MARKETING OF SCIENTIFIC AND RESEARCH ORGANIZATIONS, 2025, Vol. 57, Issue 3, p. 67–79
pISSN 2353-8503
eISSN 2353-8414

FROM PROTOTYPE TO IMPLEMENTATION IN DUAL-USE KRAKOW TECHNOLOGY PARK AS A FACILITATOR AND AN INTERMEDIARY FOR IMPLEMENTATION

Bartosz Józefowski
Deputy Director, Technology Park Department, Krakow Technology Park (KPT),
60 Podole Str., 30-394 Krakow, Poland
E-mail: bjozefowski@kpt.krakow.pl

DOI: 10.2478/minib-2025-0014

ABSTRACT

This case study examines the implementation of dual-use technologies as an execution challenge, shaped by recurring barriers, including confidentiality and information constraints, testing and validation, regulatory compliance, controlled access to end users, and extended integration cycles. Against this backdrop, Krakow Technology Park (KPT) is described as a "platform of implementation instruments" that combines incubation, acceleration programs, DIH/EDIH services, seed-stage financing instruments, and brokerage functions and sector initiatives. Together, these elements form a pipeline that can support projects from the idea stage to piloting and scaling.

The core of the case study compares two facilitation pathways. The first is KPT ScaleUp Booster, where startup–Technology Recipient collaboration is organized around a milestone-based grant disbursed in tranches and a minimum governance package, including NDAs, IP clarification, infrastructure access, and liability requirements, non-compete provisions, and implementation priority rights. The second pathway is FORT Kraków, DIANA Accelerator Poland, launched in January 2026 as a joint initiative of AGH University of Science and Technology and KPT, and presented as the Polish node in the NATO DIANA network. The findings suggest that the operator's value stems primarily from combining pipeline, governance, and access to testing environments and end users, while also facing limitations such as lock-in risk, formal and administrative burden, and the need to clearly distinguish dual-use from arms trading.

Key words: dual-use technologies; technology transfer; technology implementation; defense innovation; NATO DIANA.

Type of the work: case study

Article History
Received: December 15, 2025 | **Revised:** April 13, 2026 | **Accepted:** June 12, 2026

1. Introduction: Dual-use as an implementation challenge: why dual-use technologies require an intermediary

Dual-use technologies: solutions with civilian applications that can also be deployed in defense and security, are increasingly becoming one of the key pathways through which innovation permeates the defense sector. At the same time, their implementation is structurally more complex than in typical B2B projects, because it requires delivering market value while simultaneously managing risks related to information sensitivity, technology flow control, and access to testing environments and the end user. The literature highlights that dual-use, by definition, creates tension between the logic of open innovation (Chesbrough, 2003), collaboration, iteration, and rapid prototyping, and the logic of security, information restriction, partner vetting, and use control. In practice, this tension raises transaction costs and makes collaboration difficult without the involvement of intermediaries: actors capable of operating fluently across the languages and expectations of startups, industry, and public institutions (Vaynman & Volpe, 2023; Riebe & Reuter, 2019). The following paragraphs discuss the main challenges in this area.

Confidentiality and information constraints

The first major source of friction is confidentiality. For many dual-use technologies (e.g., cybersecurity, communications systems, sensing, data analytics), information about the solution's architecture, performance parameters, vulnerabilities, or use scenarios can itself carry operational value, and therefore constitute a security risk. Research on *dual-use software* suggests that even in civilian organizations, tool openness (such as open-source security software) creates a dilemma: it can increase transparency and speed of adoption, yet it may also facilitate misuse if the implementation context is not controlled (Silic, 2013). From the perspective of international relations and cooperation in sensitive domains, dual-use further complicates information exchange: it is difficult to draw a clear line between "civilian" and "military" applications, which can amplify distrust, disinformation risks, and concerns that collaboration may be used to extract sensitive knowledge (Vaynman & Volpe, 2023). In practice, this means that a startup cannot always communicate solution details openly, while the end user (e.g., a public authority, the military, or a critical infrastructure operator) cannot always share data, procedures, or realistic operational scenarios.

At this point, the intermediary's role is to introduce a trust layer and formal cooperation frameworks: confidentiality management, standardized contracting (e.g., NDAs), rules for accessing information and data, and limiting the circle of individuals authorized to view sensitive elements of the project. Without such a layer, many discussions remain at the

level of general declarations, never reaching the technical and operational detail required to run a pilot.

Testing, validation, and the risk of unintended use

A second area concerns testing and validation. Dual-use technologies are often designed to be modular and adaptable, which is a market advantage, but from a security perspective, it increases the risk of *repurposing*, meaning unintended or harmful use. Ethical scholarship on, for example, humanitarian drones (UAVs) stresses the ambivalence of multifunctional design. What enhances civilian utility can simultaneously enable misuse and generate new risks in conflict scenarios (Philippi, 2026). Similarly, in AI, there is a growing need for robust validation mechanisms, particularly when solutions are intended for high-sensitivity domains (e.g., defense and space), where misclassification, unexpected model behavior, or integration failures may have operational consequences (León Serrano et al., 2025).

In practice, startups rarely have access to testing environments that faithfully reflect end-user conditions, whether operational, infrastructural, or procedural. At the same time, end users, especially public ones, are reluctant to open their infrastructure, data, or test ranges without assurances that the project is formally structured and conducted under controlled conditions. An intermediary, typically the operator of a program or an ecosystem, reduces this barrier by creating a safer pathway from prototype to pilot. This includes selecting an appropriate testing mode, establishing access rules, supporting the definition of validation criteria, and reducing operational risk on both sides.

Compliance: export controls, technology transfer, and the capability gap

A third block of challenges concerns compliance. Dual-use projects intersect with regulations on export controls and technology transfer, in Europe governed in part by legal frameworks such as Regulation (EU) 2021/821.[1] Research on universities and research-intensive environments shows that export-control rules directly shape how research and collaboration are conducted, and that institutions must build procedures and capabilities to avoid violations. In parallel, empirical studies indicate a substantial knowledge gap among researchers and innovators regarding compliance requirements,

[1] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) PE/54/2020/REV/technology assessment for peace and security emphasizes that controlling distribution and limiting misuse require not only regulation2.

underscoring the importance of training and awareness-building programs. Without them, the risk of inadvertent non-compliance during technology transfer increases (Badrul Hisham et al., 2025).

In this sense, the intermediary acts as an institutional translator. It helps determine whether a project may fall under control regimes, clarifies information and documentation obligations, supports cross-border collaboration, and helps design a commercialization pathway that avoids deadlocks at the negotiation or implementation stage.

Access to the end user and verification of intended use

A fourth element is access to the end user. In dual-use, achieving product market fit is more difficult because the market is partly closed and procurement and implementation mechanisms are complex. In addition, there is the challenge of verifying both the counterparty and the intended use so that the technology does not reach unauthorized recipients or is not deployed in ways that contradict the declared purpose. Literature on cybersecurity and on technology assessment for peace and security emphasizes that controlling distribution and limiting misuse requires not only regulation, but also organizational practices, monitoring, and decision gates embedded in the implementation process (Riebe & Reuter, 2019). International-relations scholarship similarly argues that trust and the partner's intent are foundational to dual-use, thereby reinforcing the role of intermediaries and institutions that anchor cooperation (Vaynman & Volpe, 2023).

Longer implementation cycles: integration, hybrid architecture, and legacy systems

Finally, dual-use often entails longer implementation cycles. This is driven by both formal requirements (authorizations, procedures, verification) and the technical effort required to integrate with existing systems. In high-criticality domains (e.g., aviation and integrated systems), the literature emphasizes the challenges of integrating modular architectures with legacy systems, thereby extending testing, validation, and certification phases (Gaska et al., 2017). In dual-use, there is an additional requirement to adapt the solution to two distinct use logics, civilian and defense, which rarely align with each other in operational requirements.

Conclusion: the intermediary as a mechanism for reducing risk and transaction costs

In sum, dual-use implementations are difficult not because technologies are lacking, but because the implementation space is burdened with additional layers of risk, formalization, and information constraints. An intermediary, understood as an ecosystem operator, an accelerator program operator, or an institution capable of organizing collaboration, performs an infrastructural function. It creates secure conditions for

information flows, enables controlled testing and piloting, strengthens regulatory compliance capabilities, and reduces the distance to the end user.

In the following sections of this case study, we show how these functions are institutionalized in the practice of KPT, both in the pathway that connects startups with technology recipients and in KPT's role as a hub for dual-use initiatives linked to NATO and EU programs.

2. Krakow Technology Park (KPT) as a platform of implementation instruments

In technology projects, especially those with dual-use potential, a single support program is rarely sufficient. In practice, what is needed is a sequence of instruments that takes a team (or a company) from the idea stage and an early MVP (Minimum Viable Product), through testing and PoC (Proof of Concept) and piloting, to scaling the solution. KPT can therefore be described not as "one accelerator", but as a platform of instruments that includes: (1) incubation and a working environment, (2) acceleration programmes oriented toward implementation with technology recipients, (3) DIH/EDIH-type services ((European) Digital Innovation Hub) supporting transformation and implementation testing, (4) capital instruments (seed and pre-seed, technology pre-incubation), and (5) sector initiatives and brokerage functions that facilitate entry into specialized markets.

1. **Incubation (idea → MVP):** KPT's incubation strand combines organizational and capability-building support with an infrastructural component, including office space;
2. **Implementation-oriented acceleration (MVP → PoC/pilot):** An illustrative example is KPT ScaleUp Booster, a program in which the collaboration component with partners and technology recipients is particularly important, alongside a direct cash grant;
3. **DIH/EDIH and implementation services (PoC → pilot/scale):** In the DIH/EDIH model, the critical element is the implementation layer, including audits and support in securing investment (hub4industry);
4. **Financing and commercialization (PoC → pilot/scale):** KPT's instrument portfolio also includes equity-based solutions. The KPT Seed Fund operates as a tool for early-stage equity investments and advisory support in the earliest phases of company development;
5. **Brokerage functions and sector initiatives (cross-cutting):** Cross-sector technology transfer is supported through brokerage functions. One example is collaboration within the network of European Space Agency business application brokers and ambassadors, as well as other sector initiatives such as Digital Dragons (conference, accelerator, and

industry ecosystem, reports). These initiatives create specialized channels for the development of firms and projects, even if they are not, per se, dual-use instruments.

In the dual-use context, what matters is that such a bundle of instruments can be aligned with requirements related to selection, constrained access to the end user, testing, and compliance, without reducing the operator's role to marketing or promotion. For the purposes of this case study, we therefore treat KPT as an architecture of intermediation, meaning a set of tools and roles that reduce the transaction costs of collaboration across startups, industry, and institutions, including public ones. The following sections show how this architecture is applied in pathways related to defense.

The above overview of KPT's instruments and functions is summarized in Table 1, which outlines a pipeline of tools that can be activated at different points along the project development path (from idea to MVP to PoC to pilot to scale). From the perspective of dual-use implementation, the most relevant elements are those that enforce work on a real problem in a real end-user environment (such as acceleration programs embedded with technology recipients), or those that enable feasibility testing and controlled, secure piloting (DIH and EDIH services). Financial instruments (seed and pre-seed) play a complementary role; they can accelerate technological development, but they do not in themselves replace the implementation layer of access, validation, and governance. Finally, sector initiatives and brokerage functions strengthen specialization and cross-sector transfer. Their relevance to dual-use may be indirect, but it can be substantial where technologies (e.g., space, communications, cybersecurity) naturally spill over between civilian and defense markets. Table 1. therefore organizes KPT's instruments by their dominant function and their potential usefulness in dual-use projects.

Table 1. Mapping KPT instruments against project development stages (authors' own elaboration).

Instrument	Stage	Dominant function	Primary recipient	Potential dual-use applications
Incubation and office space (*de minimis* mechanisms)	idea → MVP	infrastructure + basic development support	early-stage startups and teams	**medium:** builds a project base; limited sector specificity
ScaleUp-type acceleration programs (grant up to PLN 300,000; work with a technology recipient)	MVP → PoC/pilot	grant + mentoring plus implementation-oriented matchmaking	startups with a prototype/MVP; industrial partners (technology recipients)	**high:** challenge-driven work and on-site testing with the recipient aligns with dual-use implementation logic

Instrument	Stage	Dominant function	Primary recipient	Potential dual-use applications
hub4industry (DIH/EDIH: audits, PoC, training; *de minimis*)	PoC → pilot → scale	PoC/testing + implementation advisory	SMEs and industrial firms (technology recipients)	**medium to high:** useful for implementation in critical environments (e.g., cyber, OT/IT integration)
KPT Seed Fund (seed)*	MVP/PoC → pilot	financing + advisory support	early-stage startups	**medium:** valuable for deep tech; dual-use relevance depends on portfolio profile and target markets
ESA Business Applications broker/ambassador (transfer of space technologies into market applications)	idea → PoC (cross-cutting)	matchmaking + cross-sector bridge	SMEs & startups	**high (indirect):** space technologies often have a dual-use profile; brokerage helps identify applications and partners
Digital Dragons (conference/accelerator /reports)	idea → scale (sector-specific)	sector initiative + networking	game development studios, investors, industry partners	**low to medium:** primarily a sector lever for capabilities and business development
Sector Skills Council: Gaming and GameDev	cross-cutting (skills)	competence development and education	SMEs & startups, education providers, labor-market institutions	**low (direct):** strengthens human capital; dual-use may benefit via spillovers (digital and managerial capabilities)
FORT Kraków: DIANA Accelerator Poland	MVP → PoC → pilot	matchmaking + mentoring + validation /testing (*via* a network) + cohort internationalization	deep-tech and dual-use startups	**high:** entry into the DIANA network, access to an accelerator, and a testing ecosystem

* KPT no longer conducts its own investment activities (formerly: KPT Seed Fund / INNOventure), as it has determined that the VC market in Poland is now sufficiently developed.

Table 1 shows that KPT's instruments span the full project development cycle, from incubation and capability-building support to piloting mechanisms and financing. In the dual-use context, the most critical parts of this pipeline are those that increase access to testing environments and to technology recipients, while also formalizing collaboration through matchmaking and governance arrangements. At the same time, not all instruments are dual-use specific; their role is primarily to shorten the path to implementation.

3. KPT ScaleUp Booster as a startup–Technology Recipient (TR) collaboration mechanism

The sector pathway within KPT ScaleUp Booster is built around collaboration between a startup and a Technology Recipient (TR), meaning an industrial partner that contributes a clearly defined implementation challenge, a testing environment, and the resources required to run a pilot. In practical terms, this enables a project to progress through successive stages, from problem clarification and an initial prototype, through PoC and piloting, to preparation for scaling.

In this model, the TR is not an auxiliary participant. It functions as the implementation node because the testing environment, infrastructure, security regimes, integration requirements, and the real acceptance criteria for the solution sit on the recipient's side. The program targets startups whose solutions address identified TR needs, including in Industry 4.0 domains, and meet a minimum level of implementation readiness. The evaluation criteria explicitly require at least TRL 6, meaning readiness for demonstration in an environment close to operational conditions. In parallel, the program emphasizes technological maturity and readiness to pilot in industrial settings, or at a minimum, a documented MVP. This is not an "idea-stage" program; it is designed for testing in a real operational context.

Within the Industry 4.0 TR pathway, the maximum support per startup is up to PLN 300,000. The grant is implementation-oriented: it finances work leading to milestones defined in an individual acceleration plan, and reporting is anchored in whether pilot results are measurable, observable, and documentable. Disbursement is milestone-based and occurs in three tranches, approximately 30% / 35% / 35% of the grant value. This structure operates as a straightforward risk-management mechanism. It limits upfront funding, enforces a cadence of evidence, and supports continuation or course correction when the pilot reveals integration, security, or operational barriers.

From a "how it works" perspective, the program requires not only technological and implementation progress, but also formal discipline, including eligibility checks, declarations, conflict-of-interest safeguards, and a structured settlement and reporting

path. This layer also matters for dual-use because it reinforces a culture of compliance, even though it does not replace export-control and security regimes specific to defense.

If a pilot requires access to the TR's infrastructure, the startup may be required to sign an infrastructure-access agreement, and the TR may require the startup to carry third-party liability insurance, with coverage levels agreed between the parties. This is a standard feature of B2B and B2G implementation work. Testing on the TR's assets, such as equipment, production lines, networks, or facilities, creates risks of damage and downtime that must be contractually addressed before operational testing can begin.

The TR may also require an NDA. The program rules further provide a non-compete obligation regarding TR in a defined area during the program and for three months after completion, as well as TR's priority right to implement solutions developed and validated within the pilot project. These provisions are important because they show that the program is not designed to end with a "demo." Instead, it structures a path toward implementation within the TR organization, at the cost of certain constraints on the startup, particularly regarding parallel discussions and projects in directly competing areas. On the startup side, the program strongly emphasizes the obligation to hold full rights to the proposed solution and to manage intellectual property to enable implementation and commercial exploitation.

In practice, this is a boundary condition for collaboration. A TR will not initiate a pilot, especially on sensitive infrastructure, if the IP status is unclear or exposed to third-party claims.

Table 2. Governance mechanisms in startup-Technology Recipient (TR) collaboration.

Risk area	Governance mechanism	Implications for collaboration
NDA and confidentiality	The TR may require a non-disclosure agreement (NDA) as a condition for access to information and the pilot environment.	Information circulation around the project is constrained; without an NDA, pilots often do not start. The benefit is the ability to work with the TR's real data and processes.
Intellectual property (IP)	The startup declares, among other things, that it holds full rights to the solution and that it does not infringe any third-party rights. The IP position must enable implementation and commercialization.	The TR reduces legal implementation risk; the startup must clarify authorship and contributions, licenses, and any dependencies (e.g., components, data, employee IP rights).

Risk area	Governance mechanism	Implications for collaboration
Liability insurance and infrastructure access	When using the TR infrastructure, the startup must hold third-party liability insurance, with coverage agreed between the parties.	The pilot becomes operationally "real" because it involves TR assets, but formalization and preparatory costs on the startup side increase. The TR limits exposure to damage and downtime.
Non-compete and implementation priority	The startup commits to a non-compete obligation vis-à-vis the TR in a defined area during the program and for three months afterward. The TR receives a priority right to implement solutions validated within the pilot.	The TR increases the likelihood that a pilot translates into implementation; the startup limits parallel activity in directly competing areas. This stabilizes the relationship but reduces short-term commercial flexibility.
Tranche-based disbursement	The grant is paid in tranches linked to milestones (approx. 30% / 35% / 35% of the grant value).	Funding is tied to progress and evidence of delivery. This supports risk control and continuation decisions, while requiring the startup to deliver results aligned with the budget and spending plan.

In operational terms, the mechanisms discussed above can be treated as a "minimum governance package" typical of B2B pilots carried out on a partner's infrastructure and data. In projects with dual-use potential, however, their importance increases because they help reduce risks linked to confidentiality, the sensitivity of testing environments, and legal and organizational uncertainty on both sides. Put differently, the closer an implementation moves toward the domains of security and critical infrastructure, the more formally structured collaboration becomes a prerequisite for moving from prototype to a real pilot and, in the next step, to implementation.

4. FORT Kraków: DIANA Accelerator Poland as a gateway to the NATO network

On 22 January 2026, Kraków Technology Park (KPT) hosted the official opening of FORT Kraków: DIANA Accelerator Poland, presented as the Polish node within the NATO DIANA network. The initiative was launched as a joint undertaking of AGH University of Science and Technology in Kraków and Kraków Technology Park, and its program is embedded in a broader ecosystem linking public administration, the technology community, and allied structures. The inauguration was attended, among

others, by Polish Deputy Prime Minister and Minister of National Defense Władysław Kosiniak-Kamysz, reinforcing the interpretation of this pathway as strategically significant rather than merely regional or sectoral.

The accelerator points to technological areas typical of dual-use solutions, including artificial intelligence, autonomous systems, information and communication technologies, connectivity, energy, biotechnology, and advanced materials. At the same time, it emphasizes a "prototype to implementation" logic. In defense and security contexts, a technology demonstration alone is rarely sufficient; what is needed is a pathway for validation, testing, and integration into the end user's systems and processes. The program also signals the potential presence of startups from allied countries within the cohort, which matters for the circulation of know-how and standards, as well as for the speed of learning in the defense-tech domain.

Importantly, within the logic of this case study, the DIANA pathway is not an "alternative" to civilian-industrial instruments such as programs built around collaboration with a technology recipient. Instead, it is a parallel channel with a different access architecture. Its center of gravity lies in connecting to an allied network (procedures, rules, contacts, testing pathways), rather than relying exclusively on a startup–industrial partner relationship in the civilian market.

DIANA is an accelerator network that connects technology firms with military end users, mentors, and investors to accelerate the development, validation, and adoption of innovations that respond to operational needs. From the startup's perspective, this means access to a transnational ecosystem in which technology is assessed not only for novelty, but also for usefulness and implementability under demanding conditions. At the organizational level, DIANA provides collaboration frames: program cadence, expectations regarding progress and validation evidence, and channels for engagement with defense stakeholders. A key element is testing and verification, understood as network-based access to environments where solutions can be assessed in conditions closer to real-world use cases than in a standard market demo.

At the ecosystem level, DIANA supports the alignment of language and collaboration standards, including criteria of "implementation readiness," which reduces transaction costs on both sides of the innovator–institution interface. In effect, DIANA acts as a gateway to a network where the pace of iteration is coupled with access to the end user and testing pathways, not only with financing and mentoring. The international cohort dimension and knowledge transfer further increase the Polish node's exposure to practices and solutions developed elsewhere in NATO.

5. How the operator closes the prototype-to-implementation gap

Across both pathways discussed here, startup–Technology Recipient (TR) collaboration in KPT ScaleUp Booster and acceleration within the NATO DIANA network, the same implementation problem recurs. Dual-use solutions rarely move "straight" from prototype to end-user implementation because the path is shaped by barriers related to confidentiality, testing and validation, regulatory compliance, and the need for controlled access to recipients and infrastructure. The literature describes this as an interplay of risks (information security, misuse risk, constrained knowledge exchange), validation requirements, and complex authorization and deployment pathways that extend commercialization cycles and materially increase the transaction costs of collaboration.

In this configuration, the role of an operator such as Krakow Technology Park is to stitch stakeholder interests together through a repeatable pipeline and a set of governance mechanisms that stabilize the startup–user or startup–partner relationship while also limiting formal risks. First, the operator organizes matchmaking, meaning challenge–solution pairing and selection, which reduces information asymmetry and partner search costs. Second, it provides collaboration frames (NDA and confidentiality, pilot rules, responsibility allocation, and managed access to infrastructure), directly addressing barriers to testing environments and end-user access. Third, it ties project progress to milestones and staged settlement (tranches), which reduces risk on both sides when implementation requires iterative refinement under operational conditions. Fourth, it embeds compliance filters, including activity exclusions, which is particularly important given that public debate sometimes conflates dual-use with the arms trade. These are not the same, and support instruments typically include explicit sectoral restrictions.

As a result, "closing the gap" through this type of facilitation is not about replacing the parties in their technological decisions. It is about providing process infrastructure: from selection and matching, through collaboration frames and validation, to the transition into piloting or testing, and finally to an implementation decision (or project termination) based on evidence.

6. Conclusions and limitations

A comparison of the two primary acceleration pathways suggests that the operator's greatest value lies not in a single instrument (such as a grant), but in a coherent architecture that combines pipeline, governance, and access to the end user.

At the same time, the model has limitations and risks that should be stated explicitly. On the TR and piloting side, a typical risk is lock-in resulting from non-compete clauses

and implementation of priority rights. From the startup's perspective this can constrain commercialization freedom, while from the TR's perspective it protects organizational investment in the pilot. A second limitation is administrative burden and bargaining asymmetry: the more regulated the context is (sensitive data, critical infrastructure, security requirements), the higher the cost of documentation, testing, and alignment, which can extend implementation cycles. A third risk, important from a communication standpoint, is the conflation of dual-use with arms trading or weapons-related activity. Support instruments often explicitly exclude financing for activities related to, among other things, trade in explosives, weapons, and ammunition. Therefore, program and project descriptions require exceptional precision.

References

Badrul Hisham, A. A., Mohamed Yusof, N. A., Salleh, S. H., & Saimy, I. S. (2025). Knowledge of strategic trade act 2010 and technology transfer among researchers in Malaysia. *Research Ethics*, *21*(4), 689–727.

Chesbrough, H. W. (2003). *Open innovation: The new imperative for creating and profiting from technology*. Harvard Business Press.

Gaska, T., Gaska, M., Summerville, D., & Chen, Y. (2017). Model Based Engineering for Advanced Integrated Modular Avionics-Focus and Challenges. Presented at the AHS International 73rd Annual Forum & Technology, Display, Fort Worth, Texas, USA, May 9–11.

León Serrano, G., Pérez Martínez, F., & de la Fuente Chacón, J. C. (2025). The dual use of artificial intelligence: Analysis of trends and policies in the defence space sector. *International Journal of Engineering Business Management*, *17*, 18479790251398347.

Philippi, M. (2026). The ambivalence of multi-purpose design: On the dual-use and misuse risks of humanitarian UAVs. *Research Ethics*, *22*(1), 1–20.

Riebe, T., & Reuter, C. (2019). Dual-use and dilemmas for cybersecurity, peace and technology assessment. In *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (pp. 165–183). Wiesbaden: Springer Fachmedien Wiesbaden.

Silic, M. (2013). Dual-use open source security software in organizations–dilemma: help or hinder?. *Computers & Security*, *39*, 386–395.

Vaynman, J., & Volpe, T. A. (2023). Dual use deception: How technology shapes cooperation in international relations. *International Organization*, *77*(3), 599–632.