerged to challenge the primary incumbents. Several of these entrants have successfully completed public and M&A exits for their venture backers, including Palantir and Rocket Lab. Both argue that younger military technology companies can scale well to reach excellent fundamentals and high valuation multiples.

Following in the footsteps of these instances, a diversified ecosystem of military tech firms has emerged in recent years, driven by strong market demand and creative founders eager to make a difference in national security.

## Bessemer's defense tech market map



⌘

Picture 5: main defence tech companies

Source: Bessemer's Venture Partner

By interviewing founders and experts navigating the substantial transformations in the defence industry, Bessemer has identified five core theses that it is especially eager to back with investment.

- Advanced AI/ML solutions will be the next frontier of national security. The defence community is not sitting idly by as the AI revolution takes over the consumer and commercial industries. Last year, the Department of Defence drew out and publicized its formal AI adoption strategy. Advancements and applications of artificial intelligence and machine learning will be critical to the national agenda and the defence community's daily operations. This might look like: Automating manual processes leads to increased productivity. High-quality output papers and work products. Faster assessment, which is crucial in real-time circumstances. More accurate insights to influence decisions.

Internal DOD champions see that entrepreneurs are not only producing the finest ideas in the space, but they are also willing and courageous enough to disturb the status quo in order to promote meaningful change. Across the

department, we've already seen the adoption of AI/ML applications in a variety of use cases, including Vannevar Labs for foreign text workflows, Dextral.ai for government procurement and sales automation, Axion Ray for engineering and quality analytics automation, and Yurts.ai for enterprise AI in search and documentation (Klempner, Rodriguez, & Swartz, 2024).

- The DOD is embracing the contemporary data and AI infrastructure stack, coupled with new network infrastructure advancements. The success of any modern organization, commercial or federal, is dependent on the insights gained or products developed from its data. The modern data stack is critical in the expanding field of defence technology since intelligence is derived from data in various formats (video, picture, text, speech, etc.). Various parts of the government are making significant expenditures to upgrade their data and AI infrastructure stacks, with essential requirements for both cloud and on-premises deployments. Startups such as Enabled Intelligence for data labeling, Unstructured.io for ETL for LLMs, and TurbineOne's MLOps platform are on the front lines of giving the defence community with the foundation to harness cutting-edge solutions to extract the maximum value from their data troves. Similarly, in the network infrastructure space, businesses like Aalyria are pioneering new ways to provide, connect, and orchestrate networks across organizations (Klempner, Rodriguez, & Swartz, 2024).
- A renewed emphasis on best-in-class cybersecurity solutions as table stakes. Best-in-class cybersecurity has become synonymous with strong national security in the digital age, and the need to enhance cybersecurity in the face of emerging threats grows. But significant progress has been made. For instance, early in 2022, the Office of Management and Budget published a White House Memorandum setting forth a Federal zero trust architecture (ZTA) policy, mandating agencies to satisfy particular cybersecurity requirements and objectives by the end of 2024. That same year, the Biden

administration released Executive Order 14028, which focused on improving the nation's cybersecurity.

Protection against all potential legacy and new attack surfaces cannot be overstated, and we see multiple technology giants stepping up to assist. From Bastille Technologies for wireless threat intelligence and Claroty for industry cybersecurity to Defence Unicorns for DevSecOps software for air-gapped networks and Virtru for zero-trust data-centric security, numerous startups are driving innovation and strengthening the government's defences against increasingly sophisticated and persistent threat campaigns (Klempner, Rodriguez, & Swartz, 2024).

- Verticalized solutions will serve as the foundation for the next generation of military technology titans. At Bessemer, we've witnessed vertical software revolutionize every industry, having invested in vertical SaaS leaders such as Procore, Shopify, Toast, and many more for over a decade. Each business industry has unique requirements that may not be fully met by horizontal solutions. With this in mind, we notice a similar pattern unfolding in the DOD environment. Each branch has distinct demands and hardware and software stacks, allowing budding defence tech businesses to enter the market by offering purpose-built solutions for vertical attack vectors before expanding into new verticals and teams. From ShieldAI for AI-piloted aircraft to Modern Intelligence for an all-platform all-sensor maritime awareness solution to Picogrid for land-based solutions to connect fragmented defence systems, we expect verticalized solutions for various segments of the DOD to expand in the coming years (Klempner, Rodriguez, & Swartz, 2024).
- We are in the early stages of autonomous systems attaining their full potential in the defence industry. As previously said, autonomous technologies have emerged as a critical paradigm for gaining a competitive advantage during wartime, and the military technology industry is still in its early stages. As the DOD continues

to investigate this technological paradigm, we anticipate more interest in companies developing autonomous robots and technologies.

The rise of defence tech decacorn Anduril is a testament to the adoption of unmanned aerial vehicles (UAVs), and we see many startups following suit, such as Skydio providing autonomous AI-powered drones, Saildrone for uncrewed surface vehicles, and Primordial Labs building voice-controlled autonomy software (Klempner, Rodriguez, & Swartz, 2024).

These companies are just a few examples of how the military sector is embracing autonomous technology on the battlefield and beyond. As another example, Hadrian is reinventing modern manufacturing, whereas Varda is the world's first orbital manufacturing and reentry platform.

The rapid deployment of modern technology into battlefields during conflicts between countries (rather than non-state actors) indicates a paradigm shift in military operations. Ukraine exemplifies this new reality and how defence systems have evolved in recent years. Ukraine is a case study that demonstrates three areas of defence technology that will require major and quick attention: 1) Unmanned aerial vehicles (UAVs); 2) cybersecurity; and 3) mass communication and social media.

- UAVs: Drones have shown to be invaluable for reconnaissance, targeting, and strike operations. They can attack one another if necessary and can help with the transfer of supplies and soldiers. Every month, Ukraine's armed forces lose 10,000 drones owing to Russian electronic warfare (EW). Clearly, today's conflicts involve a large number of unmanned aircraft systems.
- Cybersecurity: In Ukraine, cyberspace has emerged as an important battleground for offensive operations. This was demonstrated by a recent hack on Kyivstar, Ukraine's major telecom operator, which was one of the most significant cyber attacks in European history. The strike seriously disrupted Internet and mobile connections for millions of individuals, emphasizing the growing role of digital domains in modern conflicts.

- Mass communications: Social media and news platforms have also become hotly disputed venues, with the rapid dissemination of misinformation and disinformation posing threats to society. The distribution of information, as well as the factual accuracy of that information, has a fundamental impact on democracy. It is an opportunity for entrepreneurs to develop solutions that address both social and financial fraud, such as preventing and mitigating social engineering, cybercrimes (including propaganda), and emerging dangers to contemporary warfare.

Over 30 US entrepreneurs have already implemented goods in Ukraine, but the demand for improved technology solutions develops in the ever-changing realm of military operations. As the nature of conflicts evolves, the government must remain on the cutting edge. In this age of rising geopolitical tension and violence, it appears certain that US defence spending would increase significantly in the coming years. In surveying the defence tech landscape, Bessmer Venture Partners identifies five key qualities and dynamics it seeks when investing in these founders and their businesses.

1. High "defence IQ": While investors have typically tended to invest in dual-use innovations, we are delighted to support the frontier of entrepreneurs who monetize primarily (or entirely) through the government. Empirically, higher degrees of government concentration necessitate a greater ability to handle the complexity of government procurement procedures. This means that the founding team should have a high "defence IQ"—it wins the company respect and allows federal salesmen to communicate with contracting officers. A high defence IQ can manifest in a variety of ways, including former military service on active duty, civilian professional service, and relationships with defence agencies outside the government (for example, from a previous defence-focused investing employment).
2. Expansive TAM: The US defence budget for 2024 is \$886 billion, thus capturing even a small portion of this market would provide enormous opportunity for the next generation of defence technology businesses.

However, the defence budget is divided across the Department of Defence's hundreds of agencies based on a variety of technological focus areas. We're thrilled to support companies who can market solutions that address common needs across several branches of the DOD. Many of these enterprises can sell to other liberal regimes around the world. For example, the AUKUS (Australia, UK, and US) agreement entails strategic collaboration on technologies such as cybersecurity and AI.

3. Contracts are sticky, substantial sources of revenue: The ultimate goal for startups is to be part of a DOD Program of Record (PoR). A PoR is an explicit line item in the DOD budget that allocates cash (sometimes in the tens of millions of dollars) for the startup's technology. A PoR is also quite sticky, which means that the funds are often renewed year after year. Beyond the immediate cash benefit, being on a PoR provides unrivaled legitimacy and reputation. Such designation not only demonstrates a strong vote of confidence by a defence agency, but it also opens the door to significant, long-term support for other agencies and partners. The fastest time to a PoR is three to four years. Another sort of contract that is appealing to startups is the Indefinite Delivery, Indefinite Quantity (IDIQ) contract. An IDIQ contract allows for variations in the number and timing of orders over a specific period, as opposed to standard fixed-price contracts, which require the government to specify a set quantity of items or a particular scope of work. Under an IDIQ contract, the government agrees to buy goods or services as needed, up to a predetermined value or quantity. Startups under an IDIQ essentially get a hunting license for the duration of the IDIQ to discover defence agencies suffering from the challenges specified in the IDIQ and meet those needs without having to start a new procurement procedure each time. The DOD awards two types of contracts: PoRs and IDIQs. Others include cooperative research and development agreements (CRADAs) and OTAs (as previously stated). Alternatively, companies may choose not to sell directly to the DOD, instead acting as subcontractors to the huge defence primes.

4. Non-dilutive finance—The government provides excellent non-dilutive funding for companies. The most notable are Small Business Innovation Research (SBIR) awards, which have three "phases."

The purpose of Phase I is to demonstrate the viability of a proposed innovation. It usually entails a short-term endeavor to do research and show the concept's feasibility. Phase I SBIRs typically last less than a year and award less than \$250,000.

If a company successfully completes Phase I and establishes the feasibility of a technology, Phase II SBIRs strive to advance the innovation through more detailed R&D, testing, and prototype creation. More developed technology and enterprises can proceed directly to Phase II (D2P2) without first completing Phase I.

Only approximately 5% of companies advance from Phase II to Phase III SBIRs, creating another "valley of death" in selling to defence. However, unlike earlier phases, Phase III is not a direct component of the SBIR program. Instead, it signifies the technology's move to the commercial sector. Phase III funding is likely to come from non-SBIR sources (such as government contracts or private investment).

Some defence agencies have their own specific programs. For example, the Air Force's Strategic Funding Increase (STRATFI) and Tactical Funding Increase (TACFI) programs provide up to \$15 million to companies attempting to bridge the valley of death from Phase II to Phase III SBIRs.

5. Early traction in selling to the DOD: As previously stated, selling to the government is challenging, and the degree of difficulty varies every company. For example, while all corporations require FedRAMP certification, munitions-related businesses must also comply with the International Trade in Arms Regulation, which is a more stringent process. Some companies may require federal salesmen or forward-deployed engineers with FBI Secret/Top-Secret clearance. Bessemer does not rule out investments based on this type of sales friction; we prefer firms who

have made considerable progress in navigating the maze of regulations and processes required to sell their products.

Selling to the government involves complications and potential hazards, which many businesses do not want to bear. However, we believe it is a short-sighted perspective – the benefits can well outweigh the hazards.

A business-to-government approach can present significant challenges. Securing contracts often involves protracted negotiations that stretch over several years before yielding the large, multi-million-dollar agreements companies seek.

Revenue becomes difficult to predict, as government awards tend to arrive in irregular lumps—frequently culminating in a surge of sales around September, when the U.S. fiscal year closes—making quarterly forecasts particularly volatile.

On top of this, navigating the layers of bureaucracy within each federal agency adds complexity and slows progress, and shifting political winds and partisan priorities can further disrupt deal flow and extend sales cycles.

Adopting a business-to-government approach offers access to an extraordinarily large and stable customer: the U.S. defence and intelligence community, which commands an \$886 billion budget in 2024 and operates through dozens of branch-level entities that function much like independent Fortune 100 companies. This ecosystem not only provides a highly resilient revenue base—with virtually zero credit risk and strong resistance to economic downturns—but also rewards incumbents: once an initial contract is secured, expanding the scope of work is relatively straightforward, often resulting in exceptionally high net dollar retention. Moreover, partnering with the Department of Defence can accelerate product development by positioning the government as an ideal “beta” customer. Its non-dilutive funding programs, such as targeted grants, enable startups to refine technologies in real-world settings, enhancing both performance and credibility. As procurement offices become more open to working with emerging companies, landing a defence contract can also serve as a powerful go-to-market lever, helping innovators establish market leadership and fend off competitors.

Recent legal challenges by startups like SpaceX and Palantir illustrate how new entrants can even reshape the defence contracting landscape. SpaceX's successful 2014 lawsuit against the Air Force broke United Launch Alliance's longstanding monopoly on national security launches, while Palantir's 2016 victory compelled the Army to revise its acquisition processes to embrace commercial software solutions. Such breakthroughs have opened the door for a broader range of entrepreneurial ventures to compete for and win Department of Defence business. Other Transaction Agreements (OTAs) have played an important role in allowing unconventional contractors to sell to the government more easily, particularly since their expansion after 2015. Furthermore, measures have resulted in the formation of organizations such as the Defence Innovation Unit, AFWERX, and NAVAL X, which, beginning in 2015, promote collaboration between private enterprises and the DOD, facilitating startup interaction with the defence industry.

In light of these developments, the defence sector has opened its doors to a new generation of agile, mission-driven ventures. What was once viewed as the exclusive domain of legacy primes has evolved into a dynamic ecosystem where startups can both pioneer breakthrough capabilities and scale rapidly through government partnerships. By engaging deeply with DoD processes—from non-dilutive R&D programs to modernized procurement vehicles—entrepreneurs stand to not only accelerate their own growth but also strengthen national security at a critical juncture. As geopolitical pressures mount and technology cycles accelerate, cultivating this symbiosis between innovation and defence will be essential. Ultimately, the companies that master the art of translating cutting-edge research into deployable solutions will not only capture significant market share but will also play a pivotal role in safeguarding democratic values and strategic stability for years to come.

# Chapter 2: Technology Innovations and Israeli Defence Forces

## 2.1: The disruptive evolution of middle east geopolitical context

### 2.1.1: Regional Power Shift

The Israeli Defence Forces (IDF) are at a critical juncture, facing a complex and ever-changing geopolitical situation that requires not only military force but also decisive technological superiority. This necessity derives from a convergence of regional and global variables that threaten Israel's security and necessitate ongoing adaptation and innovation.

In recent years, the geopolitical environment surrounding Israel has evolved significantly, imposing several challenges on the Israel Defence Forces (IDF) that go far beyond traditional territorial defence and require a continuous process of adaptation and innovation on both the technological and strategic levels. Among the most prominent threats is that posed by Iran, whose nuclear policy and development of advanced missile systems have caused Israel deep concern. The possibility that Tehran may achieve advanced nuclear capabilities, juxtaposed with the continued enhancement of its missile capabilities, compels the IDF to invest in state-of-the-art air defence systems, as well as to develop deterrence and response strategies that can cope with any escalation.

### 2.1.2: Non-State Actors & Hybrid Threats

The Iranian threat is further complicated by Tehran's support for groups such as Hezbollah and other militias operating in Syria and elsewhere, creating a dangerous ripple effect that extends the risk on multiple fronts, both north with the Lebanese border and east with the Syrian theater. This network of armed and agile non-state allies requires the IDF not only to enhance conventional capabilities but also considerable preparedness for asymmetric and hybrid warfare operations.

The deteriorating and complex regional dynamics, marked by internal conflicts in neighbouring countries such as Syria and Lebanon, add additional layers of risk as these scenarios become fertile ground for the activities of extremist groups and armed militias, often backed by outside interests. Instability in neighbouring regions has prompted Israel to review and adapt its operational doctrines, integrating intelligence and rapid response capabilities in environments where the line between conventional and unconventional operations is increasingly thin. The creation of new alliances, as evidenced by the Abraham Accords, has been a double-edged sword: on the one hand, it has enabled strategic collaboration with some Arab countries, strengthening Israel's position in the region; on the other, it has exacerbated polarization, triggering a coordinated reaction by actors opposed to these agreements, with potential repercussions for regional stability and the ability to prevent new forms of conflict.

### 2.1.3 Cyber and Information Warfare

In addition to traditional dangers, the IDF must deal with the increased sophistication of hybrid warfare operations, in which technology and information manipulation play an increasingly important role. Cyberattacks on key infrastructure and attempts to sway public opinion through disinformation campaigns have shown a new dimension of warfare in which nonlethal actions can

have far-reaching strategic implications. This reality has driven the Defence Forces to create advanced cyber defence and digital intelligence capabilities, with major investments in technologies to defend information systems but also conduct offensive operations against possible attackers in cyberspace.

Another important part of the IDF's response to emerging challenges is technological progress. The necessity to preserve a strategic advantage has resulted in significant investments in air defence systems like the Iron Dome, as well as in the development and integration of emerging technology like drones and robotics. These increasingly advanced instruments are used for both reconnaissance and targeted strikes, resulting in higher precision and speed of response in asymmetric conflict circumstances. As a result, technological innovation has become an essential component of the IDF doctrine, which must coherently integrate traditional capabilities with digital and autonomous ones to respond effectively to a quickly changing environment.

#### 2.1.4: The Gaza War

Another element that marked a turning point in the evolution of the Israel Defence Forces is the the ongoing war with Gaza. This fight served as a key test case for the IDF's operational capability and strategic flexibility, revealing both strengths and opportunities for growth. During the fight, the complexity of the operational circumstances, which included densely populated urban surroundings, and a large network of underground tunnels used to marshal attacks and counterattacks, necessitated fast modification of military tactics. Israeli forces had to balance the need to neutralize enemy threats with the need to limit civilian casualties, a challenge that highlighted the importance of strategic planning and precision operations. Moreover, the experience in Gaza underscored the relevance of electronic warfare and the ability to dominate cyberspace, as both aspects played a crucial role in coordinating operations and countering the adversary's propaganda and disinformation strategies. The conflict accelerated the process of technological

renewal within the IDF, prompting the military command to further invest in advanced intelligence systems, drones, and electronic warfare tools to ensure a greater capacity for real-time data collection and analysis. Lessons learned on the ground underlined the importance of improved interoperability among the various operating units, as well as closer cooperation with international partners for intelligence exchange and strategic support. At the same time, the severity of the battle has highlighted the significance of continuous training and changes to operational doctrines to ensure that the armed forces can respond quickly and effectively in crises.

#### 2.1.5: The conservation of the technological superiority

In this context, maintaining a technological advantage emerges as a crucial strategic element for Israel. In a landscape where threats are multiplying and diversifying, technological superiority not only represents a strengthening of offensive and defensive capabilities but also forms the basis for a timely and targeted response to potential attacks. The ability to monitor adversaries' activities in real-time, to intercept premonitory signals, and to respond with surgical precision makes it possible to prevent escalation and contain crises that could escalate into larger conflicts. Investing in advanced cyber security systems, data collection and analysis technologies, and secure communication platforms has made it possible for Israel to anticipate and neutralize threats before they materialize, turning technology into a true deterrence tool. This strategic advantage also translates into the ability to conduct offensive operations in cyberspace, where the ability to target enemies' critical infrastructure acts as a deterrent and strengthens Israel's position in the global context. Experience in the field, particularly during the conflict in Gaza, has shown how mastery of the information domain and the use of emerging technologies can make the difference between a successful operation and a crisis that gets out of control.

Israel's technological leadership is not limited to the military sphere but also extends to the civilian sphere, where an innovative ecosystem formed by the collaboration of industry, academia, and military institutions fosters the development of advanced solutions capable of responding to changing national defence needs. This convergence of the public and commercial sectors has established an innovative culture that allows obstacles to be turned into opportunities, improving the state's resilience and ensuring a flexible and coordinated response to crises. In an era when the rapidity of change and sophistication of threats require a response that combines military, cyber, and strategic capabilities, continuous technological upgrading becomes not only an operational choice but an existential necessity to protect one's interests and maintain strategic balance in the region.

In this sense, dual-use technology has strategic value for Israel that extends far beyond developing military weapons. This strategy, which incorporates ideas and technology applicable to both civilian and military domains, is a significant strength for the state's resilience and creativity (Alvarez-Aragones, 2024). The technology's dual-use nature enables Israel to capitalize on synergies between the civilian sector, particularly high-tech and industrial innovation, and the military, resulting in a dynamic ecosystem capable of addressing complex and ever-changing challenges.

One of the most important characteristics of the dual-use strategy is its capacity to speed the development and deployment of cutting-edge technical solutions. In a global market where competition is severe and breakthroughs develop quickly, Israel's ability to integrate technologies with civil and military applications allows it to stay ahead of the curve. The same technologies that drive sectors such as information technology, telecommunications, robotics, and artificial intelligence can be used to improve the operational capabilities of the Israel Defence Forces (IDF), ensuring that technological advances are quickly translated into strategic advantages on the ground.

Dual-use technology also has serious national security implications. Critical infrastructures and communication networks, which are essential in both residents'

daily lives and military operations, must be safeguarded against more complex threats. The capacity to create modern cybersecurity solutions and surveillance systems that can be utilized in both civilian and military settings offers integrated and robust protection that can mitigate risks and prevent assaults (Ding & Dafoe, 2021). This dual usage allows for the development of a layered defence in which technological advancements serve as a shield against external threats, bolstering Israel's strategic position both within its borders and in the international arena (Barlaw, 2025).

Another critical factor is training and the sharing of expertise. Incorporating dual-use technology encourages collaboration across academic institutions, research centers, and private firms, creating a fertile environment for idea exchange and novel applications. This collaboration between universities, start-ups, and the industrial sector has allowed Israel to create a globally recognized innovation ecosystem capable of attracting investment and talent from all over the world (Startup Nation Central, 2024; Eliezer, n.d.). The transfer of information and technologies generated in the civil sector to the military, and vice versa, improves the state's ability to adapt fast to change and respond effectively to crises.

Furthermore, the dual use strategy has a huge impact on Israel's reputation and global projection. Being recognized as a technology innovation leader with solutions applicable to both civil and military markets boost the state's diplomatic and strategic position. Such acknowledgment helps to build international collaborations, facilitates the sharing of knowledge, and strengthens strategic relationships, all of which contribute to national security. The ability to export new technologies and recruit strategic partners is critical to maintaining the balance of power in today's global climate, where technology is increasingly important (Ding & Dafoe, 2021).

Finally, the utilization of dual-use technology enables Israel to reduce the risks associated with its reliance on external suppliers and global markets. The production and development of technologies that may be applied in a variety of areas lessen the state's susceptibility in times of stress or economic crisis, resulting in greater strategic autonomy. In this approach, Israel can preserve its inventive

potential while also protecting its interests, assuring continuity and stability during times of geopolitical upheaval.

To summarize, dual-use technology is important to Israel on several levels: it accelerates technological growth, boosts national security, encourages civil-military collaboration, contributes to international reputation, and ensures more strategic autonomy. This integrated approach, which converts civic inventions into weapons of power and defence, is a critical component of the state's security and development policy, allowing it to adapt dynamically and proactively to the challenges of a rapidly changing geopolitical landscape.

## 2.2: Innovation challenges for the Israeli Defence Forces

### 2.2.1: Institutional Reform: AI & Autonomy Administration

In recent years, the Israel Defence Forces (IDF) have embarked on an ambitious transformation to preserve their qualitative military edge amid a rapidly evolving threat landscape. At the core of this effort is the Artificial Intelligence and Autonomy Administration, established on 31 December 2024 under the Ministry of Defence's Directorate of Defence Research & Development (DDR&D), which was created to unify disparate research streams and accelerate the fielding of AI-driven capabilities across land, air, naval, intelligence, and space domains (Felstead, 2025; Euro-sd, 2025). This landmark reorganization marks the first new administration in two decades. It reflects a deliberate shift from isolated prototyping toward a holistic, lifecycle-oriented approach in which algorithms, unmanned platforms, and human operators operate as tightly integrated teams.

This institutional innovation has been partly driven by the dramatic proliferation of low-cost, commercially available drones wielded by nonstate actors, whose small

radar cross-sections and unpredictable swarm tactics have exposed critical gaps in traditional point-defence systems (Wall Street Journal, 2024).

### 2.2.2 Directed-Energy & Air Defence (Iron Beam)

In response, the IDF has fast-tracked the development of the Iron Beam directed-energy laser system to complement kinetic interceptors such as Iron Dome, aiming to counter massed drone attacks with virtually unlimited “magazine depth.” Yet, early field trials have revealed significant challenges, beam attenuation in adverse weather, power supply constraints, and questions over long-range terminal accuracy, which have postponed full operational deployment beyond its original 2025 target (Magnuson, 2025; Axios, 2024).

### 2.2.3 Unmanned Ground Systems & Urban Operations

Beyond the skies, the IDF has invested heavily in robotic ground vehicles and demining platforms to mitigate risks in urban and subterranean combat theaters. Deployments in Gaza have demonstrated the value of lightweight unmanned ground vehicles equipped with lidar and multispectral sensors for tunnel mapping and improvised explosive device detection, but they have also underscored persistent limitations in battery endurance, terrain agility, and human-machine interface design during high-pressure engagements (Tech Tonic, 2025; Reuters, 2025). Overcoming these hurdles requires not only technological refinement but also user-centered engineering, sophisticated simulation environments for operator training, and open communication protocols to avoid opaque “black-box” behaviors in mission-critical algorithms.

## 2.2.4 Cybersecurity & C2 Resilience

Simultaneously, the IDF's expanding network of interconnected systems, ranging from frontline command posts to unmanned platforms and satellite links, has broadened its cyberattack surface. Advanced adversaries now target critical data flows and command-and-control architectures through sophisticated intrusion campaigns, compelling the implementation of state-of-the-art cryptographic frameworks and real-time anomaly detection tools. Balancing robust cybersecurity measures with the need for ultra-low latency data exchange remains a formidable challenge, as overly stringent defences can introduce delays detrimental to battlefield decision cycles (Sobelman, 2025; Springer, 2024).

Organizational and legal complexities add further friction to Israel's innovation ecosystem. While the "startup nation" ethos fosters close collaboration between the IDF, technology firms, and academic institutions, facilitated by vehicles like the Innovation Accelerator and MAGNET consortium, the pathway from proof-of-concept to field-certified system is encumbered by rigorous security reviews, export controls, and patent regulations that can deter foreign investment (JNS.org, 2025; Barlaw, 2025). Interoperability requirements with U.S. defence systems, essential for joint operations, layer additional compliance demands on procurement cycles and technical integration efforts.

Ethical and legal considerations loom equally large as AI-aided targeting and autonomous weapons move closer to operational reality. The IDF has convened multidisciplinary panels of legal scholars, ethicists, and technologists to draft guidelines ensuring that human judgment remains central to lethal decision-making, yet debates persist over accountability, transparency, and adherence to international humanitarian law (Financial Times, 2025; Time, 2024). The tension between reducing collateral harm through precision AI and the risk of "automation bias" underscores the need for rigorous oversight frameworks that evolve in step with technological advances.

Looking forward, the IDF's ability to sustain its strategic edge will depend on integrating flexible innovation processes that bridge laboratory breakthroughs and combat-ready applications. This entails expanding war-gaming facilities to simulate multi-domain scenarios, adopting modular open-architecture systems to facilitate plug-and-play upgrades, and deepening human-machine teaming doctrines through iterative field exercises. Equally important is securing stable funding streams, estimated at some 4 billion shekels for AI infrastructure alone, to shield defence R&D from political and economic fluctuations while preserving the agility that has defined Israel's approach to national security (Sobelman, 2025; JNS.org, 2025). Only through a holistic strategy, one that weaves together advanced algorithms, autonomous platforms, cybersecurity, ethical governance, and organizational agility, can the IDF navigate the shifting dynamics of twenty-first-century warfare and maintain its role as a global leader in defence innovation.

## 2.3 Technology Innovations and Israeli Defence Forces

### 2.3.1 Deep Tech as a source of innovation for the IDF

Deep tech is also playing an increasingly important role in the defence context, and Israel, with its dynamic innovation ecosystem and focus on national security, is at the forefront of this technological revolution.

The Deep tech research, and in general all the tech research in the Army sector, aims to the improvement of technological and strategic superiority to provide a decisive technological advantage and reduce dependence on obsolete or vulnerable technologies. Just concluded war with Gaza and Libano, and the perennial state of tension with Gaza made this an unavoidable necessity for Israel, not just for surviving as a state but also for counting in the international scene.

Deep Tech's impact on the Israeli armed forces is obvious in several crucial areas. Artificial intelligence (AI) is used to evaluate enormous volumes of data from sensors and drones, thereby boosting military operations' efficiency, target recognition, and real-time decision support. Robotics plays an important part, with robots employed in dangerous missions including surveillance, demining, and battle to reduce the risk to soldiers. Cybersecurity is a significant focus, with Deep Tech tools being deployed to defend critical infrastructure from cyberattacks. Finally, advanced material research has resulted in the development of new military vehicle armor, sensors, and propulsion systems, which improve protection, mobility, and firepower.

We, therefore, look at how Deep Tech is shaping Israeli defence, with a focus on the companies involved, the technologies used, and the impact of these innovations on national security.

The Israeli landscape is characterized by a robust ecosystem of start-ups and technological enterprises, as well as a significant emphasis on national security. Leading businesses such as Rafael Advanced Defence Systems, Elbit Systems, and Israel Aerospace Industries (IAI) are at the forefront of developing Deep Tech applications for defence.

Rafael Advanced Defence Systems Ltd. is a renowned Israeli defence corporation that specializes in the research, manufacture, and maintenance of advanced technology and integrated systems for military use. It was established in 1948 as the National Defence Research and Development Laboratory of the Israeli Ministry of Defence and was formed as a limited liability company in 2002.

Rafael created the PUZZLE Suite, a system that tackles the complicated reality of today's battlespaces by delivering a comprehensive, AI-based Decision Support System that uses massive amounts of data to generate fused transdisciplinary intelligence. The system integrates data from a variety of sensor sources, including VISINT (Visual Intelligence, visual data such as photos, satellite imagery, and videos, etc.) and SIGINT (Signals Intelligence, communications/electronic systems), to produce a comprehensive and filtered dataset using advanced AI and Machine

Learning algorithms. The system's ability to rapidly collect and evaluate information empowers military decision-makers, reducing operating timelines and increasing operational effectiveness.

In recent years, armed forces worldwide have made significant investments in advanced sensor technology to improve their intelligence-collecting capabilities. However, the increasing volume of data collected from these sensors frequently exceeds the capacity for timely analysis and utilization. Notably, a considerable amount of the data stays unexplored, resulting in inefficient target development and, in certain cases, wasteful deployment of expensive armaments.

The PUZZLE is composed of various components. The SIGNAL.AI component, which is intended for use by SIGINT analysts, spans tens of thousands of networks and uses the entire range of RF (radio frequency) input to identify, categorize, and locate adversary networks. The IMILITE component is a national-level IMINT and GEOINT system that integrates all assets and produces high-volume, multi-sensor products to provide a unified intelligence picture. The TARGETS component allows targeteers to submit transdisciplinary queries over vast volumes of data, which are developed by skilled analysts using an innovative visual exploitation tool. The FORCE component is a net-centric, national-level effector hub that connects all units across fronts and arenas. It generates dynamic, weighted lists, links request to effectors, and develops an end-to-end plan. Now let's examine more in-depth the various components of the Puzzle system.

SIGNAL.AI is an AI-powered exploitation system for SIGINT analysts. Using cutting-edge AI technologies, this decision support system converts massive amounts of data into usable actionable insights, allowing fewer analysts to make faster and more accurate judgments. Designed for operational situations with tens of thousands of networks and several analysts working simultaneously, the system allows for the exploration of all RF input, both content and non-content. It discovers communication networks in Areas of Interest, aids in the classification of adversary networks, creates combined geographic epicenters, offers SNA (System Network Architecture) analysis tools, detects anomalies, and issues alerts.

IMILITE is an AI-powered combat-proven Imagery Intelligence (IMINT) system. IMILITE is intended to address the current global security issues and support the entire intelligence operations cycle. The system provides quick access to pertinent visual data and integrates many visual data sources to create a full situational picture of dangers, opportunities, and courses of action. IMILITE develops novel solutions for utilizing visual and geospatial data in real-time operations, intelligence research, and strategic decision-making processes. It is a real multi-sensor system that integrates all visual collection assets for unified operation and facilitates the integration of old and future ISR (Intelligence, Surveillance, Reconnaissance) systems.

TARGETS is a combat-proven technology that supports the targeteer's entire operating cycle, finding the most relevant targets by leveraging high-volume information gathered from several data sources. The technology finds bottlenecks to increase efficiency, allows numerous real-time processes at once, and delivers an accurate image of the opponent. The Target Center allows the targeteer to do multi-domain queries across enormous volumes of diverse data, which are defined using an advanced visual exploration tool. All activities for each goal are recorded, allowing for real-time and offline analysis of target handling and the discovery of bottlenecks such as discrepancies between expected and actual targets, a shortage of resources, and fundamental causes.

FORCE is a powerful, network-centric, national-level effector hub that maximizes the utilization of all effectors, allowing for target neutralization at the lowest possible cost and risk to fighters and civilians. The system, which is connected to all units across all fronts and arenas, leverages today's most powerful technologies to aid Targeteers by quickly reviewing and prioritizing requests and providing dynamic weighted lists. It processes massive amounts of data in near-real time, matching attack requests with specific types of weapons, firepower, ammo, position, route, and so on. The system creates a plan that executes the commander's policies and is approved by people before being carried out.

Elbit Systems is a significant Israeli military and defence technology business that was established in 1966. Its headquarters are in Haifa, Israel. The company offers a diverse range of products, including avionics systems, unmanned aerial vehicles (UAVs), communication, surveillance, and reconnaissance systems, as well as electro-optical and electronic warfare solutions.

Elbit Systems focuses on electronic warfare systems, drones, and AI-based command and control systems, while IAI develops artificial intelligence technology for satellite image processing and aerial surveillance.

Elbit Systems announced a considerable increase in earnings in the third quarter of 2024, thanks to the increased demand from international customers and the Israeli military in reaction to the just concluded wars with Hamas in Gaza and Hezbollah in Lebanon. Earnings per share grew to \$2.21 from \$1.71 a year ago, as revenue increased from \$1.50 billion to \$1.72 billion, primarily due to sales of drones and aerospace systems. The company's order backlog has reached \$22 billion, with international customers accounting for two-thirds of the total.

Elbit Systems is firmly committed to the deep tech industry, creating breakthrough technologies domestically and through strategic collaborations. Incubit Ventures, the company's technological incubator, plays an important role in this approach by investing in early-stage deep tech start-ups. Incubit offers these entrepreneurs strategic investments, providing funds of approximately \$1 million for the first two years of selected startups, as well as extensive support, such as office space, legal, marketing, and business guidance.

Elbit Systems experts support the startup evaluation process by assessing each team's technological distinctiveness, risks, and time-to-market. This evaluation investigates the concept's underlying technology, validates its scientific and commercial viability, identifies potential synergies with Elbit's areas of interest, and analyzes the proposing team. Although Incubit is primarily interested in civil applications, any connection with the homeland security market is viewed as an added value. Once selected, the start-ups are coached through the development of a

thorough work plan, which is presented to Incubit's investment committee and then to the Israeli Innovation Authority investment committee.

Another important tool for Israel in the technological race is Unit 8200, Israel's elite military intelligence agency, which we will talk about later in much more depth. Unit 8200 is the Israel Defence Forces' largest single military outfit, akin to the National Security Agency in the United States or the GCHQ in Britain. It is descended from the early codebreaking and intelligence groups established in 1948 when Israel was founded. In addition to spying on Palestinians in the occupied West Bank and Gaza, it operates in all locations, including conflict zones, and works closely with military command headquarters during wartime. Its personnel are selected from young people in their late teens and early 20s, some identified from highly competitive high school programs, and many of whom have gone on to careers in Israel's booming high-tech and cybersecurity sector.

They collect and analyze signals intelligence and cybersecurity and use AI algorithms to evaluate massive volumes of data in real-time. This enables Israel to identify and destroy threats before they appear, making it one of the most secure countries in cyberspace. Israel's latest military performance is there for all to see, and it is largely due to artificial intelligence that Israel has been able to mitigate the number of casualties among its military personnel. According to several Israeli media outlets, since the conflict began on Oct. 7, 2023, the Tel Aviv military has reportedly used artificial intelligence (AI)-based software to identify and target tens of thousands of targets suspected of belonging to the ranks of Hamas or other terrorist groups in the Gaza Strip and Lebanon. The use of AI has been admitted, in the early months of 2024, by the Army's officers to enhance target detection, intelligence analysis, adaptive scenario processing, and command and control streamlining. On the other hand, integrating AI-based technologies to manage the massive amounts of data that are currently flooding the military environment and battlefield has become critical not just for the individual security of the soldiers, but also for managing the large volumes of data that are now flooding the military environment has become indispensable. AI-powered systems can filter through

massive amounts of data and identify relationships that humans might otherwise miss. This capacity is very important for threat identification, counterterrorism, and information-collecting missions. By automating the collecting, analysis, and reaction processes, Israel has developed an AI-powered surveillance and intelligence infrastructure that drastically minimizes human error while increasing operational efficiency.

A very important AI-powered database of the IDF, according to an investigation of the +972 Magazine and Local Call, a Hebrew language independent information site, is the Lavender. Operated by Unit 8200, it is technically a smart database that combines and sorts information on people who may be members of Hamas or other organized armed groups. Lavender's database appears to be extensive, which is understandable given that Hamas's al Qassam forces numbered 30-40,000 members when the most recent clashes erupted. Islamic Jihad adds a few thousand fighters. This program analyzes a wide range of data, including photos, biographical data, and WhatsApp contacts, to create a list of suspected militants, mainly affiliated with the military wings of Hamas and Palestinian Islamic Jihad. According to +972 and Local Call, the army relied almost solely on Lavender during the initial weeks of the battle, registering up to 37,000 Palestinians as suspected militants and their residences for potential air strikes.

Lavender, as a broad database, may theoretically serve a variety of applications. Some are unrelated to targeting, such as determining which individuals should be detained or questioned. It could also be useful when organizing an operation in a specific area to identify organized armed group members or other persons of interest, as well as to gauge the enemy's density in that area.

During the early stages of the conflict, the military allowed officers broad permission to use Lavender's target lists, with no requirement to thoroughly analyze why the machine made those decisions or review the underlying intelligence material on which they were based. According to one source, human staff frequently functioned as a "rubber stamp" for the machine's decisions, and it normally spent only "20

seconds" on each target before authorizing a bombing, just to ensure that the target indicated by Lavender was male.

In the Israeli army, the term "human target" refers to a senior military officer who, under the guidelines of the army's Department of International Law, can be murdered in his private residence even if civilians are present. Intelligence sources told +972 and Local Call that during previous Israeli wars, because it was a "particularly brutal" way to kill someone, often killing an entire family along with the target, these human targets were carefully marked, and only high-level military commanders' homes were bombed to maintain the principle of proportionality under international law.

However, following October 7, when Hamas-led militants launched a murderous attack on southern Israeli villages, murdering over 1,200 people and capturing 240, the army, according to sources, took a drastically different strategy. As part of Operation Iron Swords, the army determined to treat all Hamas military wing agents as human targets, regardless of rank or military value. That changed everything.

The new policy also presented technical challenges for Israeli intelligence. In previous wars, an officer had to go through a complex and lengthy "indictment" process before authorizing the assassination of a single human target: checking for evidence that the person was indeed a high-level member of the Hamas military wing, finding out where he lived, his contacts, and finally knowing when he was home in real-time. When the target list was limited to a few dozen senior officials, intelligence personnel could perform the process of indicting and locating them on their own.

However, as the list was expanded to include tens of thousands of lower-level agents, the Israeli army decided it needed to rely on automated software and artificial intelligence. According to sources, the role of human personnel in incriminating Palestinians as military agents has been delegated, with the IA handling the majority of the workload. According to four sources who spoke with +972 and Local Call, Lavender, which was developed to create human objectives during the ongoing war, has dispatched over 37,000 Palestinians as "Hamas militants."

"We did not know who the junior operatives were, because Israel did not routinely track them before the war," an IDF officer explained to +972 and Local Call, explaining the rationale behind the development of this targeting machine for the current war. "They wanted to allow us to attack automatically. This is the holy grail. Once you switch to automaticity, target generation goes crazy."

According to sources, approval for the automatic adoption of Lavender's kill lists, which had previously been used only as an auxiliary tool, was granted about two weeks after the war began after intelligence personnel "manually" checked the accuracy of a random sample of several hundred targets chosen by the artificial intelligence system. When the sample revealed that Lavender's results were 90% accurate in determining an individual's Hamas allegiance, the military approved the system's wider deployment. From that point forward, sources stated that if Lavender determined that a subject was a Hamas member, they were asked to treat it virtually as a command, with no obligation to independently investigate why the computer had reached that judgment or to review the raw intelligence material.

"At 5 a.m., the air force would bomb all the houses we had marked," Bob stated. "We evacuated thousands of people. We didn't go through them one by one; instead, we programmed everything into automatic systems, and as soon as one of the marked individuals entered the residence, he was immediately targeted. "We bombed him and his home."

The deadly results of this easing of restrictions in the initial phase of the war have been staggering. According to data from the Palestinian Ministry of Health in Gaza, which the Israeli army has relied on almost exclusively since the beginning of the war, Israel has killed about 15,000 Palestinians-almost half the death toll so far-in the first six weeks of the war.

The Lavender program analyses data collected from a mass surveillance system on the majority of the Gaza Strip's 2.3 million population before rating and ranking the possibility that any given person is involved in the Hamas or JIP armed branch. According to sources, the system rates practically every person in Gaza on a scale of 1 to 100, indicating the possibility that he or she is a terrorist.

According to the sources, Lavender learns to recognize the traits of known Hamas and JIP operators, which were fed into the computer as training data, and subsequently to identify these same characteristics in the general population. An individual with multiple incriminating qualities earns a high score and immediately becomes a prospective target for elimination.

In the novel "The Human-Machine Team," the current commander of Unit 8200 advocates for such a system without mentioning Lavender. The commander laments that human troops are a "bottleneck" that inhibits the army's capacity during a military operation, stating, "We cannot process so much information." It doesn't matter how many people are assigned to generate targets throughout the battle; you can't produce enough targets each day."

He proposes artificial intelligence as a solution to this problem. The book provides a concise method for creating a "goal machine," similar in description to Lavender, using AI and machine learning algorithms. The guide provides various instances of the "hundreds and thousands" of traits that can improve an individual's rating, such as joining a Whatsapp group with a known militant, switching cell phones every few months, and often changing addresses.

Visual information, cellular information, social media connections, battlefield information, phone contacts, and photos. While humans initially choose these features, the commander says, the machine will eventually be able to recognize them independently. This, he claims, may allow the military to manufacture tens of thousands of targets, but the decision to attack them remains human.

Another AI system widely used by the IDF is "The Gospel", this system is differentiated from "Lavender" for not being used to identify human targets but being limited to directing intelligence analysts to information about "objects" (such as buildings and other structures) that may qualify as military objectives.

The IDF defines Gospel as analyzing databases containing information entered by intelligence analysts from a variety of sources. These databases are most likely derived from satellite photography, drone footage, cyber intelligence, phone intercepts, human intelligence, open-source material, and operational reports.

According to reports, these facts are regularly updated as new information becomes available. It is a process comparable to what a human analyst would do. Gospel, on the other hand, filters information considerably faster and more reliably, ensuring that all accessible information on a prospective military objective has been considered. Consider it a mechanism that "connects the dots" for intelligence analysts.

Furthermore, targeted analysts have access to the raw intelligence that underpins a Gospel-generated suggestion. Analysts can then independently assess the quality of the information and the correctness of determinations like the object's position and kind. They may also consider additional pertinent information that is not in the system.

The implementation of Deep Tech has resulted in a major improvement in the Israeli military forces' situational awareness, allowing commanders to make more informed judgments. Automation and robotics have improved operational efficiency by freeing up human resources for other tasks. The deployment of robotics and autonomous systems in dangerous operations has reduced human losses, while ongoing investment in Deep Tech R&D has helped Israel to maintain a technological advantage over its rivals.

### 2.3.2: The deep tech innovation ecosystem in Israel

In 2024, Israel cemented its status as a worldwide scale-up powerhouse. Despite continued war and geopolitical concerns, the tech industry accomplished significant milestones, including surprising investment levels, high-value M&A transactions, and excellent performance by public businesses. This resilience originates from Israel's unwavering commitment to innovation, which is strengthened by the ecosystem's increasing maturity and sophistication. Scaling is no longer limited to unicorns. Growth is currently driven by strategic acquisitions, record-breaking fundraising rounds, and growing global integration, with Israel functioning as a hub for multinational R&D. However, maintaining this

pace necessitates tackling crucial issues such as promoting academic research, early-stage innovation, preparing for the AI revolution, and preserving long-term economic stability.

In a difficult and dynamic year like 2024, Israel's innovation ecosystem once again showed its endurance and adaptability. Despite domestic uncertainties and geopolitical tensions, one key insight emerges: global dynamics, particularly US investment trends, consistently outweigh local challenges, allowing Israel to thrive as a global hub for innovation, investment, and leadership in critical sectors such as cybersecurity. Equally crucial is the realization that Israel's innovation ecosystem has progressed beyond its status as a production line for early-stage firms. It has grown into a scale-up powerhouse, aided by the active participation of big international corporations.

Let's start this deep tech innovation ecosystem analysis with some data taken from the "Startup Nation Central Annual Report 2024"

- **Economic Contribution:** The Israeli tech ecosystem, with a GDP share double that of the U.S. tech sector, led Israel's economic growth with a 2.2% increase in high-tech GDP (Q1-Q3 2024), while the overall economy contracted by 1.5%.
- **Private Funding Growth:** Israeli tech companies raised over \$12 billion in 2024, a 27% year-over-year increase.
- **Global Perspective:** This trend in funding rounds and amounts is aligned with the U.S. VC trends and outpaced Europe and Asia.
- **Early-Stage Activity:** Early rounds (pre-seed to Series A) accounted for 80% of deals, while late-stage funding saw its dollar volume peak, nearing 2021 levels.
- **MNC Activity:** Multinational corporations increased M&A activity in Israel, including several high-value deals, while their private investments showed steady performance throughout 2024.

Israel's technology economy is undergoing a significant metamorphosis, from a startup-centric paradigm to a scale-up powerhouse. This progression is

characterized by larger fundraising rounds, a growing number of mature enterprises, and an increase in acquisition-driven exits. Israeli scale-ups are no longer only acquisition targets; they have evolved into active acquirers, fostering larger ecosystems and promoting long-term growth. The scope of these purchases demonstrates not just the enormous capital involved, but also Israeli companies' desire to expand and compete on a worldwide scale.

The market success of Israeli technology businesses reflects this trend. An equal-weight index of the top 70 Israeli IT firms (valued at more than \$50 million) trading on NASDAQ increased by 15.8% in 2024, outperforming the NASDAQ 100 equal-weight index, which increased by 9.4%. Furthermore, Israeli public companies listed on NASDAQ have proven resilience, constantly increasing revenues and productivity in the face of external obstacles. The scale-up ecosystem's strength is demonstrated by the 15 mega-rounds recorded in 2024, which totaled \$4 billion and accounted for 41% of overall funding, a major increase from 2023's nine rounds and \$2 billion (22%).

Israel continues to dominate the global cybersecurity environment, with private finance accounting for more than 40% of US cybersecurity efforts. Israelis founded half of the world's top ten cybersecurity companies, with seven still maintaining local R&D labs. Furthermore, all ten industry heavyweights have bought Israeli cybersecurity startups in recent years, demonstrating the country's critical position in global innovation. The median fundraising round in cybersecurity was more than double the average across Israel's IT ecosystem, indicating investor confidence in the industry. The country's cybersecurity expertise is also intimately linked with its defence sector, addressing challenges ranging from state-sponsored cyberattacks to vital infrastructure protection, cementing Israel's leadership in security and defence.

2024 was also a record year for mergers and acquisitions in Israel, with acquisition-driven departures setting new highs. Israeli companies played critical roles in big transactions, demonstrating their growing strategic importance and financial power in the global market. Multinational firms with R&D and innovation activities in Israel

have dramatically boosted their acquisition activity, bolstering the country's status as a worldwide technology and innovation hub.

While Israel's IT industry continues to show extraordinary strength, numerous concerns must be addressed to assure long-term success. A global fall in startup formation is having an influence on Israel's innovation pipeline, reducing the number of new entrants and limiting the diversity of future chances, even though current companies remain of high quality. Furthermore, a drop in the number of financing rounds is stifling early-stage innovation and reducing the pipeline for new innovations. To counteract this, appropriate grants and incentives could help provide more chances for new businesses.

Judicial and economic uncertainty, combined with regional instability, pose serious threats to Israel's position as a worldwide technology hub. Investor confidence is harmed by uncertain judicial changes and economic policies, while geopolitical turmoil heightens perceived risks for international partners. Clear long-term strategies will be critical to retaining Israel's leadership in the global technology ecosystem. At the same time, Israel's innovation sectors are under strain, with lower support for startups in developing domains jeopardizing the country's usually diversified spectrum of enterprises. Providing tailored incentives to investors and international firms could help to sustain growth in a variety of areas.

Finally, as AI drives a new industrial revolution, Israel must ensure that it has the resources, talent, and R&D capabilities to remain competitive. Proactive government assistance, strategic focus, and adaptable regulation will be critical to promoting growth in this quickly changing sector. Addressing these difficulties will be critical to Israel's ongoing success as a worldwide technology leader.

### 2.3.3: Israeli Innovation Funding Trends

In 2024, Israel's private funding was \$10.6 billion, a 28% increase over the \$8.3 billion reported in 2023. Accounting for yet-to-be-reported rounds and rounds with unreported quantities, overall fundraising is estimated at \$12.2 billion, up 31% from

last year's adjusted number (Appendix D). This development reflects a revived investor confidence in Israel's innovation sector, even though the area and worldwide markets remain uncertain. However, the recorded number of rounds fell for the second consecutive year, to 766 rounds in 2024, a 4% decrease from 2023 (Appendix E). This suggests a preference for larger, high-value investments, with investors concentrating their efforts on established enterprises and emerging sectors such as cybersecurity and business software.

The overall increase in finance highlights Israel's sustained position as a global leader in innovation and its capacity to attract large capital. Key industries like cybersecurity and business software continue to drive this performance, demonstrating the ecosystem's adaptability and resilience to changing market circumstances (*Startup Nation Central, 2024*).

The negative association between the number of rounds and total capital raised in the United States and Israel indicates a deliberate shift among investors toward fewer but larger investments in mature enterprises. As technology ecosystems evolve, capital is increasingly channeled toward companies with established revenue streams and great growth prospects. Economic uncertainty has exacerbated this trend, leading investors to concentrate on late-stage rounds, which are regarded as lesser risk. Furthermore, capital-intensive industries such as artificial intelligence and cybersecurity have received significant attention, resulting in larger investment rounds while decreasing the number of rounds. This approach indicates a rising emphasis on scaling existing firms rather than assisting many early-stage entrepreneurs (*Startup Nation Central, 2024*).

In 2024, the funding landscape reflected a continued emphasis on scaling and maturing businesses, with notable shifts in early, mid, and late-stage funding rounds. It highlighted a growing dominance of early-stage deals in terms of number, while late-stage deals accounted for an increasing share of total funding, indicating a concerning shift away from early-growth funding.

Early-stage rounds dominated funding activity, representing 80% of all rounds but accounting for only 29% of the total funding amount, reflecting the smaller

investment sizes at this stage (Appendix B). This trend underscores the continued expansion of early-stage investments and their essential role in fostering emerging startups. Mid-stage rounds contributed 30% of total funding, reinforcing their importance in supporting scaling companies. Meanwhile, late-stage rounds, though comprising just 5% of all rounds, secured 40% of total funding, emphasizing a strategic shift toward fewer but higher-value investments aimed at accelerating the growth of mature companies (Appendix C). Overall, the funding landscape in 2024 demonstrated a growing emphasis on impactful investments, supporting long-term innovation and sustainable expansion.

This was the part about the private companies, now let's analyze the public companies' founding trend.

2024 was a year of contrasts for Israel's high-tech ecosystem. On the one hand, Israeli public companies, particularly those listed on Nasdaq, demonstrated amazing resiliency. These firms generated significant revenue growth and displayed excellent operational efficiency, cementing Israel's position as a global leader in scalable technology corporations. On the other hand, Israeli public businesses saw a prolonged dip in public offerings and a general decrease in fundraising activity, highlighting the capital market's ongoing issues.

One significant positive aspect has been the increased involvement of Israeli growth businesses as both big employment and innovation enablers. Their growing share of tech employment demonstrates their stability, while the rise of Corporate Venture Capital (CVC) emphasizes their importance as strategic drivers of ecosystem expansion.

However, maintaining this progress necessitates addressing a fundamental issue: the future of Israel's talent pipeline. Recent data show significant losses in STEM education outcomes among children, as well as troubling ability disparities between young adults and their global peers. These tendencies jeopardize Israel's capacity to develop the imaginative minds required to drive the next wave of growth.

Israel, to ensure its high technology future, must prioritize investment in education and human resources at all levels. Improving STEM programs, AI, and English skills,

connecting academic courses with industrial needs, and cultivating a culture of continuous learning are all critical measures. The ecosystem's success has always been dependent on its talent; sustaining its continuity is critical to long-term, sustainable growth.

The graph below compares the performance of two indexes over the last year: the Finder Index, computed by Startup Nation Central and based on Israeli firms traded on NASDAQ, and the NASDAQ 100 Equal Weighted index. Both indexes are produced using an equal-weighting methodology, which means that each company contributes equally to the overall performance. This technique provides a balanced perspective, which is especially relevant when comparing indices to companies of varied market sizes. To better alignment with the NASDAQ 100 EW, the Finder NASDAQ Index contains a \$50 million market capitalization minimum criterion, which minimizes volatility.

The data shows a strong link between the two indices, with trending upward throughout the year. However, the Finder NASDAQ Index has grown at a 15.8% pace since the beginning of the year, compared to the NASDAQ 100 Equal Weighted Index's 9.4% growth rate during the same period (Appendix F). This shows that Israeli public companies listed on NASDAQ are mostly influenced by the same global economic drivers as their worldwide counterparts. These findings support the durability and competitiveness of Israeli public enterprises, which continue to thrive despite local challenges and turmoil. This underscores the importance of encouraging growth across the ecosystem, from startups to more mature organizations, and demonstrates the continued strength of Israel's tech landscape in a dynamic global economy (*Startup Nation Central, 2024*).

Between 2018 and 2024, public enterprises had extraordinary development, with the average number of employees per company increasing by 22%, from 1,213 to 1,479. Revenue increased even more dramatically, by 33.8%, from \$426 million in 2018 to \$570 million in 2024 (Appendix G).

The data, which is based on 139 public businesses listed on NASDAQ, also shows trends in revenue per employee, an important indication of operational efficiency.

This statistic fell from \$375K in 2019 to \$312K in 2021, during the COVID-19 pandemic. However, a resurgence began in 2022, with revenue per employee returning to 2019 levels by 2024. The period from 2022 to 2024 was particularly significant, with average revenues increasing by \$184 million and revenue per employee rising by 20% (Appendix H).

Overall, this analysis demonstrates that Israeli public companies listed on NASDAQ not only recovered from challenges but emerged stronger, using innovation and staff expansion to achieve long-term economic effects. These trends reflect the overall dynamism of Israel's tech ecosystem and its capacity to sustain leadership in competitive global marketplaces.

Startup Nation Central conducted the following analysis of the Israeli high-tech ecosystem's economic metrics in the first three quarters of 2024, in partnership with the Aaron Institute of Economic Policy. It is mostly based on data from the Central Bureau of Statistics (CBS) and provides insight into the ecosystem's economic effect trends.

The high-tech sector continues to stabilize the Israeli economy, accounting for 20% of GDP and 40% of economic growth. For the first three quarters of 2024, the sector's GDP per employee increased by 2.2% (in NIS terms), reaching NIS 632K, while employment in the sector declined by 0.7%, resulting in 1.5% rise in High tech GDP. This expansion counterbalances a broader loss in Israel's total GDP, highlighting the sector's resiliency in the face of difficult conditions.

High-tech exports per employee rose by 2.2% to NIS 511K (Startup Nation Central, 2024). The strong association (0.87) between exports per employee and GDP per employee demonstrates the industry's ongoing productivity growth (Appendix I).

High-tech employment declined to 394K workers in Israel, marking a 0.7% decrease compared to Q1-Q3 2023. R&D professions saw a 4.9% growth, indicating a strategic shift towards core innovation and technical roles. Meanwhile, several professional groups experienced losses, including Business & Administrative (-6.8%) and Product positions (-4.8%) (Appendix J). This suggests deliberating

refocusing reallocating resources to high-value activities, sometimes motivated by cost savings.

The high-tech sector's performance in 2024 emphasizes its importance to Israel's economic stability. Despite the sector's issues, including job losses and global uncertainty, its GDP contribution, productivity, and export-driven development demonstrate its importance as a foundation of resilience. As Israel's economy faces global and internal difficulties, boosting high-tech through state support for R&D, innovation, and digitization is critical. The patterns identified in this analysis demonstrate the sector's ability to adapt and survive, making it a critical driver of growth in an increasingly competitive global marketplace.

After presenting the performance of the Israeli tech sector let's go more focused on the Israel's defence tech sector.

#### 2.3.4: Incubators and accelerators

The Israeli ecosystem has thrived in recent years because of creative entrepreneurs that dare to think outside the box and devise unique technology solutions when others find it too difficult and give up. However, having a good idea is not always enough. Sure, Israel's ecosystem provides entrepreneurs with many helpful tools, such as massive VC availability, an impressive network of connections (due to Israel's unique dominance in terms of MNC presence), and a renowned academic infrastructure of research in multiple fields; however, standing out in a place where everyone believes they have just invented the Next Best Thing is a difficult task to master.

That is where incubators and accelerators come in: they do not only deal with the financial elements of businesses but also provide startups with a comprehensive framework that includes training and the transfer of knowledge and expertise, hence increasing the possibilities of companies' success.

In Israel, incubators are funded with the help of the State of Israel, which sees entrepreneurship and innovation as one of the most important catalysts for the

growth of the economy. The Israel Innovation Authority operates several incubator programs together with major companies, that provide startups with the complete infrastructure needed to develop their product, including office space, laboratory, scientific and technological guidance as well as business, legal, and marketing consulting. Apart from financial investments, the incubator mentors the startups in the process of product development.

Accelerators are another type of support program. Unlike incubators, which get state funding, accelerators are run by Israeli or international enterprises or non-governmental organizations. These projects are intended to introduce innovation into organizations, but not through the traditional way of R&D facilities. Companies are looking for fresh innovations that do not adhere to formal regulations and bring unique thinking to existing products and technologies. Israel currently has around 90 accelerators and counting. The primary distinction between accelerators and incubators (apart from finance) is that accelerators are intended to accelerate the startup's progress within a limited, set time frame. The classic structure of an accelerator is a relatively low amount of investment (between 5-25 thousand dollars), in addition to about 4 months of guidance and support, in exchange for a percentage of the shares in the company.

The most important authority for Innovation in Israel is the Israel Innovation Authority. It is in charge of the country's innovation policy and is an independent and impartial statutory public organization that works in the best interests of the Israeli innovation ecosystem and the Israeli economy as a whole. Its objective is to invest in innovation to achieve long-term and equitable growth.

The Authority is crucial in developing Israel's innovation ecosystem. It provides conditional funds to accelerate breakthrough scientific developments and actively strives to lay the groundwork and infrastructure for future technologies. Its purpose is to maintain technological and economic leadership while increasing productivity and boosting Israel's global competitiveness.

Innovation is by far the most important resource for the State of Israel, functioning as a national asset critical to economic growth. The Israel Innovation Authority

attempts to advance and encourage technological innovation in Israel through a variety of support instruments. Its purpose is to boost the innovation ecosystem by promoting innovation, entrepreneurship, and disruptive technologies as drivers of inclusive and long-term economic growth.

With extensive knowledge and understanding of the unique challenges that Israeli businesses and entrepreneurs face, the Israel Innovation Authority offers a range of practical tools and funding platforms aimed at meeting the dynamic and changing needs of the local and international innovation ecosystems. It offers conditional grants to support disruptive technological innovations and is involved in laying the groundwork and infrastructure for future technologies to maintain Israeli technological and economic leadership while also improving productivity and global competitiveness.

The authority is divided into four divisions: Startup Division, Growth and Advanced Manufacturing Division, Technological Infrastructure Division, and International Collaboration Division.

The Startup Division provides one-of-a-kind solutions to support the early stages of technology efforts, such as pre-seed or beginning R&D, assisting them in turning their ideas into reality while meeting crucial funding milestones.

Division programs include:

- Technological Incubators Funding Program;
- Startup Fund;
- Tnufa (Ideation) Incentive Program;
- Human Capital for High-Tech Fund;
- Visas for Foreign High-Tech Experts.

The Venture Incubators funding programme aims to support the creation of new technology start-ups and early-stage investments. The selected incubators operate for five years and offer start-ups technological, financial, and operational support to turn innovative ideas into commercial products. The programme is aimed at venture capitalists, multinational companies, and experienced investors interested in financing start-ups within the incubator. The Israel Innovation Authority provides

grants of up to NIS 40 million to cover operating expenses and equipment investments in the first five years, with funding percentages decreasing from 70 per cent to 50 per cent. Benefits include reducing financial risk, strengthening the position of an experienced investor, and access to a diversified portfolio of innovative start-ups. To participate, incubators must meet several requirements, including being entities registered in Israel, having a qualified management team, and securing financial resources of at least NIS 120m. Selection is based on the experience of the partners, the added value offered to the start-ups, the quality of the management team, the available financial resources and the soundness of the business plan.

The Israel Innovation Authority's Startup Fund is a funding initiative designed to help Israeli start-ups in their early phases by making non-dilutive investments to encourage the development of deep-tech and high-risk products. Israel, widely regarded as one of the world's leading technological hubs, owes much of its success to a favorable regulatory environment and government programs focused on promoting the hi-tech industry. The fund was established to solve global concerns such as climate change, healthcare, and food security, where software solutions alone are insufficient and advanced technologies with large intellectual property content, high risk, and lengthy development durations are required.

Despite the market slowdown, the program strives to promote and prepare the Israeli start-up community for the future by providing funds in the form of co-investment from private investors. The goal is to mitigate the inherent risk of investing in early-stage, deep-tech, and R&D-intensive enterprises. The program is aimed toward Israeli start-ups in the Pre-Seed, Seed, and Round A stages, which must undergo a rigorous due diligence procedure to confirm the quality of the technology and the team's capacity to effectively execute the project.

The financial assistance includes a grant of 60% of the Investment (up to NIS 1.5 million) for Pre-Seed firms, 50% (up to NIS 5 million) for Seed companies, and 30% (up to NIS 15 million) for Round A businesses. Furthermore, start-ups with at least one founder from underrepresented groups in the hi-tech sector (women, Arabs, ultra-Orthodox) or based in Israel's peripheral areas receive a 10% bonus, bringing the

maximum funding to NIS 1.65 million, NIS 5.5 million, and NIS 16.5 million, respectively. The money is non-dilutive, which implies that the Innovation Authority does not acquire capital stock or voting rights in the recipient enterprises.

Participating in the initiative provides several benefits to both start-ups and private investors. Companies can coordinate funding with their own fundraising efforts to provide financial stability till the next investment round. Investors, on the other hand, profit from exposure to cutting-edge technology and pre-selection of the top deep-tech start-ups, resulting in lower risk and a higher likelihood of successful fundraising rounds.

To be eligible, companies must be lawfully registered and operating in Israel, with the majority of their activities focused on research and development. Furthermore, unique constraints depend on the stage of the company: Pre-Seeds cannot raise more than NIS 1.5 million and have a turnover of less than NIS 300,000; Seeds cannot raise more than NIS 7.5 million and have a turnover of less than NIS 3 million; and Round A cannot raise more than NIS 50 million and have a turnover of less than NIS 30 million. Finally, a considerable portion of the generated funds must be committed to research and development: at least 80% for Pre-Seed, 75% for Seed, and 50% for Round A.

The Startup Fund thus represents a strategic opportunity for Israeli deep-tech start-ups, allowing them to access capital that is critical to overcoming the challenges of long development times and high regulatory barriers, thereby contributing to the growth and competitiveness of the country's technology ecosystem.

The Ideation Incentive Programme (Tnufa) is an Israel Innovation Authority initiative to help rising Israeli entrepreneurs and start-ups create and validate new technology concepts. The primary goal is to assist early-stage projects in achieving proof of concept and assessing commercial viability.

The scheme is aimed at entrepreneurs and new Israeli start-ups, and it provides a conditional grant of up to NIS 200,000 over a 12-month period, which covers 80% of the allowed budget. One of the most significant advantages is that entrepreneurs do not have to leave

their current jobs or give up their project rights to obtain funding. Furthermore, the program's support serves as a quality certification, making it easier to raise further money. At the end of the assistance period, the project may apply for additional funding through other Innovation Authority programs.

The funding approach is particularly appealing because the program shares in the risk of the company's growth but does not need capital contributions or a percentage of future earnings. However, the corporation must repay the funds through royalties on product sales.

The funding can be used to create an initial prototype, protect intellectual property, and establish business plans, with expenses covering materials, components, consulting, patents, and exhibitions but not salaries or overheads.

The Israel Innovation Authority's Human Capital for High-Tech Fund Programme aims to boost human resources in Israel's high-tech sector, with a concentration on research and development (R&D) positions. This program promotes innovative solutions for the training and placement of qualified individuals, thereby increasing the competitiveness and growth of the national technology industry.

The primary goal is to promote activities aimed at recruiting, selecting, training, internships, and job placement for new and experienced high-tech professionals. The program is designed for businesses and non-governmental organizations (NGOs) who produce programs centered on human capital management and technology industry training.

Funding varies according to the stage of project development. During the start-up phase, up to NIS 1 million can be applied for, with the grant covering 50% to 70% of the approved budget. In the growth and expansion phase, funding can reach NIS 15 million, with a grant covering 30% to 50%; in extreme situations, for particularly creative projects, the grant can be 60% or 70%.

Participation in the program has various benefits: in addition to contributing to the expansion of the high-tech industry, enterprises can profit from a favorable financing model, which reduces recruitment and training risks. Furthermore, companies are not required to repay the financing as long as they meet the specified goals and

milestones. Finally, the Innovation Authority's backing serves as a quality mark, allowing the enterprises participating to grow over time.

As a result, this project represents a strategic opportunity for businesses and non-governmental organizations (NGOs) looking to invest in the development of talent in Israel's high-tech sector.

The Israel Innovation Authority, in partnership with the Population and Immigration Authority, created the Visas for Foreign High-Tech Experts Incentive Program in 2018. Its goal is to ease the bureaucratic process of attracting foreign technology experts to Israel. This program tackles Israel's growing scarcity of talented workers in the high-tech sector by making it easier for enterprises to attract international expertise.

The Growth Division runs a variety of Incentive programs to help high-tech enterprises in the sales growth stage, as well as established high-tech companies who use growth channels based on technological innovation and/or seek funds for creative research and development.

Division programs include:

- Incentive Program to Encourage the Establishment of Multinational Companies' R&D Centers in the Fields of Biotechnology and Health;
- Incentive Programs for Innovation with Government Entities;
- Generic R&D Incentive Program for Large Companies;
- R&D Fund;
- R&D Preparatory Incentive Program for Companies in the Manufacturing Industry;
- MOFET – R&D in the Manufacturing Industry.

The Incentive Program to Encourage the Establishment of Multinational Companies' R&D Centers in Biotechnology and Health is a pilot initiative aimed at attracting large foreign industrial corporations involved in biotechnology and health to establish or expand their R&D and innovation operations in Israel. The initiative also aims to boost enterprises' management and global value chain activities in Israel, hence promoting growth in the local biotech and health sectors.

It also seeks to expand employment prospects by pushing enterprises to hire more people in Israel, including both R&D and non-R&D employees.

The Joint Government Support for Pilot Programs is a collaboration between the Israel Innovation Authority and other government agencies to fund high-risk R&D and pilot programs in specific fields. This initiative offers financial assistance, regulatory guidance, access to state-owned testing facilities, and chances to incorporate innovative technology into Israel's innovation ecosystem.

The Generic R&D Incentive Program for Large Companies encourages long-term research and development by large Israeli corporations, allowing them to generate new technological knowledge and infrastructure for future innovative goods. The program fosters long-term R&D expenditures by awarding funds for long-term research programs or collaborative initiatives with other Israeli enterprises, with the added benefit that recipients are not forced to pay royalties to the Innovation Authority.

Eligible companies must meet at least one of the following criteria: employ at least 200 R&D personnel in Israel, have an R&D budget of at least USD 20 million in Israel, generate annual sales of more than USD 70 million (including subsidiaries) in the previous three years, or be part of a parent company with total revenue exceeding USD 2.5 billion (holding at least 80%). The program provides cash incentives ranging from 20% to 50% of authorized R&D expenses, with an additional 10% available to enterprises working in Area 'A' Development Regions.

Companies that participate in this incentive program receive significant financial support with no obligation to repay royalties, allowing them to focus on long-term R&D operations that improve their technological skills and create a competitive advantage in global markets. The program eliminates financial risks while retaining full profit potential, making it an appealing funding strategy for large corporations seeking to engage in innovation.

The R&D Fund is the State of Israel's largest financial incentive program for Israeli firms conducting research and development activities. It is available to firms at all phases of development, from startups to large organizations, and in a variety of

industries, including hardware, software, communications, life sciences, medical devices, cyber, IoT, finance, and cleantech. The program's goal is to promote technical innovation and boost the Israeli economy by giving financial help for the development of new goods or upgrades to existing technologies.

Eligible enterprises receive financial support ranging from 20% to 50% of approved R&D expenditures, with extra incentives for companies operating in Development Zones (+10%) or near the Gaza Strip (+25%). Startups managed by entrepreneurs from minority groups, the Ultra-Orthodox community, or women may obtain up to 75% capital in the first year and 70% in the second. The program follows an appealing financing approach, covering development risks without requiring payback until the idea reaches commercialization, at which point capital is reimbursed through royalty payments.

Companies participating in the R&D Fund receive financial support to undertake high-risk, creative ideas that provide a competitive edge and access to new markets. Support from the Innovation Authority also serves as a quality mark, confirming a company's R&D activities and enhancing its capacity to attract private investment. The innovative Authority's R&D Preparatory Incentive Program for Manufacturers is a support effort targeted at supporting manufacturing enterprises with little or no prior R&D expertise in driving innovative processes. The initiative aims to boost the competitiveness of participating enterprises by promoting technical developments and streamlining manufacturing processes. It provides structured support through four specialized tracks: the Basic Support Track, which helps companies formulate new products or processes by mapping technological capabilities; the Technological Feasibility Examination Track, which assists in assessing the feasibility of new technologies and mitigating technological risks; and the Developing Solutions for Production Flaws Track, which focuses on identifying and resolving technological issues in the manufacturing process.

Eligible applicants include Israeli industrial companies that operate in traditional or mixed-traditional technology sectors (such as food, textiles, plastics, metals, and construction materials) or mixed-high-tech manufacturing sectors (such as

chemistry, electrical equipment, and machinery production), as long as a significant portion of their workforce is engaged in manufacturing.

The program provides financial assistance covering 66% of the approved budget (up to NIS 75,000) and 75% (up to NIS 100,000) for enterprises in Area 'A' Development Regions. Funding is provided for consultant costs, market surveys, patent research, lab tests, material procurement, and other technology development expenses. Participating enterprises can identify technology gaps, increase production efficiency, and plan for future R&D projects with the Innovation Authority's assistance. Manufacturing enterprises who participate in the program can improve their technological capabilities, incorporate innovation into their operations, and raise their industry competitiveness.

The MOFET, R&D in the Manufacturing Industry program is an Innovation Authority effort that aims to boost Israel's manufacturing sector by encouraging innovation and technological advancements. Given the rising global competitiveness, this program offers targeted incentives to assist industrial enterprises in developing new goods, improving existing ones, and improving manufacturing processes. The ultimate goal is to increase productivity, establish technological distinctiveness, and gain a competitive advantage in both domestic and international markets.

The program is intended for Israeli firms or industrial factories who generate at least 50% of their revenue through industrial manufacturing. Eligible sectors include traditional industries (food, textiles, paper, etc.), mixed-traditional sectors (rubber, plastics, metals, ceramics), mixed-high-tech sectors (chemicals, electrical equipment, machinery, medical devices), and high-tech industries (pharmaceuticals, aerospace, electronics, computers). Furthermore, enterprises must employ at least 30% of their staff in manufacturing positions, with R&D employees accounting for no more than 10% of the entire workforce.

The program provides financial assistance for 30%-50% of R&D expenses, with an extra 10% increase for projects in Area 'A' Development Regions or those carried out in partnership with recognized research institutions. Mold development (up to NIS 500,000), prototyping of unique production machinery (up to NIS 500,000),

knowledge acquisition integral to the R&D program (up to NIS 250,000), and product commercialization and marketing (up to 15% of the approved budget) are examples of R&D-related costs that are eligible for funding.

For companies new to R&D and engaged in manufacturing in Israel, the program provides royalty exemptions for the first three approved R&D projects, along with 50% funding of the approved budget. After the royalty exemption period, companies (except high-tech manufacturers) benefit from a reduced 1.3% royalty rate.

Companies who participate in the MOFET program receive specialized financial support, allowing them to pursue R&D initiatives with lower financial risk, improve their technological capabilities, and enter new markets with competitive, creative goods. The program is especially useful to enterprises who are starting R&D activities, as it provides preferential circumstances and strategic support to guarantee their successful integration into the innovation-driven economy.

The Technological Infrastructure Division is responsible for funding applied R&D infrastructure, promoting applied research in academia, technology transfer, leveraging R&D for dual use technologies, exchanging knowledge and experience, and developing groundbreaking innovation through an integrated group of researchers from academia and industry.

Division programs include:

- TELEM (The National Infrastructure Forum for Research and Development)
- Leveraging R&D for Dual Use Technologies – MEIMAD
- Applied Research in Academia
- Knowledge Commercialization
- MAGNET Consortia
- Users' Association R&D Infrastructure
- Promoting Applied Research in Academia
- Infrastructure and Equipment.

TELEM was founded in late 1997 on the Israeli National Academy of Sciences initiative. The Forum is a volunteer organization dedicated to promoting R&D programs and initiatives in scientific and technological domains by establishing

national R&D infrastructures as well as inter-organizational, inter-departmental, and worldwide cooperation (Israel Innovation Authority, n.d.).

The first nanotechnology research institute was founded at the Technion in 2005 for a five-year term with a total investment of USD 78 million, sponsored equally by the Technion, a philanthropic fund, and the State of Israel. TELEM members were responsible for implementing the funding. The program's goal is to encourage investment in academic nanotechnology institutes in order to establish and build an academic technological infrastructure capable of addressing industry demands.

As part of the construction of the Technion's nanotechnology R&D center, valuable infrastructural equipment was obtained, which can be used by researchers from other universities and industries. Nanotechnology centers were established at five additional research institutes, including the Weizmann Institute, Hebrew University, Tel Aviv University, Bar Ilan University, and Ben Gurion University, two years after the Technion center was founded.

The overall investment in these facilities is around USD 142 million, with around 20% of that invested in 2009. The other nanotechnology centers use the same "triangle funding" strategy as was used to build the institution at the Technion.

As part of the construction of the Technion's nanotechnology R&D center, valuable infrastructural equipment was obtained, which can be used by researchers from other universities and industries. Nanotechnology centers were established at five additional research institutes, including the Weizmann Institute, Hebrew University, Tel Aviv University, Bar Ilan University, and Ben Gurion University, two years after the Technion center was founded.

The overall investment in these facilities is around USD 142 million, with around 20% of that invested in 2009. The other nanotechnology centers use the same "triangle funding" strategy as was used to build the institution at the Technion.

13 initiatives with combined Israeli-German finance were launched in 2018, totaling around NIS 80 million over three years. At the heart of these programs is the transfer

of information from nanotechnology institutes in academia to Israeli industry, in collaboration with German research centers and industry. The research programs focus on photonics, materials, diagnostics, drug administration, coatings, electronic component and sensor efficiency, and energy utilization (Israel Innovation Authority, n.d.).

The incentive program is designed to foster collaboration among the Forum's member organizations on all aspects of research and development, guiding the launch, management, and evaluation of projects; combining financial and other resources from members' budgets and relevant agencies; and designating clear accountability for establishing, operating, and overseeing national R&D infrastructures (Israel Innovation Authority, n.d.).

The incentive program targets both Forum members and select external partners, formalized through agreements that define each party's commitments. It supports projects such as the MIDGAM Tissue Bank, a Ministry of Health-supervised repository of human biological specimens for medical and biological research, and the Israel National Nanotechnology Initiative, which invests in academic nanotech centers to build a robust technological infrastructure for industry use (Israel Innovation Authority, n.d.).

MEIMAD brings together the Innovation Authority, the Ministry of Finance and the Ministry of Defence Administration to back the creation of dual-use technologies that serve both defence and civilian markets. By funding Israeli small- and medium-sized enterprises—those with annual sales up to US \$100 million—and academic research bodies, this program offers grants covering 50 % to 90 % of project costs, depending on the activity's scope and nature. Whether you're transferring military know-how to commercial products, developing novel services, spinning out university research or facilitating technology transfer, MEIMAD unlocks the pathway to bolster national security capabilities while tapping into significant market potential (Israel Innovation Authority, n.d.).

The Applied Research in Academia program is designed to advance innovative academic research toward commercialization by encouraging collaborations

between Israeli research institutions and industry. Its primary aim is to bridge the gap between academic discoveries and the technological needs of the private sector, enabling projects to reach key milestones that attract business interest. When a company joins a research consortium, it increases the likelihood of the research being commercialized within the Israeli economy.

This initiative is open to research teams from all Israeli universities, colleges, and medical centers, provided their projects build on existing basic research and present original, industrially relevant innovation. The program offers financial support, either independently or in collaboration with a corporation, that does not require repayment through royalties. Funding is typically provided for one or two years, with the possibility of a third-year extension at a reduced grant rate (66% or 75%). Research institutions applying without corporate backing can receive (Israel Innovation Authority, n.d.):

- Up to NIS 440,000 per year at a 75% or 85% support rate for a single institution.
- Up to NIS 660,000 for two collaborating institutions (max NIS 400,000 each).
- Up to NIS 770,000 for three collaborating institutions (max NIS 400,000 each).

When supported by a corporation, funding increases to:

- NIS 550,000 per year at 80% or 90% for a single institution.
- NIS 700,000 for two partners (max NIS 500,000 each).
- NIS 810,000 for three institutions (max NIS 500,000 each).

The accompanying corporation plays a vital role in steering research objectives and providing professional input, while contributing 10% of the project's costs. In return, it gains exclusive first negotiation rights for commercialization upon project completion.

Projects approved by the Technology Infrastructure Division may also receive the assistance of a commercial technology expert to enhance the transition from R&D to market. This added benefit is subject to approval and requires a formal waiver and disclaimer.

For academic institutions, the program provides essential funding and increased commercialization prospects while retaining full ownership of the research outcomes. For participating corporations, it offers a strategic opportunity to shape innovative research aligned with their future goals, with the advantage of early access to potential commercialization agreements, all for a relatively modest investment (Israel Innovation Authority, n.d.).

The Knowledge Commercialization program is designed to transform academic research into market-ready innovation by facilitating collaboration between research institutions and industrial companies. Through three sub-programs, MAGNETON, Knowledge Import, and Continued MAGNET, it supports the adaptation, validation, and development of cutting-edge technologies to meet commercial needs (Israel Innovation Authority, n.d.).

MAGNETON focuses on transferring technologies from one or more Israeli research institutes to a single industrial partner, validating study results, and tailoring innovations to business applications. The Knowledge Import track promotes partnerships between Israeli companies and foreign research institutes to verify and adapt external discoveries for local development. Meanwhile, Continued MAGNET supports follow-up R&D projects that extend work previously approved under the MAGNET Consortium framework (Israel Innovation Authority, n.d.).

This initiative is open to Israeli industrial companies seeking to develop new or improved products based on research findings, as well as academic groups from recognized Israeli research institutions aiming to commercialize their innovations in collaboration with an industry partner. The research must be original, technologically feasible, and fully owned by the participating institution. In all cases, academia is not treated as a subcontractor but as a full partner, while funding is channeled through the corporate entity (Israel Innovation Authority, n.d.).

Participants can receive a grant covering up to 66% of the approved project budget, capped at NIS 3.4 million for up to 24 months, with no requirement to repay royalties (Israel Innovation Authority, n.d.).

For research institutions, the program offers a powerful channel for bringing scientific discoveries to market. For industrial companies, it provides access to groundbreaking technologies and a structured, lower-risk framework for testing their feasibility. Upon completion of the project and successful proof of concept, the company has the exclusive option to acquire commercialization rights and independently pursue product development, enabling both parties to drive innovation and economic growth (Israel Innovation Authority, n.d.).

The Users' Association R&D Infrastructure program supports collaborative efforts among industrial companies within the same technological sector to establish and operate shared research and development infrastructure. By pooling resources and expertise, participating companies can jointly develop facilities or systems essential to advancing their R&D goals (Israel Innovation Authority, n.d.).

This initiative is aimed at companies actively involved in research and development that recognize the value of collective infrastructure investment to support ongoing innovation in their field. Rather than providing direct grants to individual firms, the program funds an independent legal entity—the Association—formed by the participating companies.

The Association may receive up to 66% of the approved project budget, while the remaining 34% must be contributed by the member companies. Projects can span up to three years, with the option to extend the support for an additional three years, allowing long-term collaboration and sustained impact on industry-wide technological advancement (Israel Innovation Authority, n.d.).

The Promoting Applied Research in Academia program is designed to advance academic innovations with technological potential to a stage where they can attract industrial interest and be commercialized. By fostering collaboration between research institutions and corporate partners, this initiative aims to align academic research with industry needs and drive high-value innovation into the Israeli economy.

The core objective is to close the gap between academic knowledge and market application by guiding research projects toward meaningful milestones. These

milestones should position the project for commercialization through a formal agreement with a business entity. The involvement of a supporting corporation, either from the outset or during the project's lifecycle, greatly enhances the likelihood of successful commercialization (Israel Innovation Authority, n.d.).

This incentive is intended for research groups based in Israeli universities, colleges, medical centers, or technical research institutes who wish to carry out applied research that builds on their prior basic research. Proposals can involve one to three Technology Transfer Offices (TTOs), representing up to three collaborating researchers from one or more institutions. The research must be both innovative in its industrial application and relevant to the Israeli market, offering significant added value to the national economy.

Academic participants can receive funding of up to NIS 1,250,000 for a single researcher, with an additional NIS 250,000 available per additional researcher (up to three in total). Funding covers 80% of the approved budget if the project does not include a corporate partner and up to 90% when one is involved. All grants are royalty-free, regardless of whether a corporation is involved (Israel Innovation Authority, n.d.).

A supporting corporation plays a key role by contributing 10% of the project budget, guiding research goals, and gaining first negotiation rights for a commercialization agreement upon completion. If the project reaches Technology Readiness Level 5 (TRL5), testing may be carried out in the corporation's service laboratory. The Innovation Authority may also assist in identifying and integrating a suitable corporate partner for approved projects that lack one initially (Israel Innovation Authority, n.d.).

Overall, this program offers research institutions the opportunity to turn scientific insights into industrial solutions while providing companies with early access to transformative technologies.

The International Collaboration Division is in charge of arranging international collaboration in innovative R&D knowledge and technology between Israeli

enterprises and equivalent organizations abroad, thereby providing numerous competitive advantages to the Israeli industry in the worldwide market.

The Europe, Americas, and Asia Pacific Desks, as well as the desk for multinational corporations, provide support for such strategic alliances through a variety of bilateral cooperation agreements and bi-national funds, as well as the EU Framework Programme for Research and Innovation.

Division programs include:

- Bilateral Programs for Parallel Support;
- R&D Cooperation with Multinational Corporations;
- EU Framework Agreements - Horizon Europe;
- Program for Boosting Participation of Israeli Companies in the European Frameworks Program – Horizon Europe;
- Incentive Program for Adapting Products for Emerging Markets;
- Bi-national Funds.

The Bilateral R&D Incentive Program supports Israeli companies engaged in international collaborations aimed at developing new technological products or significantly enhancing existing technologies with a clear path to commercialization. This initiative operates through partnerships between the Israel Innovation Authority and foreign entities such as national, regional, or local government bodies, which jointly fund the projects. By offering financial assistance, the program helps mitigate the risks associated with R&D and provides support in identifying suitable international technology partners. It targets Israeli tech companies across all sectors, fostering strategic global networks, expanding access to technological expertise, and enabling product scale-up and entry into international markets, ultimately boosting the global competitiveness of Israeli industry. Approved projects must have an annual budget ranging from NIS 500,000 to NIS 1.5 million, distributed over a period of up to five years. Funding covers 50% to 60% of the approved budget in the first three years, while in the fourth and fifth years, the support drops to 30% and 40% respectively, contingent on meeting predefined criteria. Participating in this program enhances institutional investment in Israel's high-tech sector and

allows the broader economy to benefit from the sector's success, while offering companies the opportunity to integrate cutting-edge innovations developed with international partners.

The R&D Collaboration with Multinational Corporations (MNC) Program facilitates partnerships between Israeli startups and leading global corporations to promote joint research and development efforts. Recognizing Israel's reputation as the "Startup Nation," this initiative leverages the innovation of small, agile companies and the market access, resources, and commercialization capabilities of large multinationals. The goal is to enable startups and MNCs to co-develop technologies by sharing R&D risks and combining expertise. Within this framework, the Israel Innovation Authority and the participating MNC each commit to supporting pre-approved joint projects. Although financial grants are provided solely by the Innovation Authority and the Israeli company, the MNC can contribute either through direct funding or in-kind support such as lab access, personnel, equipment, or technical mentorship. This mutually beneficial arrangement allows both entities to access unique technological insights, identify high-potential partners, and enhance the commercialization potential of innovative products globally. To apply, Israeli companies must submit an executive summary for approval, typically in response to a joint call for proposals by the MNC and the Authority. If approved, they may then apply for the grant through standard Innovation Authority procedures. Eligibility requires the MNC to have annual revenues over USD 1.5 billion, significant R&D investments, and a global R&D presence. Israeli companies must demonstrate strong R&D capabilities, have annual revenues under USD 70 million, and be unaffiliated with the MNC. Projects must involve both parties in R&D and align with the MNC's core business, while intellectual property generated may be solely owned by the Israeli company, jointly owned, or licensed non-exclusively to the MNC. Joint ownership is permissible under the R&D Law if both entities contribute to the development, ensuring that the Israeli company retains full rights to use the IP while the MNC enjoys unrestricted, royalty-free use globally, provided this does not hinder the Israeli partner's ability to exploit the technology.

Horizon Europe, the European Union’s flagship research and innovation programme for 2021–2027, provides a €95.5 billion investment across all major scientific and technological fields to drive excellence, tackle global challenges, and boost European competitiveness. Open to organisations in the 27 EU member states and 19 associated countries—including Israel—Horizon Europe is built on four pillars: “Excellent Science,” which funds frontier research through the European Research Council, researcher mobility via Marie Skłodowska-Curie Actions, and pan-European research infrastructures; “Global Challenges and European Industrial Competitiveness,” where consortia tackle six thematic clusters ranging from health and security to digital industries, climate, energy, mobility, and the bioeconomy; “Innovative Europe,” which backs game-changing startups and scale-ups through the European Innovation Council, fosters regional innovation networks, and bolsters the European Institute of Innovation and Technology; and “Widening Participation and Strengthening the European Research Area,” which spreads excellence, reforms the research landscape, and cultivates public-private partnerships (with 49 currently active and ten more slated for launch in 2025). Cross-cutting “Missions” unite consortium-based efforts to confront pressing societal issues—such as climate adaptation, cancer, ocean restoration, smart city development, soil health, and the New European Bauhaus—while funding opportunities extend to universities, research centres, businesses (including SMEs), non-profits, and public authorities registered in Israel, all of which can tap into Horizon Europe’s collaborative networks and financial support.

### 2.3.5 The Talpiot Program

For more than fifteen years, Hamas has been constructing a huge network of tunnels across the Gaza Strip. The tunnels, dubbed the "Metro" by the Israel Defence Forces (IDF), reach for up to 500 miles, or double the size of New York City's metro system, and cover an area about twice the size of Washington, DC. These tunnels, which are typically created beneath residential and protected areas, provide military benefits

by allowing fighters and weapons to move freely without being subject to airstrikes while being protected by de facto human shields. The IDF's principal purpose in its combat with Hamas is to locate and destroy these tunnels (Balkus, 2024).

The IDF has reported that it has destroyed approximately 20% of the tunnels so far, employing a variety of methods. One of the key instruments used by the IDF is a sensor system known as Power Number, which was developed approximately a decade ago by three graduates of Talpiot, an advanced IDF training institution.

Talpiot arose in the aftermath of another disastrous surprise attack on Israel, the Yom Kippur War in 1973, during which the IDF was caught off guard and lost over a thousand tanks and 20% of its air force. The IDF's leadership at the time recognized that if the Israeli state was to exist in the future, it would have to outthink a numerically superior adversary. This would imply reaching a level of technological superiority that would neutralize the Arab governments' larger military forces.

To answer this problem, the IDF initially proposed establishing an institute fashioned after Xerox PARC, the Silicon Valley research and development group responsible for several groundbreaking computing developments, including the personal computer. However, the Israelis quickly recognized they lacked the wherewithal to establish such an institute. Instead of establishing an institute with experienced researchers, the Israelis wanted to identify a small number of their country's brightest young people and, during their peak of invention, charge them with designing weaponry no other country had. This program evolved into Talpiot (Balkus, 2024).

This institutional architecture reflected the fact that, while Israel did not have much money, it did have a population of many academically bright young men who were required to serve in the IDF once they turned eighteen. Over time, the program evolved to serve a similar role in Israeli society as Ivy League universities do in the United States. Despite its numerous issues, the university system is here to stay. If anything, prominent institutions are growing increasingly important as centers of power not only in the United States, but also in other wealthy countries, such as

China. The Talpiot program demonstrates how colleges could be supplemented or partially replaced to develop a new national elite (Balkus, 2024).

Dan Sharon, the first commander of Talpiot and a former IDF paratrooper, recruited his friend Felix Dothan, who had recently finished his PhD dissertation at Hebrew University on "the development of thinking and how one could improve his or her own thinking." Dothan's goal at Talpiot was not just to impart technical knowledge or choose the brightest minds; it was to teach people how to think and learn quickly (Balkus, 2024).

Together, they produced a memo outlining what they were seeking for in recruits: "We require individuals with a high IQ. We are searching for the top 5% in terms of intelligence, creativity, focus, stability, and pleasant personalities." Furthermore, applicants must demonstrate "dedication to their homeland and a strong will to survive in the unit." They wanted the brightest men (and, eventually, women) they could find at a time when they still believed anything was possible. However, they desired more than raw intelligence, which presented a severe selection challenge (Balkus, 2024).

Dothan and colleagues began working on a selection process to identify applicants who met their requirements. Talpiot was founded in 1979 and was initially designed for a cohort of 25 people chosen from a pool of up to 10,000 test takers to complete a bachelor's degree in physics and mathematics (computer science was added in 1983) from Hebrew University, with four years of content compressed into three years. Talpiot's executives collaborated with academic advisors to develop psychometric tests to assess candidates' cognitive abilities and inventiveness. The two hundred or so shortlisted candidates went through a rigorous interview in which they were given logical puzzles designed to test their creativity and critical thinking skills, as well as asked to explain physical phenomena that went much beyond what they had learned in school (Balkus, 2024).

A drawback in the selection procedure was rapidly recognized; highly inventive technical minds do not always have "stable and pleasant personalities," and members of Talpiot's inaugural classes struggled to work as a team. Additional

personality tests were implemented, putting prospective recruits through severe simulations to assess their leadership and teamwork abilities, as well as drive and "moral value." Once accepted into the program, Talpiot students spent almost all of their time together, fostering a strong camaraderie (Balkus, 2024).

Talpiot's curriculum intentionally stretched cadets beyond their comfort zones by first pinpointing each student's strongest problem-solving approaches and then challenging them with tasks that contradicted those tendencies. This method forced trainees to adapt and devise novel solutions; as alumnus David Kutasov noted, Talpiot "breaks" conventional thinking common even at elite U.S. universities and drives participants toward originality (Balkus, 2024). Such rigor leads to a substantial dropout rate, with roughly one in four selected candidates not completing the program (Balkus, 2024).

The program operates under the joint sponsorship of the Israeli Air Force and Maf'at (the Administration for the Development of Weapons and the Technological Industry), which functions as the central coordinator of Israel's defence R&D efforts, linking the IDF, major defence contractors, the Institute for Biological Research, and the Israeli Space Agency (Balkus, 2024). Although officially tied to the Air Force, Talpiot cadets spend significant time embedded in various IDF units; these rotations ensure that theoretical lessons from the classroom are applied directly to field exercises and realistic combat scenarios (Balkus, 2024).

Throughout the three-year undergraduate phase, Talpiot officers craft R&D position profiles aligned with each military branch's top priorities and work to secure placements that maximize each cadet's future influence (Balkus, 2024). After earning their degrees, graduates fulfill a six-year service obligation—most often in R&D roles within the Army, Navy, or Air Force—though some may pursue combat paths such as fighter pilot training (Balkus, 2024).

Israel's most promising cadets are required to undertake "the Project," which involves conceiving an innovative solution to a defence-related challenge, estimating its costs, and delivering a working prototype. Many of these student initiatives are

later adopted by the IDF; for instance, an early Talpiot mockup eventually evolved into the Iron Dome missile-defence system (Balkus, 2024).

Talpiot initially competed with Unit 8200, Israel's equivalent of the U.S. NSA, for top recruits. Rather than undermine one another, Talpiot and Unit 8200 leadership agreed informally to collaborate on identifying exceptional candidates, leaving each individual to choose between the two paths (Balkus, 2024).

This integrated talent search begins as early as elementary school and continues through supplementary programs in middle and high school. One notable feeder is the Nachshon Program, which employs Talpiot's educational methods to cultivate Israel's brightest technical minds. Additionally, institutions like the Israeli Arts and Science Academy (IASA), a boarding school for gifted students, have been established. Currently, about 7 percent of Talpiot's fifty cadets are IASA alumni, and a quarter of IASA graduates eventually earn doctorates in STEM fields (Balkus, 2024).

Programs such as Talpiot and Unit 8200 admit only Israeli citizens, and their alumni have exerted an outsized influence on both Israel's economy and military capabilities. Despite Israel's relatively modest defence budget, approximately \$23.6 billion compared to U.S. defence R&D spending (roughly \$130 billion annually), the IDF repeatedly produces groundbreaking systems in line with Talpiot's goal to develop entirely novel weaponry (Balkus, 2024).

These systems often emerge from U.S.–Israel collaboration. Beyond Iron Dome—manufactured jointly by Israeli and American contractors with significant U.S. funding—another example is the Stuxnet computer virus, which disabled about 20 percent of Iran's nuclear centrifuges and physically degraded hundreds of targets. Stuxnet is widely believed to have been a joint NSA–Unit 8200 effort (Balkus, 2024). Talpiot alumni have been credited with influencing virtually every IDF weapons and communications platform, as well as the entire Israeli intelligence toolkit (Balkus, 2024). Several have been honored with the Israeli Defence Prize—the nation's highest award for contributions that significantly enhance state security. Beyond

military applications, Talpiot graduates have launched over a hundred companies valued collectively at more than \$50 billion (Balkus, 2024).

A standout example is Check Point Software, founded by veterans of Talpiot and Unit 8200. In 1993, they created one of the first antivirus and cybersecurity suites for internet-connected PCs. Today, Check Point is Israel's leading cybersecurity firm and, by market capitalization, the second-largest Israeli company overall. This success spurred Israel's cybersecurity sector, which in 2021 represented nearly 10 percent of the global market. A 2018 study found that around 80 percent of Israeli cybersecurity founders had served in IDF intelligence units. Meanwhile, Israel's aerospace and defence exports approached \$13 billion in 2022, driven largely by drone and electronic-warfare technologies developed within the IDF's R&D framework (Balkus, 2024).

Combined, aerospace, defence, and cybersecurity contribute about 15 percent of Israel's yearly exports. Much of this economic strength stems from leadership and technical talent emerging from Talpiot and Unit 8200. Alumni have also launched venture-capital firms, such as Glilot Capital Partners and Axon, which specifically back startups founded by veterans of these elite units (Balkus, 2024).

Increasingly, former Talpiot members are founding companies across diverse sectors, transportation, healthcare, construction, agriculture, media, and beyond, helping to cement Israel's reputation as a global tech powerhouse. In 2023, despite a population of just nine million, Israel hosted 89 unicorn startups (valued over \$1 billion), ranking it alongside the likes of Estonia and Singapore in unicorns per capita, surpassing the United States on that metric (Balkus, 2024).

Talpiot alumni have also made remarkable academic contributions. Notable figures include Yoav Freund, co-recipient of the Gödel Prize for machine-learning theory, and Elon Lindenstrauss, who earned the Fields Medal, the so-called "Nobel Prize of Mathematics", for his work in dynamics. Another graduate received a technical Grammy for developing audio-mixing technology. Unlike many selective academic programs, Talpiot deliberately avoids overemphasizing conformity, thereby fostering wide-ranging intellectual exploration. For example, Harvard astrophysicist

Avi Loeb, an ex-Talpiot participant, is globally recognized for proposing that 'Oumuamua (the first interstellar object detected in our solar system) might be an artificial construct (Balkus, 2024).

Talpiot's impact is especially striking given its small alumni base, around 2,000 graduates, equivalent to a typical freshman class at Harvard (Balkus, 2024). Its success has inspired similar initiatives abroad, such as a South Korean program explicitly modeled on Talpiot; China has adopted comparable efforts as well (Balkus, 2024).

Attempting to establish a program like Talpiot in the U.S. would necessitate collaboration with a leading university akin to Talpiot's partnership with Hebrew University. Yet, many American campuses would resist an undergraduate research-and-development track focused on novel weaponry. For decades, Harvard, Yale, and Columbia prohibited ROTC activities on their grounds until 2011, and Stanford Business School recently blocked students from forming any defence-technology clubs (Balkus, 2024).

Ironically, while Talpiot's founders looked to America's Ivy League as a model, the U.S. was already veering away from such programs. U.S. diplomatic recruitment illustrates this shift: historically, the Foreign Service Officer Test (FSOT) was a rigorous, three-and-a-half-day examination covering history, geography, foreign cultures, and politics, with a pass rate near 20 percent. However, a 1989 court ruling found the FSOT's general background section discriminatory, since men passed at roughly twice the rate of women, prompting the State Department to shorten and simplify the exam. In 2022, grading was changed from pass/fail to a scaled score to allow hiring of lower-scoring candidates from underrepresented groups. Any U.S. talent-development program mirroring Talpiot would face similar "disparate impact" legal challenges and pressure to prioritize diversity and inclusion, especially at elite universities that already select students via different criteria (Balkus, 2024). By contrast, in Israel, veterans of elite IDF units routinely ascend to leadership roles in business and politics. Prime Ministers Benjamin Netanyahu and Naftali Bennett both served in Sayeret Matkal (the IDF's special-forces unit), reflecting a public

consensus on the moral clarity of defence. Entry into this elite class often begins with programs like Talpiot (Balkus, 2024).

Historically, similar pathways existed for the U.S. elite: Ivy League graduates once sought CIA careers as zealously as today's graduates pursue positions at McKinsey. Yet, over time, advancement within those institutions slowed, reducing their appeal to ambitious young people. Currently, the U.S. model struggles to identify its most talented youth and fails to provide them with meaningful channels for impact. Implementing an approach based on patriotism-driven psychometric selection and rigorous training would demand a seismic shift in American ideology and, perhaps more dauntingly, a willingness to grant substantial authority to young innovators. While Talpiot is not the sole template for nurturing top talent, any U.S. alternative must fundamentally transform how future leaders are chosen and educated (Balkus, 2024).

### 2.3.6: The Unit 8200

Given Israel's geopolitical context, Unit 8200's work is undeniably important: of all the institutional tasks assigned to a military unit, Unit 8200 plays an essential role in monitoring potential threats to the Jewish state, carrying out all those proactive actions to ensure active surveillance (the so-called early warning). This aims to intercept and prevent potentially hostile actions by extremist groups, hostile nations, or terrorist networks. In essence, the information gathered is processed and used to avert potential assaults, identify emerging dangers, and ultimately ensure Israeli national security (Geopop, 2024).

At this point, some may wonder how one might join the 8200 unit. As one may easily guess, the operations mentioned provide a clear picture of the scope of this unique unit's operations. It is simple to envision that the recruitment process, as well as the preparation gained by the group's members, are reserved for a select few members who are constantly trained.

Potentially appealing profiles comprise the most talented candidates from Israeli schools and training institutes. The young people, chosen from among the best, go through extensive training programs with the goal of training and preparing them to tackle the problems of modern intelligence. Contrary to expectations, sources describing the operational environment within the 8200 unit describe an approach that is not typical of a military unit: instead, a more innovative approach appears to be favoured, leaving plenty of room for initiative and the exploration of new solutions to complex problems. A form of think tank with military ties. This mentality has inspired many former 8200 unit members to start their own technological enterprises after they leave the military (Geopop, 2024).

The IDF's Military Intelligence Unit 8200 has played a key role in transforming Israel into a "start-up nation," a global center of technical innovation with the highest concentration of start-ups outside of Silicon Valley (All Israel News Staff, 2024).

At least five tech businesses founded by Unit 8200 alumni are publicly traded in the United States, with a combined valuation of approximately \$160 billion. Private enterprises founded by former 8200 soldiers are worth billions more.

In July, the leading cloud-security business, Wiz, was on the verge of negotiating a \$23 billion acquisition deal with Google. It would have been Google's largest acquisition ever. After the deal fell apart, Wiz CEO and 8200 veteran Assaf Rappaport told staff that he wanted to reach \$1 billion in revenue before considering a public-market offering (Kruppa & Perry, 2024).

Wiz and the 8200 grads are tackling a large commercial problem, how to keep big firms secure, with the skills and focus they honed in the military. They and the firms they've founded have become hot commodities as more sectors migrate massive volumes of business records to the cloud, which is continuously under attack by opportunistic hackers. While Unit 8200 alumni used to talk about their service in whispers, they now promote it in press releases to recruit clients and investment funds for new startups (Kruppa & Perry, 2024).

Palo Alto Networks, the largest publicly traded cybersecurity business and a product of the 8200 pipeline, has recently acquired many startups managed by the unit's

graduates. Greylock Partners and Sequoia Capital, two of Silicon Valley's most legendary venture capital firms, have lately hired Israeli partners. Elsewhere, Silicon Valley's investment engine has slowed. Startup funding is more difficult to come by than it was a few years ago, and venture investment has dropped by around half from its peak in 2022. The Israeli military recruits for Unit 8200 as early as elementary school, scouting robotics clubs and after-school coding programs for ability. Soldiers generally maintain long-term contact with leaders and fellow recruits after serving in the unit. The Tel Aviv-based Unit 8200 alumni organization hosts business-skills training events and webinars for its members. They frequently organize reunions with former soldiers in cities throughout the world (Kruppa & Perry, 2024).

Alumni note that while in Unit 8200, they acquire real cybersecurity skills as well as the most recent surveillance tactics. Their concentration on Israel's national security enables them to grasp cyber-offense and cyber-defence after leaving the service. Unit 8200 pushes its members to question their leaders and confront tough problems with unknown solutions. Many believe that their high-pressure atmosphere and quick thinking help them succeed in business outside of the military (Kruppa & Perry, 2024).

"It almost makes you feel like you can do anything," Kobi Samboursky said of his six-year stint in Unit 8200. In 2011, Samboursky founded venture capital firm Glilot Capital Partners, which was named after the unit's military base outside Tel Aviv. "I've been through worse situations, so what's a deadline? What's a competitor? What is an investor? "Everything appears to be easier." (Kruppa & Perry, 2024).

The majority of the enterprises in which Tel Aviv-based Glilot Capital's initial \$30 million fund invested were managed by former unit soldiers. Since then, the fund's value has increased at an annual rate of 84.1% after expenses, according to Samboursky. He prefers teams with co-founders from Unit 8200 because it indicates that they have gone through difficult challenges together, he said. "There's incredible freedom to operate at such a young age, and the problems you're presented with are quite raw," said Yotam Segev, CEO of Cyera, which was created in

2021 by former Unit 8200 personnel. Cyera, like Wiz, checks cloud-based corporate files for potential data security issues. It raised \$300 million in April from investors, valuing the company at \$1.4 billion (Kruppa & Perry, 2024).

Segev founded Cyera in New York with Tamar Bar-Ilan, a fellow Unit 8200 veteran, to market cloud data security solutions he developed while in the military. When he started looking for finance, colleagues in the unit suggested he approach to venture financier Gili Raanan, an early backer of Wiz through his venture capital firm Cyberstarts, which is situated in the Israeli beach resort of Mikhmoret. Raanan became Cyera's initial investor (Kruppa & Perry, 2024).

Raanan later recommended Cyera to Sequoia's senior partner, Doug Leone. Leone has managed Sequoia's investments in four firms run by former Unit 8200 troops, all of which have received Cyberstarts funding.

When Sanaz Yashar, a fellow Unit 8200 soldier, was fundraising for her cybersecurity business Zafran, Segev suggested that she do the same and seek funding from Leone.

"He's almost from our own unit," Yashar remembered Segev saying about Leone.

"He's from the neighborhood."

Yashar, who arrived in Israel from Iran at the age of 17, was recruited into Unit 8200 while studying biology at Tel Aviv University. Early in the process, an officer led her to a windowless meeting room and demonstrated how to remotely access and intercept an Iranian military officer's equipment and communications."The adrenaline that you feel in your blood in that moment is not something I can compare to anything else," Yashar told the crowd. She worked for 15 years, eventually leading a department of analysts

Yashar said she sees more young people entering Unit 8200 because they believe it is the best way to become digital leaders. She was dismayed when recent registrants asked her about recruiting and compensation at computer companies when she came to give a lecture a few years ago.

"It's time to understand that the mission is more important than anything else, and the technology is just an enabler for the mission," Yashar told CNN (Kruppa & Perry, 2024).

Unit 8200 is a branch of Israel's military intelligence agency, Aman. It is especially adept at intercepting communications and electronic signals from foreign opponents like Iran. It also creates cybersecurity solutions to safeguard the nation's networks while invading others. The unit has played an important role in the country's recent battles, notably the current fight against Hamas in Gaza. At any given moment, many thousand Israelis serve in Unit 8200 as part of Israel's mandatory military duty, which begins at the age of 18. To get admitted, they must pass a number of technical tests and training courses. Not everyone concentrates on computer science. Alumni stated that they worked alongside professionals in language and physics (Kruppa & Perry, 2024).

## 2.4: Conclusion

The Israeli Defence Forces (IDF) represent a compelling case study of how national security imperatives can drive technological innovation in highly dynamic geopolitical environments. Facing multifaceted threats ranging from asymmetric warfare to advanced cyberattacks, Israel has strategically positioned innovation not merely as a support mechanism but as a central pillar of its defence doctrine. The integration of cutting-edge technologies, particularly those with dual-use potential, has allowed the IDF to maintain a qualitative edge, enabling both offensive capabilities and defensive resilience in an increasingly contested region.

This technological trajectory has been deeply supported by the broader Israeli innovation ecosystem, where close collaboration between military institutions, academia, and private start-ups fosters a fertile environment for the rapid development and deployment of novel solutions. The convergence of civil and military innovation has blurred traditional boundaries and created a virtuous cycle of knowledge exchange, funding, and talent acquisition that reinforces Israel's strategic autonomy.

However, the path forward is not without challenges. The IDF must navigate a complex landscape of ethical concerns, regulatory constraints, and the ever-present risk of technological overreliance. Furthermore, ensuring interoperability, cybersecurity, and the scalability of new systems remains critical for long-term sustainability. As future conflicts are likely to be defined as much by bytes as by bullets, the IDF's capacity to anticipate change and remain agile in its innovation efforts will be essential.

Ultimately, the Israeli experience underscores the broader relevance of innovation as a strategic asset, not only for national defence but also for shaping geopolitical influence and deterrence. It demonstrates that in a world defined by rapid disruption and hybrid threats, technological superiority is no longer a luxury, but a necessity.

## Chapter 3: Technology Innovation and Italian Defence Forces

### 3.1: The disruptive evolution of European geopolitical context

In recent years, the geopolitical context of Europe has undergone a profound transformation. This shift, which many scholars and analysts characterize as disruptive, has been catalyzed by a confluence of historical ruptures, global power realignments, technological upheavals, and ideological divergence. The Russian invasion of Ukraine in 2022 marked a definitive rupture in the post-Cold War European security architecture, but the roots of the disruption stretch far deeper, into the evolving dynamics of transatlantic relations, the rise of geoeconomics, and the fragility of multilateral institutions.

For three decades following the collapse of the Soviet Union, Europe largely embraced a normative order based on liberal democratic values, multilateralism, and economic interdependence. This era, often called the post-Cold War settlement, was characterized by the enlargement of the European Union and NATO, the diffusion of globalized capitalism, and a belief in the "end of history" thesis (Fukuyama, 1992).

However, this consensus began to fray with events such as the 2008 global financial crisis, the Eurozone sovereign debt crises, Brexit, and the resurgence of authoritarianism. The invasion of Ukraine in 2014 and the full-scale war launched in 2022 shattered the illusion that Europe was immune to conventional military conflict. It also revealed the vulnerability of Europe's energy dependence,

institutional complacency, and military underinvestment (Brattberg & Hamilton, 2022).

The 2022 invasion acted as a geopolitical catalyst. It reinvigorated NATO, prompted historic shifts in countries like Sweden and Finland, and elevated defence and deterrence to the top of the European policy agenda. According to High Representative Josep Borrell, Europe had entered a "geopolitical awakening," requiring it to "learn to speak the language of power" (Borrell, 2022).

In response to new geopolitical threats, the European Union has increasingly turned to the concept of "strategic autonomy." Initially an economic doctrine aimed at reducing reliance on foreign technology and supply chains, it has evolved into a broader geopolitical strategy encompassing defence, digital sovereignty, and energy independence (Lippert, von Ondarza & Perthes, 2019).

The COVID-19 pandemic and the war in Ukraine further demonstrated the fragility of globalized supply chains. In response, the EU has promoted reshoring, critical infrastructure protection, and the diversification of strategic dependencies (Leonard et al., 2023). The European Defence Fund, Permanent Structured Cooperation (PESCO), and other initiatives now aim to enhance the EU's capabilities in defence technology and crisis response.

Yet, strategic autonomy is not without controversy. Eastern European states, in particular, remain wary of decoupling from the United States, viewing NATO as the only credible guarantor of their security. This divergence underscores a fundamental challenge: Europe's geopolitical response remains fragmented across national interests, historical memories, and threat perceptions (Martill & Sus, 2020).

One of the most disruptive aspects of the new geopolitical era is the expansion of conflict beyond traditional military dimensions. Russia's hybrid warfare; which includes cyberattacks, energy blackmail, disinformation campaigns, and support for extremist political movements, has blurred the lines between war and peace, combatant and civilian, foreign and domestic (Galeotti, 2016).

The European Union has sought to respond with tools like the Strategic Compass, cyber defence initiatives, and the European Centre of Excellence for Countering

Hybrid Threats. Nonetheless, vulnerabilities remain acute, especially in the domains of digital infrastructure, satellite communications, and critical energy supply (Fiott, 2022).

Concurrently, the geopolitical rivalry has shifted toward the economic domain. The weaponization of trade, the politicization of technology standards, and the battle over critical raw materials have given rise to a new era of geoeconomic competition. The EU's Carbon Border Adjustment Mechanism (CBAM), its regulation of digital platforms, and initiatives like the European Chips Act reflect a growing willingness to project power through regulatory and industrial policy (Schuette, 2022).

Europe's multilateral institutions, NATO, the EU, the OSCE, have been forced to adapt quickly. NATO has revived its deterrence mission, expanded its eastern presence, and deepened interoperability. The EU has adopted the Recovery and Resilience Facility, green industrial policy, and foreign policy sanctions with unprecedented speed and cohesion.

At the same time, new institutional configurations are emerging. The European Political Community (EPC), launched in 2022, provides a platform for EU and non-EU states to coordinate on shared security and political goals. Informal coalitions, such as the Weimar Triangle (France, Germany, Poland), the Visegrád Group, and the Nordic Defence Cooperation, offer more agile responses to regional challenges (Emerson, 2023).

Yet the crisis has also exposed institutional limits. The EU's foreign policy still requires unanimity, making it susceptible to vetoes. Hungary's obstructionism, divisions over China policy, and reluctance among some states to increase defence spending reveal the difficulty of forging a coherent grand strategy (Bayer & Brzozowski, 2022).

Internally, Europe faces growing political fragmentation. The rise of populist and nationalist parties in Italy, Hungary, France, and elsewhere has challenged pro-EU consensus and complicated coordinated foreign policy. Misinformation, economic grievances, and identity politics feed polarization, weakening the domestic

consensus for strategic investment and international cooperation (Inglehart & Norris, 2017).

Nevertheless, democratic resilience should not be underestimated. Civil societies have mobilized in support of Ukraine. Media and academia continue to expose disinformation and autocratic influence. European electorates, while volatile, have largely upheld support for liberal democracy, NATO membership, and climate action. The European Parliament has shown increasing assertiveness in upholding the rule of law and protecting minority rights (Kelemen, 2020).

The disruptive evolution of the European geopolitical context reflects a convergence of systemic shocks, strategic realignments, and internal reconfigurations. From the ashes of the post-Cold War order, a new multipolar, contested, and hybrid geopolitical landscape is emerging. Europe must navigate this transformation by reinforcing its strategic autonomy, modernizing its institutions, securing democratic resilience, and cultivating flexible partnerships within and beyond its borders.

Success will depend not only on hard power, but also on the capacity to innovate diplomatically, regulate assertively, and lead normatively. In this sense, Europe's geopolitical disruption is not only a crisis, but also a crucible, one in which its future strategic identity will be forged.

### 3.1.1 The Italian case

Italy occupies a complex position in Europe's evolving strategic landscape, caught between fiscal constraints, alliance commitments, and domestic skepticism. Its evolving posture encapsulates broader tensions surrounding European strategic autonomy, NATO reliance, and geopolitical ambition.

In 2024, Italy's defence outlays reached approximately 1.49 % of GDP, marginally below the NATO benchmark of 2 % (Politico, 2025). Prime Minister Giorgia Meloni affirmed that Italy will meet the 2 % target through accounting adjustments, such as including coast guard and military pension costs, and intends to gradually increase

up to 5 % of GDP by 2035, though crucially only 3.5 % would go to core defence, with the remainder allocated to broader security (Reuters, 2025a; Reuters, 2025b).

These commitments carry significant fiscal challenges: Italy's public debt centers around 135 % of GDP, and rising defence investments risk infringing EU deficit thresholds (Reuters, 2025a). Accordingly, Rome has advocated for greater flexibility in EU budget rules to accommodate increased military spending without triggering sanctions (FT, 2025).

Italian public sentiment remains largely opposed to military expansion. Only 26 % support redirecting funds toward defence, and only 16 % of young adults would volunteer to fight for the country (Reuters, 2025b). Yet, 58 % support stronger EU defence integration, while 49 % back NATO reinforcement (Reuters, 2025b).

Domestically, political fault lines complicate consensus. Deputy Prime Minister Matteo Salvini and others strongly resist further military commitments, while Foreign Minister Antonio Tajani and Meloni support incremental European rearmament (Comini, 2025). This internal dissonance poses a long-term challenge to policy coherence.

Italy's leadership is aligned with EU initiatives such as Readiness 2030 (formerly "ReArm Europe"), which aims to mobilize up to €800 billion in joint defence investments (Wikipedia, 2025). Although Italian officials initially voiced reservations, they have since agreed to a gradual implementation timeline extending to 2035, while requesting annual flexibility (Reuters, 2025a; Agenzia Nova, 2025).

Italy also favors institutional innovation through formats such as the Weimar+ security dialogue, and plays a role in European procurement frameworks like PESCO and the Strategic Compass (Agenzia Nova, 2025; Wikipedia, 2025).

Despite notable companies like Leonardo and Fincantieri, Italy's defence sector is undermined by weak operational readiness and underinvestment in force structure (GlobalData via Airforce-Technology, 2025). A recent intelligence report observed that personnel costs account for nearly 60 % of spending, leaving only 22 % for strategic acquisitions (leEuropeista, 2024). Efforts to boost procurement, e.g. naval

frigates, drones, are gaining traction, but long-term planning remains fragmented (Airforce-Technology, 2025).

Meeting NATO's defence commitment, especially scaling up to 3.5 % core defence and 5 % total security spending, will require Italy to mobilize at least €60 billion over the coming decade (Comini, 2025). While fiscal creativity (e.g. classifying infrastructure as defence) can help bridge short-term gaps, experts warn that substance must match form, notably in areas such as recruitment, infrastructure resilience, and capability modernization (Comini, 2025; Debuglies, 2025).

Italy's strategic dilemma is clear: balancing European autonomy, alliance credibility, and domestic legitimacy. Its future influence in Europe depends on delivering tangible enhancements in capability and aligning defence policy with broader institutional evolution.

### 3.2: The innovation framework adopted by Italian Defence Forces

Italy's Ministry of Defence has established a diversified innovation framework to modernize its armed forces. This framework integrates defence industrial policy, cyber and space command structures, partnerships with start-ups and SMEs, European cooperation, and emerging technologies such as AI and autonomous systems. Its strategic aims include enhancing operational capabilities, ensuring technological sovereignty, and aligning with NATO and EU modernization trends.

Since 2020–2021, Italy's MoD has advanced defence innovation through a dual-track strategy. First, it issued the Military Industry Directive, linking defence operational needs with industrial and R&D priorities. Second, it enacted reforms to align with the European Defence Fund (EDF) and strategic procurement guidelines (Marrone & Gilli, 2020). These reforms aim to improve the coherence between national capability development and multilateral acquisition strategies.

In 2020, Italy consolidated its cyber defence capabilities by creating the Network Operations Command - Comando per le Operazioni in Rete (COR). This unit combines both cyber defence and offensive operations, as well as command over military ICT infrastructure (NRDC-ITA, 2023; Real Istituto Elcano, 2024). It operates under the Joint Operations Command (COVI), unifying cyber, space, special operations, land, sea, and air domains (NRDC-ITA, 2023; Joint Operations Command information, 2025).

The creation of COR followed broader reforms including the establishment of the Italian National Cybersecurity Agency (ACN) in 2021 and the adoption of a National Cybersecurity Strategy (2022–2026), embedding the military cyber posture within a whole-of-government approach (Wikipedia ACN, 2025; Digital Watch, 2025).

Italy pioneered the establishment of a military Space Operations Command (COS) in 2020, making it one of the first in Europe (Real Istituto Elcano, 2024; Wikipedia COS, 2025). COS controls key military satellites such as SICRAL and COSMO-SkyMed and provides real-time space situational awareness (Real Istituto Elcano, 2024). A framework agreement with the Italian Space Agency (ASI) launched in 2023 strengthened civil-military cooperation in space research and training (ResearchItaly, 2023).

Italy promotes innovation by engaging start-ups and SMEs in defence technology. A notable example is Ephos, a NATO-backed chip start-up working on photonic chips. Ephos raised approximately €8.5 million to develop production facilities in Milan, supported by NATO's Defence Innovation Accelerator (Reuters, 2024). Similarly, Exein, a cybersecurity start-up focused on embedded device protection, raised €70 million in a 2025 funding round, reflecting growing domestic defence demand (Reuters, 2025).

Italian defence innovation is also driven by strategic partnerships:

- A joint venture between Leonardo and Rheinmetall (LRMV) to produce next-generation tanks (e.g. Panther KF51) under the Main Battle Tank programme (€8.2 billion budget 2025–38) (Reuters, 2024; Reddit, 2024).

- The Global Combat Air Programme (GCAP), a trilateral initiative between Italy, the UK, and Japan, intends to deliver a next-generation fighter jet by 2035. Italy's Defence Minister emphasized the importance of equitable technology sharing for national industrial benefit (Reuters, 2025).

Italy's recent defence innovation agenda is anchored in emerging domains - cyber, space, AI, and autonomous systems - that are integrated into a broader strategic analysis of its strengths and constraints.

Since 2020, Italy has established a dedicated Network Operations Command (COR) to centralize cyber-defence and offensive operations under the Joint Operations Command (COVI) (Wikipedia, 2025a). Originally known as the Joint Cybernetic Operations Command (CIOC), it was merged and restructured in 2020 to form COR, which now consolidates network security, ICT infrastructure, and cyber operations (Wikipedia, 2025a; Wikipedia, 2025b). COR's formation marked a doctrinal shift aligning Italy with NATO's multi-domain operational concept (Wikipedia, 2025a).

In parallel, Italy established the Space Operations Command (COS) in mid-2020 under the Ministry of Defence to manage military satellites—including COSMO-SkyMed and SICRAL, and integrate space operations into national planning (Wikipedia, 2025b). Operational exercises like Space Insider 23 demonstrated COS's role in cross-domain planning within complex joint drills conducted by the Air & Space Operations Command (Ministero della Difesa, 2023; Wikipedia, 2025b).

Italy has also invested in AI and autonomous systems through partnerships with start-ups. For example, Exein, a cybersecurity firm focusing on embedded device protection, raised €70 million in July 2025 amid growing defence demand (Reuters, 2025). Similarly, Ephos, a NATO-backed photonic-chip firm, secured \$8.5 million in September 2024 to scale operations in Milan, underscoring Italy's growing innovation ecosystem (Reuters, 2024).

### 3.2.1: Strategic Analysis: Strengths and Limitations

#### Strengths

1. **Integrated Command Structure:** The cohesive structure of COR and COS under COVI aligns Italy with NATO's multi-domain command vision and enhances operational coherence in cyber-space domains (Wikipedia, 2025a; Wikipedia, 2025b).
2. **Vibrant Public–Private Ecosystem:** Start-ups like Exein and Ephos exemplify Italy's ability to mobilize private innovation for defence use cases, connecting emerging technology sectors with national security demand (Reuters, 2025; Reuters, 2024).
3. **European Defence Partnerships:** Italian participation in European frameworks such as the Combined Space Operations Initiative (CSpO) and the European Defence Industrial Development Programme (EDIDP) demonstrates leadership in continental cooperation on space interoperability and command systems (Agenzia Nova, 2023; Ministero della Difesa, 2024).
4. **Early SSA Innovation Trials:** With Leonardo coordinating EDIDP-funded SSA initiatives like the INTEGRAL programme, Italy is advancing state-of-the-art space situational awareness tools leveraging AI-based modular command-and-control architectures (Ministero della Difesa, 2024).

#### Limitations

1. **Limited Research Funding:** Defence innovation in Italy is procurement-driven, with minimal foundational R&D investment or long-term strategy, limiting sustained innovation beyond initial pilots (Istituto Affari Internazionali, 2020).
2. **Institutional Fragmentation:** North–South regional disparities and compartmentalized governance structures hinder coherent scaling and

coordination of defence innovation across agencies (Loet Leydesdorff & Cucco, 2018).

3. Strategic Transparency Risks: Transparency International has flagged vulnerabilities in Italy's defence procurement process, where ad hoc policymaking and industry lobbying can undermine systematic planning (Transparency International Defence & Security, n.d.).
4. Cyber-AI Operational Gaps: Despite structural capacity, Italy still lags peers in mature deployment of Cyber and AI capabilities, with concerns over ethical, doctrinal, and technical readiness for naval and air force systems (Debugliesintel, 2025).

### 3.2.2 Exein and Ephos case

Italy's cybersecurity and photonics startups, Exein and Ephos, are delivering next-generation technology that strengthens national security through deep integration of private-sector innovation with public infrastructure and defence systems.

Founded in 2018 in Rome by Gianni Cuzzo, Exein develops AI-powered embedded cybersecurity software directly installed at the device level rather than relying on centralized, network-based protection mechanisms (Silicon Canals, 2024; EU-Startups, 2024). Their solution functions as a digital immune system: edge-based AI monitors and responds to threats in real time on the device itself, offering adaptive and proactive security (EU-Startups, 2024; Reuters, 2025).

By mid-2024, Exein protected over 80 million devices across industrial, automotive, aerospace, and infrastructure sectors (Silicon Canals, 2024). By mid-2025, following a €70 million Series C round led by Balderton, Exein estimated protection of over 1 billion devices, targeting triple-digit growth and expansion into the US, Asia, and Europe (EU-Startups, 2025; Reuters, 2025).

Strategic partnerships with major manufacturers—including MediaTek (supplying Exein's firmware across over 3 billion Genio chips), SECO, ARM, NVIDIA, Kontron, Daikin, and AAEON—anchor Exein's embedded security into critical global

infrastructure (Reuters, 2025; Silicon Canals, 2024). These alliances position Exein as a frontline security layer in systems increasingly central to public safety, from rail signalling to smart energy grids and defence support systems (EU-Startups, 2024; Reuters, 2025).

Exein's relevance to public security stems from its intrinsic device-level protection, which aligns with sovereign cybersecurity legislation such as the EU Cyber Resilience Act, NIS 2 directive, and ETSI and IEC standards; vital for regulated sectors including defence (EU-Startups, 2024; Reuters, 2025).

Ephos, based in Milan (with operations in San Francisco), specializes in pioneering photonic chips made of glass rather than silicon, offering faster, cooler, and denser optical connections; ideal for quantum computing, AI data centers, and secure communications (Reuters, 2024; WSJ, 2024).

In September 2024, Ephos raised \$8.5 million in a round led by Starlight Ventures and supported by NATO's Defence Innovation Accelerator (DIANA) with a €450,000 grant (Reuters, 2024). DiANA's backing underscores the strategic importance of photonic chips to NATO's future-proof infrastructure priorities.

Glass-based photonics reduce energy consumption significantly, operate at room temperature, and decrease signal loss; benefits critical for defence-grade systems requiring high throughput, low latency, and resilience (WSJ, 2024). Applications extend to encrypted military communications, resilient data transfer for satellite operations, and quantum-assisted computational tasks with national security implications (WSJ, 2024).

Both companies demonstrate how start-up agility and private innovation can strengthen public security:

1. Alignment with national security policies: Exein's edge-AI firmware supports compliance with EU regulations (e.g., NIS 2, CRA) required for critical infrastructure sectors (EU-Startups, 2024; Reuters, 2025).
2. Sovereignty and dual-use capacity: Ephos's glass photonics give Europe independent access to cutting-edge hardware, complementing strategic autonomy goals in quantum and defence systems (Reuters, 2024; WSJ, 2024).

3. NATO/EU recognition and investment: Exein's role in device-level defence and Ephos's backing via NATO DIANA point to official endorsement of their potential to uplift national and alliance-level resilience (Reuters, 2024; Reuters, 2025).

### 3.2.2: Dual Use technology in the Italian Innovation Framework

The concept of dual-use technology, innovations deployable in both civilian and military settings, forms a strategic linchpin for Italy's defence modernization aspirations. When integrated into national innovation policies and European funding schemes, dual-use solutions can both deepen Italy's innovation infrastructure and help meet ambitious GDP-based defence spending goals.

Dual-use technology enables public defence investments to yield civilian-sector benefits and vice versa. Analysts at the European Union Institute for Security Studies assert that increased defence budgets, aligned with NATO and the EU, offer a unique opportunity to spark "a dual-use Fourth Industrial Revolution tech boom" in Europe, including Italy (Teer & Spatafora, 2025). These investments support companies through early-stage financing barriers, creating "double dividends" by strengthening industrial competitiveness while fulfilling security needs.

Italy's innovation ecosystem, however, faces structural limitations. R&D spending remains low ( $\approx 0.76\%$  of GDP), far below the EU average, while patenting and technology transfer from public research institutions like CNR remain underdeveloped (EU Commission, 2025). By prioritizing dual-use solutions, Italy can more effectively leverage defence procurement as a tool to support private sector innovation, bridge fragmentation, and counterbalance the technology gap.

The Italian Ministry of Defence increasingly channels investments into dual-use R&D streams, distinct from pure military spending, as recommended by Di Camillo and Credi (2022). These dual-use lines facilitate interoperability, innovation, and flexible funding opportunities that do not compromise mission capabilities but strengthen cross-sector coordination.

At the European level, instruments such as the European Defence Fund (EDF), PESCO projects, and operational experimentation (e.g., through EDA frameworks) systematically encourage member states to embed civilian applicability into defence R&D initiatives. Companies like Exein and Ephos emerge from this environment, benefiting from both defence and commercial capital flows (Teer & Spatafora, 2025). Italy has also recently proposed an initiative, dubbed the European Security and Industrial Innovation Initiative, where just €17 billion of EU guarantees could catalyze up to €200 billion in dual-use and defence investments over five years (Reuters, 2025). This scheme illustrates how dual-use innovation can align with wider economic modernization and reduce public deficit pressure.

NATO and the EU's push toward future defence spending of 5% of GDP hinges crucially on the alignment of military and dual-use spending definitions. NATO already counts dual-use R&D and goods as legitimate defence expenditure when appropriately accounted for (Teer & Spatafora, 2025), enabling countries like Italy to reach targets without excessive core military build-up.

Italy's central bank governor cautions that arms production alone does not sustain long-term growth; instead, innovation-driven sectors produce lasting value (Panetta, 2025). Dual-use technology bridges that divide by enabling defence outlays to generate spillover benefits, improving productivity through R&D, fostering industrial competitiveness, and supporting job creation.

Further, investment models supported by public procurement frameworks and regional innovation programmes (e.g., Lombardy) can integrate dual-use criteria into procurement policy, stimulating demand for technology solutions with both civilian and defence utility (EU Commission, 2025).

### 3.2.3: Dual-Use Technology in Practice: Connecting Exein and Ephos to Italy's Defence Innovation and Spending Objectives

Exein's device-level cybersecurity, embedded directly into IoT and industrial control firmware, exemplifies dual-use innovation. Originally designed to protect commercial Internet-connected devices, such as smart meters and logistics sensors, Exein's platform was extended to safeguard defence communication nodes and critical infrastructure (Silicon Canals, 2024; Reuters, 2025). This extension required minimal hardware changes, leveraging the same AI-driven anomaly detection engine across civilian and military ecosystems (EU-Startups, 2024).

By classifying Exein's R&D and deployment under dual-use expenditures, Italy can count a portion of these costs toward its 2 % (and future 5 %) GDP defence spending targets under NATO definitions, without needing wholly new military-only hardware budgets (Teer & Spatafora, 2025). Simultaneously, civilian industries benefit from enhanced device resilience, creating broader economic spillovers (EU-Startups, 2025).

Ephos's glass-based photonic chips serve both commercial data centers and secure military communications, a quintessential dual-use outcome. Their ability to operate at room temperature with low energy consumption addresses civilian sustainability goals while meeting defence requirements for low-latency, high-bandwidth encrypted links (WSJ, 2024; Reuters, 2024).

Funding from NATO's DIANA program and EDF-linked grants counts as dual-use R&D. Italy thus leverages European co-funding mechanisms to reduce its direct defence R&D burden, helping it channel more of its GDP-linked budget into applied procurements (Teer & Spatafora, 2025). At the same time, Italy's broader economy gains from cutting-edge photonics in AI, 5G backhaul, and cloud computing markets (EU-Startups, 2024).

Integrating Exein and Ephos as dual-use pillars enables Italy's Ministry of Defence to reshape procurement:

- **Flexible Budgeting:** Dual-use classification allows portions of Exein's and Ephos's R&D to be co-financed via civilian innovation funds (e.g., Horizon Europe), reducing the impact on core defence budgets (Panetta, 2025).
- **Industrial Ecosystem Growth:** Successful scale-up of these start-ups fosters a national innovation cluster, improving Italy's low R&D intensity ( $\approx 0.76\%$  GDP) and narrowing the technology gap (EU Commission, 2025).
- **Meeting GDP Targets:** Counting qualifying dual-use R&D toward NATO/EU defence spending definitions helps Italy approach its 2 % and future 5 % GDP goals without unsustainable pure-military spending increases (Teer & Spatafora, 2025).

By harnessing Exein's embedded cybersecurity and Ephos's photonic capabilities under a dual-use approach, Italy can:

1. **Optimize Defence Outlays:** Redirect part of dual-use spending into public security without exacerbating debt ratios.
2. **Stimulate Spillover:** Enhance civilian sectors—energy, transport, telecommunications—through shared technology, supporting industrial competitiveness.
3. **Strengthen Sovereignty:** Develop indigenously controlled security-critical technologies, reducing reliance on external suppliers.

To consolidate these gains, Italy should formalize dual-use procurement guidelines, expand EU-cofunding partnerships, and integrate dual-use metrics into defence budget reporting, ensuring both innovation momentum and sustainable defence spending.

### 3.2.4: Italy–Israel Dual-Use Technology Cooperation: A Strategic Bridge for Innovation

Since the early 2000s, Italy and Israel have maintained a structured bilateral agreement focused on industrial, scientific, and technological cooperation, renewed every five years. This framework is especially relevant for dual-use innovation—technologies applicable in both civilian and defence contexts, and plays a strategic role in Italy’s high-tech and security policy landscape (MAECI, 2020; ResearchItaly, 2023).

Under the agreement, managed by a joint commission composed of Italian Ministry of Foreign Affairs representatives and the Israeli Innovation Authority (then MOST), collaborative R&D projects are selected and financed annually. The scope spans cybersecurity, ICT, space, optics, and critical infrastructure technologies (MAECI, 2020; E-002559/2025, European Parliament). Italian entities receive 50% of research funding; Israeli institutions are funded at 100% (ResearchItaly, 2023; InnovationIsrael, 2025). To date, over 220 joint projects have been funded, including 140 in industrial R&D—many with dual-use potential (MAECI, 2020).

The program actively promotes collaborative projects with civilian and defence application potential, including cybersecurity, quantum optics, encrypted communications, AI instrumentation, and space-based technologies. This structure encourages Italian start-ups and SMEs—leveraging Israeli technical expertise and joint acceleration programs overseen by MAECI and innovation partners (MAECI, 2020; ResearchItaly, 2023).

Italian start-ups like Exein (firmware-level cybersecurity) and Ephos (glass-based photonic chips) exemplify the types of innovators supported by the Italy–Israel framework:

- Exein’s embedded AI security platform aligns well with cyber-encryption projects supported under the bilateral calls, offering both industrial and defence utility.
- Ephos’s photonic chip technology complements Israeli strengths in quantum optics and secure communications, making it a fitting dual-use candidate for collaboration (Reuters, 2025; Reuters, 2024).

While there is no explicit evidence of either company participating in specific Italy–Israel projects yet, both fall within priority sectors and could be shortlisted by the joint commission for future dual-use R&D funding.

All cooperating projects undergo export control review under Italy’s UAMA licensing framework, in compliance with EU Regulation and national Law 185/90. Dual-use projects are subject to strict IP agreements, licensing limitations, and ethical scrutiny, particularly given concerns about military applicability (E-002559/2025, European Parliament; MAECI, 2020). The bilateral commission reviews content annually, though civil society observers have called for greater transparency and improved safeguards (Lancione, 2024; E-002559/2025).

The dual-use agreement fosters co-financed, cross-sector innovation by merging civilian and defence applications into a single collaborative mechanism. Joint R&D calls support technologies like cybersecurity, optics, space systems, and secure communications, which are relevant for both critical infrastructure and military resilience (MAECI, 2020; ResearchItaly, 2023). As a result, Italian start-ups such as Exein and Ephos—specializing in embedded cybersecurity and photonic hardware—are ideally positioned to benefit from joint technology transfer and co-development (Reuters, 2025; Reuters, 2024).

Through this mechanism, Italy improves access to Israeli innovation ecosystems, leveraging Israel’s high R&D intensity ( $\approx 5\%$  of GDP) and its mature start-up environment (ResearchItaly, 2023; Wikipedia, 2025). Bilateral projects enable debt-efficient technology transfers and institutional matchmaking that would otherwise require significantly larger domestic public investment.

Furthermore, co-funding by both governments reduces the burden on Italy's defence budget, allowing classification of qualifying R&D under dual-use spending. This practice helps Italy approach NATO's 2% GDP defence spending threshold, and even future 5% targets, by counting shared innovation costs without disproportionate core military expenditures (Teer & Spatafora, 2025).

The agreement also embeds institution-level oversight: a Joint Commission with representatives of MAECI, the Innovation Authority of Israel, MoD, and economic ministries evaluates and approves projects each year, supporting bilateral trust and regulatory compliance (MAECI, 2020; E-002559/2025).

Despite these strengths, the framework is criticized for limited transparency and public oversight. Italian academics and legal experts have raised objections around ethical risks posed by military applications of dual-use innovation, especially in light of Italy's constitutional and international obligations, calling for more visible governance structures and civil society engagement (Lancione, 2024; Palestine Chronicle, 2025).

Compliance processes are also complex: dual-use projects must clear export licensing under Italy's UAMA regulatory system, needing robust documentation, end-use restrictions, and inter-ministerial coordination. Critics warn that threats such as conflict escalation or misuse remain insufficiently managed (E-002559/2025; Reuters, 2024).

Additionally, the potential for strategic mismatch exists: not all dual-use projects yield meaningful defence utility, and not all military-grade innovations suit civilian scalability. This duality exposes projects to misalignment between industrial innovation objectives and defence strategic priorities.

Finally, stakeholder analysts note that while joint agreements enable co-funding, they do not guarantee robust commercialization or industrial scale-up. Italy's persistent regional disparities and weaknesses in R&D infrastructure limit national diffusion of innovation beyond isolated bilateral projects (Leydesdorff & Cucco, 2018).

### 3.3: How to build a Italian start-up ecosystem

The final section of Chapter 3 outlines a multifaceted strategy for constructing a high-functioning Italian start-up ecosystem rooted in dual-use innovation. Building on earlier analyses of the Italy–Israel cooperation model, and cases like Exein and Ephos, this plan sets the framework for aligning national policy, financing, infrastructure, human capital, and governance (MAECI, 2020; ResearchItaly, 2023; Teer & Spatafora, 2025). The overarching goal is to foster private startups capable of addressing both civilian needs and defence modernization, while enabling Italy to meet NATO/EU GDP-based defence spending targets.

#### 3.3.1: Legal and Institutional Foundations

Italy’s regulatory framework must evolve to support scalable innovation. Leveraging precedent set by the Italy–Israel dual-use calls, where eligible firms like Exein and Ephos require rapid IP agreements and export compliance, the government should reform the Innovation Authority towards a streamlined dual-use grant body (MAECI, 2020). A dedicated Dual-Use Innovation Agency would oversee project approval, manage ethics reviews, and coordinate export licensing under Law 185/90 and EU directives (Lancione, 2024). Furthermore, new regulations to standardize IP co-ownership, fast-track patents, and support technology transfer between research institutes and start-ups are critical to enable fluid innovation cycles.

Institutional architecture should establish a National Dual-Use R&D Fund, co-financed by MoD, MIUR, and the private sector, calibrated to match exemplary bilateral structures like the Italy–Israel Joint R&D Fund (InnovationIsrael, 2025). This modality ensures start-ups have access to seed and scale financing tied to defence-relevant innovation, while preserving public accountability. Alignment with

local innovation hubs in cities; enabling co-location of MoD labs and private firms—would foster synergies. These hubs should emulate Israeli techno-cyber innovation parks by integrating accelerators, academic labs, and pilot zones.

Given concerns raised by scholars and NGOs over dual-use agreements (Lancione, 2024; Palestine Chronicle, 2025), Italy must institutionalize ethical oversight. Each dual-use project should pass through an independent advisory board, including civil society representatives, legal experts, and scientific advisors, prior to approval. Annual public reporting on project objectives, ethical evaluations, and export uses should be mandated to ensure legitimacy and build societal trust.

### 3.3.2: Funding Infrastructure and Dual-Use Finance

To address the funding gap that persists in Italy’s innovation landscape, national venture capital schemes should be expanded and strategically aligned with dual-use priorities. Incentives such as public co-investment, reduced capital gains tax for dual-use seed rounds, and fast-track procurement eligibility can attract investors into sectors that straddle civil and defence applications (OECD, 2024).

Italy must better integrate start-ups into EU-level instruments such as the European Defence Fund (EDF), Horizon Europe clusters, and the EIC Accelerator. Many dual-use solutions, like Ephos’ photonic chips, can be scaled with EDF grants if classified correctly. A national taskforce should support proposal writing, matchmaking, and compliance processes to increase Italian absorption of European dual-use funding (Teer & Spatafora, 2025).

Italy’s university-linked incubators and regional accelerators must include defence innovation modules, supporting early-stage companies entering dual-use markets. Pilot programmes in cybersecurity (e.g., Exein) and optical engineering (e.g., Ephos) can be hosted at Milan Polytechnic, Sapienza, or CNR-affiliated labs. These accelerators should offer IP mentoring, regulatory guidance, and direct channels into procurement processes (EU-Startups, 2025).

National strategy should include clear financial KPIs: total private capital mobilized, number of dual-use start-ups exceeding €5M valuation, successful exits, and public-private deal volume. Monitoring these indicators will improve governance and attract sustained investor confidence (Panetta, 2025).

### 3.3.3: Funding Infrastructure and Dual-Use Finance

Italy must prioritize regional innovation ecosystems where start-ups can thrive. Milan, Turin, Rome, and Pisa should anchor clusters for cybersecurity, AI, aerospace, and quantum research. Southern Italy, often underrepresented, must benefit from public incentives to host new dual-use campuses, especially in regions with defence industrial assets (Leydesdorff & Cucco, 2018).

Establishing technology testbeds, especially for embedded security (Exein) and photonics (Ephos), can validate scalability and performance in real-world settings. Public transport systems, national energy grids, and telecom infrastructures offer natural environments for pilot trials. Coordination with defence institutions ensures dual-use validation pathways (EDA, 2025).

A federated network of testbeds, modeled on NATO DIANA experimentation nodes, should be established across Italy. This network can offer tiered environments, cyber ranges, satellite simulators, secure cloud deployments, where start-ups and SMEs test and refine technologies pre-commercialization (InnovationIsrael, 2025).

Bilateral agreements with Israel and Germany should include researcher exchange schemes. Co-funded fellowships allow Italian engineers and entrepreneurs to access Israeli defence-innovation parks or German Fraunhofer institutes, bringing back technical skills and management models (MAECI, 2020).

### 3.3.4: Human Capital, Talent and Mobility

Universities must develop new curricula focused on dual-use engineering: master's tracks in cybersecurity, AI governance, photonics, and autonomous systems should integrate defence use cases, ethical analysis, and export compliance knowledge. This helps build a workforce ready for high-trust, cross-sector work (OECD, 2024).

National fellowships modeled on Erasmus+ and Marie Curie schemes should enable dual-use entrepreneurs to spend time in Israeli or NATO-linked start-ups. These exchanges seed long-term collaborations and help start-ups localize best practices (ResearchItaly, 2023).

Italy must address brain drain by offering innovation visas for non-EU founders, stock options in lieu of salary for early employees, and simplified mechanisms for academic spin-outs to commercialize their research (Reuters, 2025).

### 3.3.5: Governance, Metrics and Strategic Alignment

KPIs must track technology readiness levels (TRLs), licensing activity, co-patenting across institutions, and defence procurement participation. Transparency dashboards should present ecosystem performance quarterly (Teer & Spatafora, 2025).

Italy can reach NATO's 2% GDP defence spending goal partly through dual-use R&D investments. By reclassifying civilian-facing innovations with verified defence applicability, budget pressures can be mitigated. This strategy supports both economic recovery and strategic autonomy (Panetta, 2025).

An inter-ministerial innovation council—integrating Defence, University, Industry, Foreign Affairs—should steer the ecosystem. It should ensure policy consistency, evaluate project performance, and coordinate with EU and NATO structures (MAECI, 2020).

Annual stakeholder consultations and citizen engagement exercises should be embedded to shape policy direction. These forums help balance innovation with ethics and respond to civil society concerns (Lancione, 2024).

### 3.3.6: Internationalization and Scaling

Italy should replicate its dual-use cooperation framework with countries beyond Israel—focusing on Germany, France, and the U.S.—to unlock market access and co-development opportunities. These agreements should include shared procurement pipelines and industrial consortia (MAECI, 2020).

Italian start-ups must play a central role in EU Defence consortia, contributing to European Defence Industrial Strategy and participating in EDF competitive calls. National support desks can help small firms prepare applications and consortia bids (Teer & Spatafora, 2025).

A national export desk for dual-use goods, coordinated with UAMA, should support SMEs navigating complex compliance while entering foreign markets. Start-ups like Exein and Ephos can be promoted as model exporters of Italian tech excellence (Reuters, 2025).

### 3.3.7: Case Studies Deep Dive

Exein is an Italian start-up founded in 2018 in Rome by cybersecurity entrepreneur Gianni Cuzzo. It has developed a firmware-level cybersecurity solution that functions as a “digital immune system” for devices connected to the Internet of Things (IoT). Exein's core innovation lies in embedding artificial intelligence into the device's firmware itself, allowing for real-time anomaly detection and preemptive response without needing centralized processing power (EU-Startups, 2025).

Initially targeting the industrial and embedded systems market, Exein quickly gained traction across sectors such as automotive, energy, critical infrastructure, and

telecommunications. The firm's dual-use potential became evident when it entered into partnerships with defence suppliers and participated in NATO-aligned security compliance programs. In 2025, Exein raised €70 million in a Series C funding round led by Balderton Capital, aimed at expanding operations across Europe, Asia, and the U.S. (Reuters, 2025).

From a dual-use perspective, Exein exemplifies how Italian start-ups can transition from civilian cybersecurity applications to military and national infrastructure use cases. By meeting regulatory standards such as NIS2 and the Cyber Resilience Act, and integrating its technology into MediaTek chips and Italian rail and energy systems, Exein has shown scalability and security at the edge. This trajectory underlines how public procurement, venture capital, and export support can converge in Italy's dual-use strategy.

The company's success also demonstrates the effectiveness of Italian-Israeli cooperation frameworks. Exein's embedded systems are particularly suited for integration into secure communication networks and defence logistics, areas that are of mutual interest in Italian-Israeli bilateral innovation calls. As a benchmark case, Exein represents the integration of deep tech, ethical compliance, and market relevance within the broader innovation ecosystem.

Ephos, headquartered in Milan with a secondary base in San Francisco, specializes in the design and manufacturing of glass-based photonic chips. Unlike traditional silicon photonics, Ephos's technology enables ultra-fast, low-heat data transmission via light, offering enormous efficiency gains for both high-performance computing and quantum communication (Reuters, 2024).

Founded by a team of physicists and engineers, Ephos operates at the frontier of semiconductor innovation, positioning itself as a critical enabler for defence applications, including satellite communications, secure networks, and signal processing systems. Its chips operate at room temperature, eliminating the need for cryogenic cooling systems, which is particularly advantageous in field deployments for military systems.

In 2024, Ephos raised \$8.5 million in early-stage funding supported by NATO's Defence Innovation Accelerator (DIANA), marking it as one of the few Italian startups to attract such recognition at the European level (Reuters, 2024). The firm is building its production capacity in Milan and integrating into both EU and transatlantic supply chains.

Ephos serves as a flagship example of Italy's potential in the dual-use semiconductor space. Its photonic chips have use cases ranging from encrypted defence communications to data centers managing critical civil services. The startup's trajectory also demonstrates how small, deep-tech firms can be anchored into national industrial strategies with relatively low capital expenditure, provided institutional frameworks like DIANA and EDF are leveraged effectively.

As a participant in the Italy-Israel innovation dialogue, Ephos benefits from potential synergies in quantum research and communications hardware. Its platform complements Israeli expertise in advanced optics and electronics, creating fertile ground for co-development in next-generation military applications and commercial infrastructure.

## Chapter 4: General Conclusion

In an era increasingly defined by geopolitical fragmentation, technological disruption, and rising threats to both global security and democratic resilience, the role of defence innovation has become not only strategic but existential. This thesis has investigated the multifaceted transformations shaping contemporary defence ecosystems, with a specific focus on dual-use technologies and the national innovation frameworks of Israel and Italy.

The comparative analysis between the Israeli and Italian cases reveals both divergences and complementarities. Israel's model, deeply rooted in a culture of risk tolerance, agile procurement, and strong civil–military integration, demonstrates how innovation can be systematically embedded into a national security doctrine (Senor & Singer, 2009). Initiatives such as Talpiot and the elite Unit 8200 have been instrumental not only in building a highly capable defence force, but also in laying the foundations for a globally competitive start-up ecosystem (Breznitz & Ornston, 2013). Dual-use innovation, in Israel, is not an exception but a systemic feature—facilitated by proactive government policy, elite education, and early-stage financing mechanisms (Avnimelech & Teubal, 2006).

Italy, in contrast, finds itself at a strategic crossroads. Despite the presence of strong academic institutions and industrial capabilities, its innovation ecosystem remains fragmented and often disconnected from defence imperatives (Leydesdorff & Cucco, 2018). Yet, recent developments—such as increasing investment through the European Defence Fund, the emergence of firms like Exein and Ephos, and bilateral frameworks like the Italy–Israel R&D Agreement—indicate a shifting momentum (Teer & Spatafora, 2025; MAECI, 2020; Reuters, 2025).

At the heart of this transformation lies the promise of deep tech dual-use innovation. This paradigm does not merely serve national defence objectives, but also functions as a catalyst for economic competitiveness, industrial resilience, and technological

sovereignty (EUISS, 2025). Italy's strategic challenge is to design institutional mechanisms that allow defence-related R&D to spill over into the civilian economy—stimulating productivity, supporting high-quality employment, and anchoring the country within Europe's broader technological value chain (OECD, 2024).

To that end, this thesis has explored how Italy might build a robust dual-use innovation ecosystem capable of mirroring some of the success factors found in Israel, while adapting them to its own political, cultural, and institutional context. The proposed roadmap includes legal and regulatory reforms, the establishment of public-private financing structures, regional innovation clusters, expanded experimentation networks, and a coherent talent development strategy. These elements, if properly integrated and sustained, can transform Italy from a passive technology adopter into a sovereign innovator within the broader European security-industrial complex.

Case studies such as Exein and Ephos provide valuable lessons. Exein has demonstrated how embedded cybersecurity, developed for industrial IoT applications, can be scaled into the defence domain through regulatory alignment and procurement integration. Ephos, on the other hand, offers a model for how next-generation photonics—developed for high-speed data centers—can serve military-grade communications and quantum computing. Both cases underscore the importance of having an agile institutional environment capable of identifying, supporting, and scaling dual-use technologies through early-stage support and transnational partnerships (EU-Startups, 2025; Reuters, 2024).

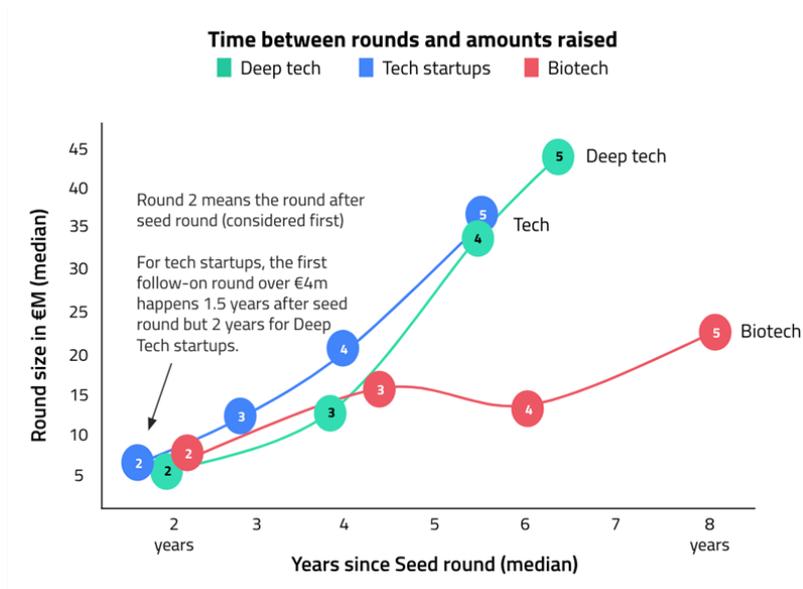
The implications of these findings are significant. Defence innovation must not be viewed as a siloed sector, but rather as a dynamic intersection of public investment, private entrepreneurship, and societal impact. Moreover, innovation governance should be guided by ethical principles and democratic accountability. The growing debate around dual-use research, particularly in light of military exports and geopolitical tensions, reinforces the need for transparency, civil oversight, and multilateral alignment (Lancione, 2024; Palestine Chronicle, 2025).

Furthermore, the convergence between civilian and military technological domains implies that innovation strategy and foreign policy are becoming increasingly interlinked. The design of future-proof national capabilities will depend not only on the strength of domestic institutions but also on international cooperation frameworks. In this context, Italy's participation in NATO's DIANA initiative, the EDF, and bilateral innovation agreements can serve as amplifiers of its innovation ecosystem, provided that coordination mechanisms are strengthened.

Ultimately, this thesis contends that innovation is inherently political. It reflects societal values, strategic ambitions, and institutional capacity. If Italy commits to building a coherent dual-use innovation strategy—grounded in ethics, sovereignty, and international collaboration—it can not only meet its defence obligations, but also assert its leadership in the evolving geopolitical-technological order. This journey will not be immediate, nor linear. Yet, with strategic vision, institutional resolve, and inclusive governance, Italy has the potential to become a key European hub for dual-use innovation—contributing not only to national security, but to the democratic resilience and technological autonomy of Europe as a whole.

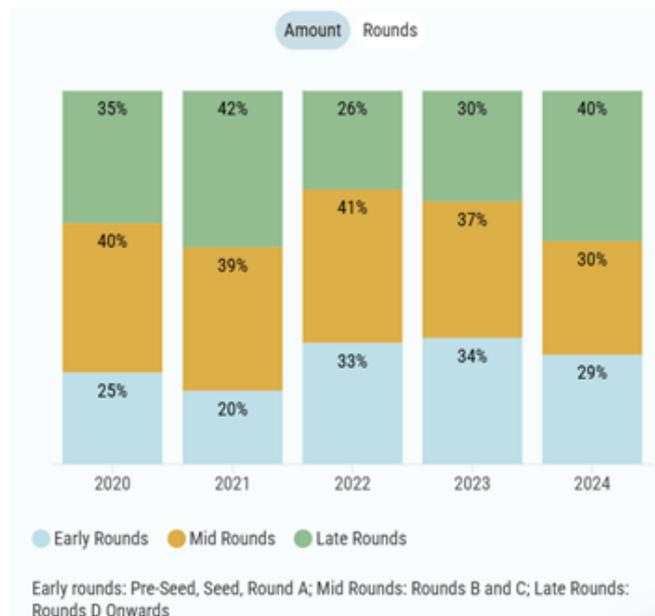
## Appendixes:

### Appendix A: Growth curves Deep Tech start-ups



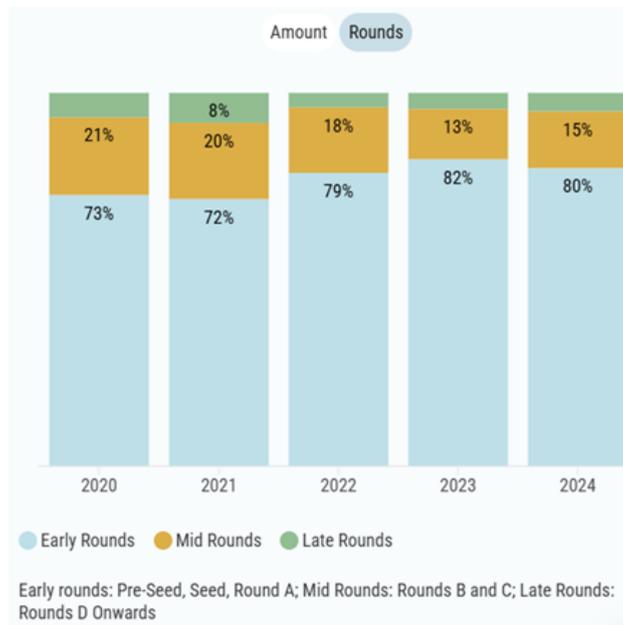
Source: *Wijngaarde, Y, 2022*

### Appendix B: Percentage of investments in the various stages



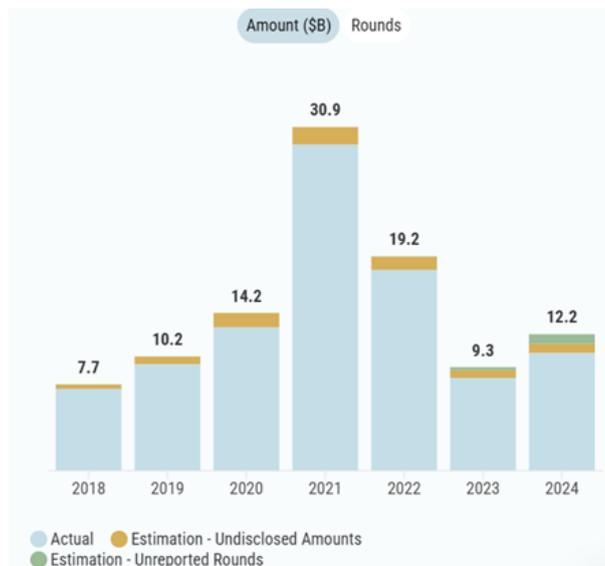
Source: *Startup Nation Central Annual Report 2024*

Appendix C: Percentage of investments in the various rounds.



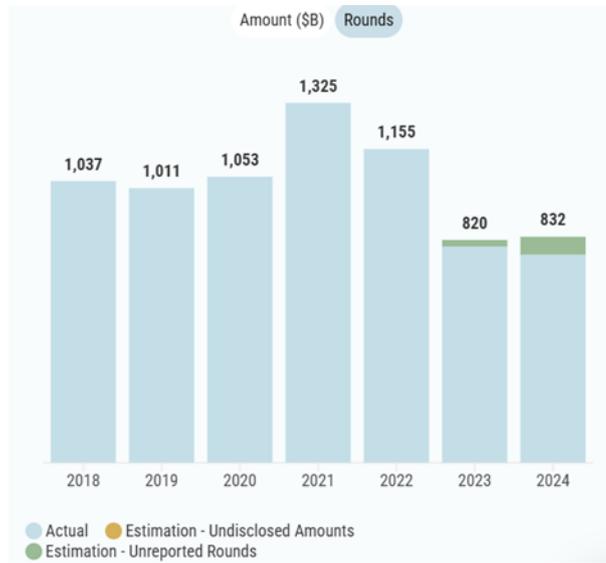
Source: *Startup Nation Central*  
*Annual Report 2024*

Appendix D: Number of billions of private foundations from 2018 to 2024



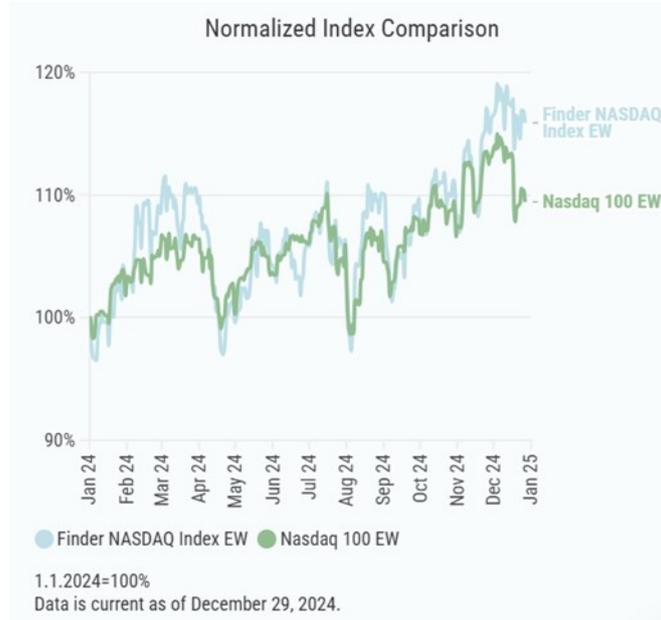
Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix E: Number of rounds of founding



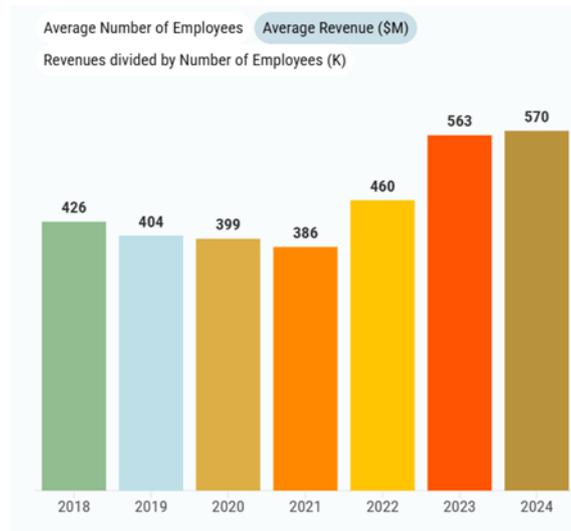
Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix F: Comparison between the two indexes



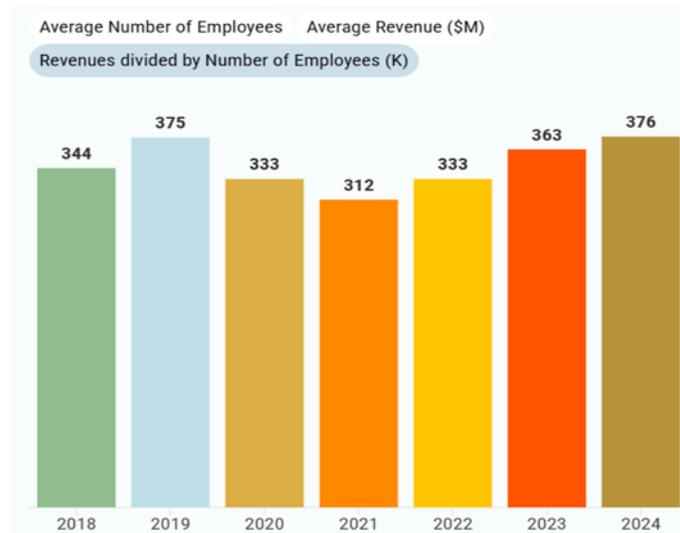
Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix G: Growing in the revenue



Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix H: Revenue concerning the number of employees



Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix I: Growth of exporting

Growth Components	Q1-Q3 2024	Q1-Q3 2024 vs. Q1-Q3 2023 Growth Rate
High-tech export per employee (NIS)	511K	2.2%
High-tech GDP per employee (NIS) *	632K	2.2%
High-tech employment	394K	-0.7%
High-tech GDP (Million NIS, 2015 Prices) *	249K	1.5%
Total GDP (Million NIS, 2015 Prices)	1,205K	-1.5%

\* Estimate

Source: *Startup Nation Central*  
*Annual Report 2024*

## Appendix J: Employer's growth

Number of employees by Profession	Q1-Q3 2024	Q1-Q3 2024 vs. Q1-Q3 2023 Growth Rate
R&D Employees	200.6K	4.9%
Product, QA, Data	81.5K	-4.8%
Business, Administrative	112.2K	-6.8%
High-tech employment	394.3K	-0.7%

Source: *Startup Nation Central*  
*Annual Report 2024*

## Bibliography:

Peña, I., & Jenik, M. (2023). Deep Tech: The New Wave. Inter-American Development Bank. <https://doi.org/10.18235/0004947>

Breaking Defence. (2024, December 18). Israel's Ministry of Defence pours money into start-ups. Breaking Defence. <http://breakingdefence.com/2024/12/israels-ministry-of-defence-pours-money-into-start-ups/>

Human Rights Watch. (2024, September 10). Gaza: Israeli military's digital tools risk civilian harm. Human Rights Watch. <https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm>

Strategy International. (2024, November 21). Publication 150. Strategy International. <https://strategyinternational.org/2024/11/21/publication150/>

The International Institute for Strategic Studies. (2023, October 10). Israel's fixation on technology created an illusion of safety. The International Institute for Strategic Studies. <https://www.iiss.org/online-analysis/commentary/2023/10/israels-fixation-on-technology-created-an-illusion-of-safety/>

Aravantinos, E. (2024, 21 novembre). The fusion of technology and defence: Israel's military-technology complex. Strategy International. <https://strategyinternational.org/2024/11/21/publication150/>

Pagine Esteri. (2024, 5 aprile). Lavender, la macchina di intelligenza artificiale che dirige i bombardamenti di Israele su Gaza. Pagine Esteri. <https://pagineesteri.it/2024/04/05/primo-piano/lavender-la-macchina-di-intelligenza-artificiale-che-dirige-i-bombardamenti-di-israele-su-gaza/>

Lieber Institute. (2024, 8 gennaio). The Gospel of Lavender: AI, law, and armed conflict. Lieber Institute West Point. <https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict/>

Rafael Advanced Defence Systems Ltd. (n.d.). PUZZLE™: AI-Based Multi-Domain Intelligence Suite at Scale. Rafael. <https://www.rafael.co.il/system/puzzle/>

Rafael Advanced Defence Systems. (n.d.). iMILITE. Rafael Advanced Defence Systems. <https://www.rafael.co.il/system/imilite/>

Rafael Advanced Defence Systems. (n.d.). SIGNAL. Rafael Advanced Defence Systems. <https://www.rafael.co.il/system/signal/>

Rafael Advanced Defence Systems. (n.d.). TARGETS. Rafael Advanced Defence Systems. <https://www.rafael.co.il/system/targets/>

Rafael Advanced Defence Systems. (n.d.). FORCE. Rafael Advanced Defence Systems. <https://www.rafael.co.il/system/force/>

Incubit Ventures. (n.d.). About Incubit. Retrieved February 10, 2025, from <https://incubitventures.com/about/>

Elbit Systems. (n.d.). Elbit Systems Open Innovation. Retrieved February 10, 2025, from <https://elbitsystems.com/open-innovation-2/>

Elbit Systems. (2020, October 15). CENS Materials, a portfolio company of Incubit - Elbit Systems' deep-tech incubator, raises \$1.5 million. Retrieved February 10, 2025, from <https://elbitsystems.com/pr-new/cens-materials-a-portfolio-company-of-incubit-elbit-systems-deep-tech-incubator-raises-1-5-million/>

Bagnoli, C., & Portincaso, M. (2021). Il Deep Tech e l'innovazione aziendale.

Dionisio, E. A., et al. (2023). Innovazione e scalabilità nel Deep Tech.

Wijngaarde, Y. (2022). Curve di crescita e scalabilità delle startup Deep Tech.

Asia Pacific Defence Reporter. (2024, February 14). Rafael Advanced Defence Systems introduces PUZZLE intelligence suite. <https://asiapacificdefencereporter.com/rafael-advanced-defence-systems-introduces-puzzle-intelligence-suite/>

Startup Nation Central. (2024). Israeli Tech 2024 Annual Report: The Year of the Scale-Up Powerhouse. [Report]. Startup Nation Finder. <https://finder.startupnationcentral.org/reports/2024-annual-report>

Eliezer, E. (n.d.). Israeli Incubators and Accelerators Explained. LinkedIn. <https://www.linkedin.com/pulse/israeli-incubators-accelerators-explained-eyal-eliezer>

Browne, O. (2023, January 27). European Deep Tech Startups. Dealroom.co. <https://dealroom.co/blog/european-deep-tech-in-2023>

Cohen, G., Yeh, D., Secon, H., Zou, K., & Taylor, M., (2024, May). FOAK Guide: A playbook for first-of-a-kind climate tech projects, Sightline Climate.

Kask, J. & Linton, G. (2023), "Editorial: Five principles for overcoming obstacles in deep-tech startup journeys", *Journal of Small Business and Enterprise Development*, Vol. 30 No. 1, pp. 1-3. <https://doi.org/10.1108/JSBED-02-2023-477>

Nedayvoda, A., Mockel, P., & Graf, L. (2020). Deep tech solutions for emerging markets.

Paschkewitz, J., Courtaux, M., Patel, V., Candelon, F., & Gourévitch, A. (2022). What CEOs need to know about deep tech. BCG Global. <https://www.bcg.com/publications/2022/ceos-need-to-know-about-deep-technologies>

Romansanta, A., Ahmadova, G., Wareham, J., & Priego, L. P. (2022). Deep tech: Unveiling the foundations (august 21, 2021). ESADE Working Papers Series 276, doi: <https://doi.org/10.2139/ssrn.4009164>.

Romme, A. G. L. (2022). Against All Odds: How Eindhoven Emerged as a Deeptech Ecosystem. *Systems*, 10(4), 119. MDPI AG. Retrieved from <http://dx.doi.org/10.3390/systems10040119>

Siegel, J.E., Krishnan, S., (2020). Cultivating Invisible Impact with Deep Technology and Creative Destruction - Letter from Academia, *Journal of Innovation Management*, [www.open-jim.org](http://www.open-jim.org), 8(3), 6-19.

Carnegie Endowment for International Peace. (2024, July 17). Governing military AI amid a geopolitical minefield (R. Csernaton). Retrieved from <https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield> Carnegie Endowment

Clark, J. (2023, November 2). DOD releases AI adoption strategy. U.S. Department of Defence. Retrieved from <https://www.defence.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/> Dipartimento della Difesa

RAND Europe. (2024). Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence. Retrieved from [https://www.rand.org/pubs/research\\_reports/RRA3295-1.html](https://www.rand.org/pubs/research_reports/RRA3295-1.html) RAND

Reuters. (2024, October 24). White House presses gov't AI use with eye on security, guardrails. Reuters. Retrieved from <https://www.reuters.com/world/us/white-house-presses-govt-ai-use-with-eye-security-guardrails-2024-10-24/> reuters.com

Klempner, J., Rodriguez, C., & Swartz, D. (2024, February 22). A rising wave of tech disruptors: The future of defence innovation? McKinsey & Company. <https://www.mckinsey.com/industries/aerospace-and-defence/our-insights/a-rising-wave-of-tech-disruptors-the-future-of-defence-innovation>

Bessemer Venture Partners. (2024, January 28). Roadmap: Defence tech. Bessemer Venture Partners. <https://www.bvp.com/atlas/roadmap-defence-tech>

Alvarez-Aragones, P. (2024, September 2). The new arms race in dual-use technologies. IE Insights. <https://www.ie.edu/insights/articles/the-new-arms-race-in-dual-use-technologies/>

Balkus, B. (2024, January 26). The U.S. can learn from Israel's cognitive meritocracy. Palladium Magazine. <https://www.palladiummag.com/2024/01/26/the-u-s-can-learn-from-israels-cognitive-meritocracy/>

Rubin, R., Dulaney, C., & Pitcher, J. (2025, May 30). A new 'revenge tax' aimed at foreign investors is rattling Wall Street. The Wall Street Journal. <https://www.wsj.com/articles/SB118368825920758806>

All Israel News Staff. (2024, September 7). Silicon Valley reaps benefits from IDF's elite Military Intelligence Unit 8200. All Israel News. <https://allisraelnews.com/silicon-valley-reaps-benefits-from-idf-s-elite-military-intelligence-unit-8200>

Fitch, A. (2024, August 31). Silicon Valley's hot talent pipeline is an Israeli army unit. The Wall Street Journal. <https://www.wsj.com/tech/silicon-valleys-hot-talent-pipeline-is-an-israeli-army-unit-e8368b4d>

Bayer, L. & Brzozowski, A. (2022). "Hungary continues to block EU response to Ukraine invasion." Euractiv.

Borrell, J. (2022). *Europe's Geopolitical Awakening*. European External Action Service.

Brattberg, E., & Hamilton, D. S. (2022). *The Transatlantic Response to Russia's War on Ukraine: Unity Amid Complexity*. Atlantic Council.

Emerson, M. (2023). *The European Political Community: A New Format for Geopolitical Cooperation*. CEPS Policy Briefs.

Fiott, D. (2022). *Defending Europe: Dual-Use Technologies and Hybrid Threats*. EU Institute for Security Studies.

Fukuyama, F. (1992). *The End of History and the Last Man*. Free Press.

Galeotti, M. (2016). "Hybrid War or Gibrinaya Voyna? Getting Russia's Non-Linear Military Challenge Right." *Parameters*, 45(4), 42–51.

Inglehart, R., & Norris, P. (2017). *Cultural Backlash: Trump, Brexit, and Authoritarian Populism*. Cambridge University Press.

Kelemen, R. D. (2020). "The European Union's Authoritarian Equilibrium." *Journal of European Public Policy*, 27(3), 481-499.

Leonard, M., Pisani-Ferry, J., Ribakova, E., Shapiro, J., & Wolff, G. B. (2023). *The Geopolitics of European Strategic Autonomy*. Bruegel.

Lippert, B., von Ondarza, N., & Perthes, V. (2019). *European Strategic Autonomy: Actors, Issues, Conflicts of Interests*. Stiftung Wissenschaft und Politik.

Martill, B., & Sus, M. (2020). "Post-Brexit EU/UK security cooperation: NATO, PESCO and beyond." *European Security*, 29(4), 455–474.

Schuetz, L. (2022). "EU Geoeconomics: Reasserting Power through Regulation." *Global Affairs*, 8(1), 89–106.

Agenzia Nova. (2025, June 12). *NATO: Ten years to reach 5 percent target, Italy asks for flexibility on defence spending*. Agenzia Nova.

Comini, N. (2025, July 9). *NATO's 5 % defence pledge and Italy: Can it? Will it? Europe's Edge*, Center for European Policy Analysis.

Debuglies. (2025). *Italy's Military Posture: Technological Gaps, Strategic Ambiguity and National Security Imperatives*. Debugliesintel.

FT. (2025, February–May). Italy optimistic EU will relax fiscal rules to boost defence spending [Financial Times].

GlobalData via Airforce-Technology. (2025). Italy struggles to meet NATO 2% target says report. Airforce-Technology.

leEuropeista. (2024, December 2). Italian defence spending: In 2027 it will only reach 1.6% of GDP.

Politico. (2025, June 25). Italy to hit NATO spending target this year as Meloni preps for Trump meeting.

Reuters. (2025a, June 23). Italy to gradually meet new NATO spending target, seeks new EU budget rules.

Reuters. (2025b, July 18). Only 16% of Italians would fight for their country, survey shows.

Wikipedia. (2025). Readiness 2030. In Wikipedia. Retrieved July 2025, from Readiness 2030 page.

Wikipedia. (2025). Agreement on 5% NATO defence spending by 2035. In Wikipedia. Retrieved July 2025, from Agreement on 5% NATO defence spending by 2035 page.

Debugliesintel. (2025). Italy's military posture: Technological gaps, strategic ambiguity and national security imperatives. Debugliesintel.

Istituto Affari Internazionali. (2020). Defence innovation: New models and procurement implications. The Italian case (Ares Policy Paper No. 74). IAI.

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North–South divide in Italy [Preprint]. arXiv.

Ministero della Difesa. (2023). Space Insider 23: Comando delle Operazioni Spaziali exercises new multi-domain scenarios. Ministero della Difesa.

Ministero della Difesa. (2024). Florence hosts the Combined Space Operations meeting. Ministero della Difesa.

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters.

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters.

Transparency International Defence & Security. (n.d.). Defence industry influence on policy agendas: Germany and Italy case study. Transparency International.

Wikipedia. (2025a). Network Operations Command (Italy). In Wikipedia. Retrieved July 2025, from [https://en.wikipedia.org/wiki/Network\\_Operations\\_Command\\_\(Italy\)](https://en.wikipedia.org/wiki/Network_Operations_Command_(Italy))

Wikipedia. (2025b). Space Operations Command (Italy). In Wikipedia. Retrieved July 2025, from [https://en.wikipedia.org/wiki/Space\\_Operations\\_Command\\_\(Italy\)](https://en.wikipedia.org/wiki/Space_Operations_Command_(Italy))

EU-Startups. (2024, July 12). Rome-based Exein raises €15 million aiming to set a global standard for embedded cybersecurity. EU-Startups. Retrieved from <https://www.eu-startups.com/2024/07/rome-based-exein-raises-e15-million-aiming-to-set-a-global-standard-for-embedded-cybersecurity/>

EU-Startups. (2025, July 16). Italian startup Exein raises €70 million to build the “immune system for digital life”. EU-Startups. Retrieved from <https://www.eu-startups.com/2025/07/italian-startup-exein-raises-e70-million-to-build-the-immune-system-for-digital-life/>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters. Retrieved from <https://www.reuters.com/technology/italian-cybersecurity-firm-exein-sees-defence-boost-it-closes-funding-round-2025-07-16/>

Reuters. (2025, January 29). Italian startup Exein to supply cybersecurity for chips to MediaTek. Reuters. Retrieved from <https://www.reuters.com/technology/cybersecurity/italian-startup-exein-supply-cybersecurity-chips-mediatek-2025-01-29/>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/nato-backed-chip-startup-ephos-raises-85-mln-italian-operations-2024-09-23/>

WSJ. (2024, November 26). Glass chips offer hope of cleaner future for quantum computing. The Wall Street Journal. Retrieved from

<https://www.wsj.com/articles/glass-chips-offer-hope-of-cleaner-future-for-quantum-computing-9c72a806>

Silicon Canals. (2024, July 12). Italy's embedded IoT cybersecurity firm Exein raises €15M. Silicon Canals. Retrieved from <https://siliconcanals.com/italy-based-exein-raises-e15m/>

Reddit user commentary. (2024, November 11). European investment in photonic semiconductors [Reddit]. Retrieved from Reddit (non-linked source).

Abramo, G., & D'Angelo, C. A. (2018). The alignment of public research supply and industry demand for effective technology transfer: The case of Italy. arXiv. Retrieved from <https://arxiv.org/abs/1812.09128>

Di Camillo, F., & Credi, O. (2022). Fattori d'impatto sull'innovazione tecnologica e sviluppo di capacità Dual-use della Difesa. Istituto Affari Internazionali. Retrieved from <https://www.iai.it/en/pubblicazioni/c09/fattori-dimpatto-sullinnovazione-tecnologica-e-sviluppo-capacita-dual-use-della>

European Commission. (2025). Rethinking investment in innovation. In European Innovation Scoreboard Report (Chapter on Italy). Publications Office of the EU. Retrieved from [https://publications.europa.eu/resource/cellar/.../DOC\\_1](https://publications.europa.eu/resource/cellar/.../DOC_1)

Panetta, F. (2025, January 16). Military output doesn't help long-term growth. Reuters news article summarizing speech by Bank of Italy governor Fabio Panetta. Retrieved from <https://www.reuters.com/markets/europe/military-spending-doesnt-help-long-term-growth-italys-central-bank-chief-says-2025-01-16/>

Teer, J., & Spatafora, G. (2025, July 3). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. European Union Institute for Security Studies. Retrieved from <https://www.iss.europa.eu/publications/briefs/when-stars-align-leveraging-european-defence-budgets-drive-dual-use-tech-boom>

Reuters. (2025, March 10). Italy pushes for 200-bln-euro defence plan using EU guarantees. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/italy-pushes-200-bln-euro-defence-plan-using-eu-guarantees-2025-03-10>

Reddit user commentary. (2025, March 13). Italy proposes European guarantee fund to stimulate private investment in defence. Army Recognition. (via Reddit). Retrieved from <https://www.reddit.com/r/WorldDefenceNews/comments/1jaalbs>

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North-South divide in Italy. arXiv. Retrieved from <https://arxiv.org/abs/1805.11821>

EU-Startups. (2024, July 12). Rome-based Exein raises €15 million aiming to set a global standard for embedded cybersecurity. EU-Startups. Retrieved from <https://www.eu-startups.com/2024/07/rome-based-exein-raises-e15-million-aiming-to-set-a-global-standard-for-embedded-cybersecurity/>

EU-Startups. (2025, July 16). Italian startup Exein raises €70 million to build the “immune system for digital life”. EU-Startups. Retrieved from <https://www.eu-startups.com/2025/07/italian-startup-exein-raises-e70-million-to-build-the-immune-system-for-digital-life/>

Panetta, F. (2025, January 16). Military output doesn't help long-term growth. Reuters. Retrieved from <https://www.reuters.com/markets/europe/military-spending-doesnt-help-long-term-growth-italys-central-bank-chief-says-2025-01-16/>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/nato-backed-chip-startup-ephos-raises-85-mln-italian-operations-2024-09-23/>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters. Retrieved from <https://www.reuters.com/technology/italian-cybersecurity-firm-exein-sees-defence-boost-it-closes-funding-round-2025-07-16/>

Teer, J., & Spatafora, G. (2025, July 3). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. European Union Institute for Security Studies. Retrieved from <https://www.iss.europa.eu/publications/briefs/when-stars-align-leveraging-european-defence-budgets-drive-dual-use-tech-boom>

WSJ. (2024, November 26). Glass chips offer hope of cleaner future for quantum computing. The Wall Street Journal. Retrieved from <https://www.wsj.com/articles/glass-chips-offer-hope-of-cleaner-future-for-quantum-computing-9c72a806>

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North-South divide in Italy [Preprint]. arXiv. Retrieved from <https://arxiv.org/abs/1805.11821>

Lancione, M. (2024, April 8). Academic objections to dual-use scientific cooperation with Israel. Michele Lancione's blog. Retrieved from <https://www.michelelancione.eu/blog/2024/04/08/interviews-on-the-academic-boycott-against-israel-new-work-to-stop-dual-use-agreement-with-italy-maeci/>

MAECI (Ministry of Foreign Affairs & International Cooperation). (2020, July 2). Annual Joint Commission meeting of the Italy-Israel industrial, scientific and technological cooperation agreement. MAECI. Retrieved from [https://www.esteri.it/en/sala\\_stampa/archivionotizie/approfondimenti/2020/07/italia-israele-riunione-annuale-della-commissione-mista-dell'accordo-di-cooperazione-industriale-scientifica-e-tecnologica/](https://www.esteri.it/en/sala_stampa/archivionotizie/approfondimenti/2020/07/italia-israele-riunione-annuale-della-commissione-mista-dell'accordo-di-cooperazione-industriale-scientifica-e-tecnologica/)

Palestine Chronicle. (2025, May 21). Formal notice to government regarding renewal of military MoU with Israel. Palestine Chronicle. Retrieved from <https://www.palestinechronicle.com/italy-israel-defence-agreement-italian-lawyers-file-complaint-with-government/>

ResearchItaly. (2023, May 12). Italy-Israel cooperation: new call for joint industrial research projects now open. RESEARCHITALY. Retrieved from <https://researchitaly.mur.gov.it/en/italy-israel-cooperation-new-call-for-proposals-for-joint-industrial-research-projects-now-open/>

Reuters. (2024, March 14). Italy arms exports to Israel continued despite block, minister says. Reuters. Retrieved from <https://www.reuters.com/world/europe/italy-arms-exports-israel-continued-despite-block-minister-says-2024-03-14/>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/nato-backed-chip-startup-ephos-raises-85-mln-italian-operations-2024-09-23/>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters. Retrieved from <https://www.reuters.com/technology/italian-cybersecurity-firm-exein-sees-defence-boost-it-closes-funding-round-2025-07-16/>

European Parliament. (2025). Written question E-002559/2025: Compliance of Italian exports of military technology to Israel (Council Common Position 2008/944/CFSP). Retrieved from [https://www.europarl.europa.eu/doceo/document/E-10-2025-002559\\_EN.html](https://www.europarl.europa.eu/doceo/document/E-10-2025-002559_EN.html)

Teer, J., & Spatafora, G. (2025, July 3). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. European Union Institute for Security Studies. Retrieved from <https://www.iss.europa.eu/publications/briefs/when-stars-align-leveraging-european-defence-budgets-drive-dual-use-tech-boom>

European Parliament. (2025). Written question E-002559/2025: Compliance of Italian exports of military technology to Israel (Council Common Position 2008/944/CFSP). Retrieved from [https://www.europarl.europa.eu/doceo/document/E-10-2025-002559\\_EN.html](https://www.europarl.europa.eu/doceo/document/E-10-2025-002559_EN.html)

InnovationIsrael. (2025, May 19). Italy-Israel Joint R&D Projects 2025: Call for proposals. Israel Innovation Authority. Retrieved from [https://innovationisrael.org.il/en/calls\\_for\\_proposal/italy-israel-projects-2025/](https://innovationisrael.org.il/en/calls_for_proposal/italy-israel-projects-2025/)

Lancione, M. (2024, April 8). Academic objections to dual-use scientific cooperation with Israel. Michele Lancione's blog. Retrieved from <https://www.michelelancione.eu/blog/2024/04/08/interviews-on-the-academic-boycott-against-israel-new-work-to-stop-dual-use-agreement-with-italy-maeci/>  
MAECI (Ministry of Foreign Affairs & International Cooperation). (2020, July 2). Annual Joint Commission meeting of the Italy–Israel industrial, scientific and technological cooperation agreement. MAECI. Retrieved from

[https://www.esteri.it/en/sala\\_stampa/archivionotizie/approfondimenti/2020/07/italia-israele-riunione-annuale-della-commissione-mista-dell'accordo-di-cooperazione-industriale-scientifica-e-tecnologica/](https://www.esteri.it/en/sala_stampa/archivionotizie/approfondimenti/2020/07/italia-israele-riunione-annuale-della-commissione-mista-dell'accordo-di-cooperazione-industriale-scientifica-e-tecnologica/)

ResearchItaly. (2023, May 12). Italy-Israel cooperation: new call for joint industrial research projects now open. RESEARCHITALY (Italian Ministry of University and Research). Retrieved from <https://researchitaly.mur.gov.it/en/italy-israel-cooperation-new-call-for-proposals-for-joint-industrial-research-projects-now-open/>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/nato-backed-chip-startup-ephos-raises-85-mln-italian-operations-2024-09-23/>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters. Retrieved from <https://www.reuters.com/technology/italian-cybersecurity-firm-exein-sees-defence-boost-it-closes-funding-round-2025-07-16/>

Wikipedia. (n.d.). Israel–Italy relations. In Wikipedia. Retrieved July 2025, from [https://en.wikipedia.org/wiki/Israel%E2%80%93Italy\\_relations](https://en.wikipedia.org/wiki/Israel%E2%80%93Italy_relations)

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North–South divide in Italy [Preprint]. arXiv. Retrieved from <https://arxiv.org/abs/1805.11821>

Lancione, M. (2024, April 8). Academic objections to dual-use scientific cooperation with Israel. Michele Lancione's blog. Retrieved from <https://www.michelelancione.eu/blog/2024/04/08/interviews-on-the-academic-boycott-against-israel-new-work-to-stop-dual-use-agreement-with-italy-maeci/>

MAECI (Ministry of Foreign Affairs & International Cooperation). (2020, July 2). Annual Joint Commission meeting of the Italy–Israel industrial, scientific and technological cooperation agreement. MAECI. Retrieved from [https://www.esteri.it/en/sala\\_stampa/archivionotizie/approfondimenti/2020/07](https://www.esteri.it/en/sala_stampa/archivionotizie/approfondimenti/2020/07)

[/italia-israele-riunione-annuale-della-commissione-mista-dell-accordo-di-cooperazione-industriale-scientifica-e-tecnologica/](#)

Palestine Chronicle. (2025, May 21). Formal notice to government regarding renewal of military MoU with Israel. Palestine Chronicle. Retrieved from <https://www.palestinechronicle.com/italy-israel-defence-agreement-italian-lawyers-file-complaint-with-government/>

ResearchItaly. (2023, May 12). Italy-Israel cooperation: new call for joint industrial research projects now open. RESEARCHITALY. Retrieved from <https://researchitaly.mur.gov.it/en/italy-israel-cooperation-new-call-for-proposals-for-joint-industrial-research-projects-now-open/>

Reuters. (2024, March 14). Italy arms exports to Israel continued despite block, minister says. Reuters. Retrieved from <https://www.reuters.com/world/europe/italy-arms-exports-israel-continued-despite-block-minister-says-2024-03-14/>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln for Italian operations. Reuters. Retrieved from <https://www.reuters.com/business/aerospace-defence/nato-backed-chip-startup-ephos-raises-85-mln-italian-operations-2024-09-23/>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. Reuters. Retrieved from <https://www.reuters.com/technology/italian-cybersecurity-firm-exein-sees-defence-boost-it-closes-funding-round-2025-07-16/>

European Parliament. (2025). Written question E-002559/2025: Compliance of Italian exports of military technology to Israel (Council Common Position 2008/944/CFSP). Retrieved from [https://www.europarl.europa.eu/doceo/document/E-10-2025-002559\\_EN.html](https://www.europarl.europa.eu/doceo/document/E-10-2025-002559_EN.html)

Teer, J., & Spatafora, G. (2025, July 3). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. European Union Institute for Security Studies. Retrieved from <https://www.iss.europa.eu/publications/briefs/when-stars-align-leveraging-european-defence-budgets-drive-dual-use-tech-boom>

EDA. (2025, February 13). EDA's first operational experimentation campaign for defence innovation takes off. <https://www.eda.europa.eu/info-hub/press-centre/latest-news/2025/02/13>

EU-Startups. (2025, July 16). Italian startup Exein raises €70 million to build the "immune system for digital life". <https://www.eu-startups.com/2025/07>

InnovationIsrael. (2025, May 19). Italy–Israel Joint R&D Projects 2025. [https://innovationisrael.org.il/en/calls\\_for\\_proposal](https://innovationisrael.org.il/en/calls_for_proposal)

Lancione, M. (2024, April 8). Academic objections to dual-use scientific cooperation with Israel. <https://www.michelelancione.eu/blog/2024/04/08>

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North–South divide in Italy. <https://arxiv.org/abs/1805.11821>

MAECI. (2020, July 2). Annual Joint Commission meeting of the Italy–Israel cooperation agreement. [https://www.esteri.it/en/sala\\_stampa/archivionotizie/approfondimenti/2020/07](https://www.esteri.it/en/sala_stampa/archivionotizie/approfondimenti/2020/07)

OECD. (2024). Italy Country Review: Innovation and Start-Up Policy. <https://www.oecd.org>

Palestine Chronicle. (2025, May 21). Formal notice to government regarding renewal of military MoU with Israel. <https://www.palestinechronicle.com>

Panetta, F. (2025, January 16). Military output doesn't help long-term growth. Reuters. <https://www.reuters.com/markets/europe>

ResearchItaly. (2023, May 12). Italy–Israel cooperation: new call for joint research. <https://researchitaly.mur.gov.it/en>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 mln. <https://www.reuters.com/business/aerospace-defence>

Reuters. (2025, July 16). Exein sees defence boost as it closes funding round. <https://www.reuters.com/technology>

Teer, J., & Spatafora, G. (2025, July 3). Leveraging European defence budgets to drive a dual-use tech boom. <https://www.iss.europa.eu/publications>

Avnimelech, G., & Teubal, M. (2006). Creating venture capital industries that co-evolve with high-tech: Insights from an extended industry life cycle perspective of

the Israeli experience. *Research Policy*, 35(10), 1477–1498.  
<https://doi.org/10.1016/j.respol.2006.09.005>

Breznitz, D., & Ornston, D. (2013). The revolutionary power of peripheral agencies: Explaining radical policy innovation in Finland and Israel. *Comparative Political Studies*, 46(10), 1219–1245. <https://doi.org/10.1177/0010414012463894>

Di Camillo, F., & Credi, O. (2022). Fattori d’impatto sull’innovazione tecnologica e sviluppo di capacità Dual-use della Difesa. Istituto Affari Internazionali. <https://www.iai.it/en/pubblicazioni/fattori-dimpatto-sullinnovazione-tecnologica-e-sviluppo-capacita-dual-use-della-difesa>

EUISS (European Union Institute for Security Studies). (2025). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. <https://www.iss.europa.eu/publications/briefs/when-stars-align-leveraging-european-defence-budgets-drive-dual-use-tech-boom>

EU-Startups. (2025, July 16). Italian startup Exein raises €70 million to build the “immune system for digital life”. <https://www.eu-startups.com/2025/07>

Lancione, M. (2024, April 8). Academic objections to dual-use scientific cooperation with Israel. <https://www.michelelancione.eu/blog/2024/04/08/interviews-on-the-academic-boycott-against-israel>

Leydesdorff, L., & Cucco, I. (2018). Regions, innovation systems, and the North–South divide in Italy. *Journal of Technology Transfer*, 43(4), 865–889. <https://doi.org/10.1007/s10961-017-9559-1>

MAECI. (2020, July 2). Annual Joint Commission meeting of the Italy–Israel cooperation agreement. [https://www.esteri.it/en/sala\\_stampa/archivionotizie/approfondimenti/2020/07](https://www.esteri.it/en/sala_stampa/archivionotizie/approfondimenti/2020/07)

OECD. (2024). Italy Country Review: Innovation and Start-Up Policy. <https://www.oecd.org>

Palestine Chronicle. (2025, May 21). Formal notice to government regarding renewal of military MoU with Israel. <https://www.palestinechronicle.com>

Reuters. (2024, September 23). NATO-backed chip startup Ephos raises \$8.5 million for Italian operations. <https://www.reuters.com/business/aerospace-defence>

Reuters. (2025, July 16). Italian cybersecurity firm Exein sees defence boost as it closes funding round. <https://www.reuters.com/technology>

Senor, D., & Singer, S. (2009). Start-Up Nation: The Story of Israel's Economic Miracle. Twelve.

Teer, J., & Spatafora, G. (2025, July 3). When stars align: Leveraging European defence budgets to drive a dual-use tech boom. EUISS. <https://www.iss.europa.eu/publications>