2
Leading Innovation in Defense
The Transformation from Closed Defense Industrial Bases to Open Innovation Ecosystems

Dr. Valérie **Merindol**
Professor and Co-Director, newPIC Chair, Paris School of Business, France

Abstract

Many large organizations across different sectors have implemented open innovation (OI) models over the preceding decades, demonstrating how adopting such a strategy necessitates cultural and organizational change as well as an evolution in network dynamics and orchestration. OI represents a new strategy inducing massive transformation for defense organizations such as air forces and their industry partners, particularly lead systems integrators. The shift from closed to OI models for defense organizations implies paradigmatic changes at the cultural, organizational, and process levels for the design and appraisal of complex military programs. OI raises three major challenges for defense organizations: Redefining how critical new technologies can be effectively explored and exploited for defense purposes; Changing supply change approaches to access emerging technologies more rapidly and securely, and; Implementing new network orchestration models.

Introduction

Open innovation (OI) fosters inflows and outflows of knowledge to accelerate internal innovation (Chesbrough, 1993). Many large organizations across different sectors have implemented OI models over the preceding decades, demonstrating how adopting such a strategy necessitates cultural and organizational change as well as an evolution in network dynamics and orchestration. OI represents a new strategy inducing massive transformation for defense organizations such as air forces and their industry partners, particularly lead systems integrators, in combining internal and external ideas and assets to create value (Merindol and Versailles, 2020). The shift from closed to OI models for defense organizations implies paradigmatic changes at the cultural, organizational, and process levels for the design and appraisal of complex military programs. The traditional boundaries with industry partners also become blurred.

Academic literature on OI documents new modes of network orchestration necessary to foster dynamic collaboration between heterogeneous actors and introduce new types of interactions. Nations such as the United States, the United Kingdom, and France have demonstrated capacities in OI for defense by launching various initiatives in this respect, but the finer details of their evolving national efforts are still being elaborated. OI raises three major challenges for defense organizations in particular, which this paper will explore: Redefining how critical new technologies can be effectively explored and exploited for defense purposes; Changing supply change approaches to access emerging technologies more rapidly and securely, and; Implementing new network orchestration models.

Redefining the Exploration of Emerging Technologies

Innovation relevant to defense does not emerge only inside the boundaries of the defense technological and industrial base (DTIB) any longer. Critical technologies for defense are more than ever "dual-use" in nature – meaning they have relevance in defense but also have various commercial applications. Dual-use technologies such as artificial intelligence (AI), robotics, and big data are all vivid outcomes of innovation ecosystems that are not, or only partially, linked to defense. The development of military capability, therefore, requires defense

organizations to attract new actors and agents of innovation and to change the ways that defense programs are managed to better allow emerging opportunities to be exploited. To explore the potential of emerging technologies better and exploit them successfully, it has become essential for defense organizations to gain from creativity and innovation that is not initially intended for defense.

The reference to dual-use technologies has changed since the Cold War era when the development of such technologies was based on a linear model of innovation (Foray, 1997). At the time, defense organizations investigated the potential for dual-use technologies mainly during the early stages of the Technological Readiness Level (TRL), cooperating with universities and research communities on specific exploration efforts or projects. The process was based on a technological 'push model' that created different activity streams (defense versus non-defense, for example) at specific levels of technological maturity. In OI models, however, the promotion of dual-use technologies is more reflexive and does not correlate to a linear model of innovation (Merindol and Versailles, 2010). The notion of dual-use involves exploration routes that can occur at different stages of the technology development lifecycle and increasingly features co-creation between defense and civilian communities as well as "spin-off" and "spin-on" points at different technological maturity levels. These evolutions have implied a need for defense organizations to modify legacy practices, processes, and the rules that frame their approach to harvesting innovation.

The notion of dual-use involves exploration routes that can occur at different stages of the technology development lifecycle and increasingly features co-creation between defense and civilian communities as well as "spin-off" and "spin-on" points at different technological maturity levels.

Identifying Future Opportunities Faster

OI in defense requires a fluidity of exchanges with heterogeneous actors that do not otherwise work on defense-related issues. To achieve this, creating mechanisms for trusted interactions, establishing a common language, and

encouraging an alignment of interests with potential contributors is essential (Merindol and Versailles, 2020). Defense organizations have tended to develop relationships with start-ups specializing in high-end technologies, attaching importance to being able to identify and begin working with entrepreneurs early on for developing solutions based on breakthrough technologies and innovation. For instance, Thales, a European lead systems integrator, has established a technology incubator and accelerator center for cybersecurity start-ups in the heart of Paris in collaboration with Station F, which may be the largest hub of its kind in France. Initiatives like this have created unique opportunities for Thales in attracting start-ups not initially focusing on defense and guiding the development of their technologies to maturity levels where they can begin working on defense needs directly with Thales engineers.

Defense organizations have also attempted to connect with a wide variety of researchers to better understand key challenges that come with a technologically disruptive and turbulent strategic environment. For example, the NATO Hub affiliated with the NATO Transformation Command has prescribed the mission of connecting with researchers across thirty NATO members to appraise military leaders with technological and strategic assessments which may impact the critical capabilities of allied militaries. With a small team of officers and engineers, the NATO Hub, an agile organization using flexible approaches for collaboration with researchers, such as by enabling participation in the network and interaction via a digital platform, can enrich the thinking and vision of NATO leaders through critical inputs by research communities focusing on technology, geopolitics, and economic trends.

Defense organizations can also initiate collaborative projects with communities that otherwise seem distant from the competencies and profiles traditionally associated with defense. This is most notably the case with prospective activities such as scenario planning, where defense strategists question basic assumptions and attempt to look beyond the boundaries of existing conceptual paradigms. In France, the Defense Innovation Agency (AID), part of the French Ministry of Defense, runs the Red Team Defense program, which collaborates with science fiction novelists to identify future threats, for example. Working with novelists enables a unique way to think out-of-the-box in identifying and preparing militaries for unusual but highly plausible threat scenarios. The Red Team Defense program generates valuable outcomes for the French Ministry of Defense by

justifying new directions for military R&D and helping guide wider collaboration with innovation ecosystems.

Fostering New Models of Collaboration

Introducing new models for collaboration into the defense environment presents two key challenges. The first relates to building effective relationships with external actors, particularly motivating them to work on innovation aimed at defense. The second challenge concerns adapting mindsets and procedures within defense organizations towards external actors that do not work on defense issues or traditionally associate with the defense community. The necessity for creating new types of collaboration and trusted interactions is stressed in addressing these challenges. Defense organizations must ensure high-quality knowledge exchanges and guarantee that value created through such exchanges can be shared equitably among all stakeholders. There is a requirement for defense organizations to make transparent rules available before the commencement of collaboration if they want to effectively complement legacy 'push models' for technology and science that can no longer fulfill defense needs.

> *New forms of collaboration for defense organizations require agility at an organizational level. Working with start-ups demands an ability to test and experiment with new solutions with high reactivity, which is achieved by introducing a culture of innovation and open mindsets.*

New forms of collaboration for defense organizations require agility at an organizational level. Working with start-ups demands an ability to test and experiment with new solutions with high reactivity, which is achieved by introducing a culture of innovation and open mindsets. In France, for example, AID communicates widely on key military issues with various entrepreneurial ecosystems, identifying high-potential start-ups and offering them access to detailed military use cases to enable and enrich experimentation activities. A key element of the French approach is to enhance responsiveness in defense organizations which will help open the door to deeper collaboration *before*

potential solutions are adapted to military uses. This objective also reflects the importance of defense organizations in becoming better at developing innovation based on user-centric approaches.

If military forces have always been at the center of defense innovation processes, their role and involvement have now changed with user-centric approaches. In technology push models, military users are only formally present at the beginning of innovation efforts to specify needs and typically return to the picture after R&D has been able to create test prototypes. In user-centric approaches, however, interactions are more informal and based on horizontal exchanges between users and technology providers. Military users remain active throughout the various developmental phases as co-creators and do so without intermediaries (Merindol and Versailles, 2020). To better embrace and promote user-centric approaches, militaries have increasingly turned to creating "labs" that serve as nesting grounds for innovation. In France, for instance, the Army, the Navy, and the Air Force all run their labs, providing military users an environment for trusted interactions and agile experimentation with researchers, start-ups, and other technology providers. These labs also allow military users to provide critical feedback on existing civilian solutions and introduce ideas that may provide new starting points for innovation.

Reshaping the Role of Lead Systems Integrators

Transitioning from the exploration of technologies to their effective exploitation implies a need to evolve acquisition frameworks strategically. Military programs are characterized by increasing levels of complexity, whether in terms of specific components or sub-systems and, at a higher level, the integration of capabilities into a system of systems. It is easier to handle innovation for components than for systems, whereas the larger the size of a specific program, the more complex it becomes, and, accordingly, also the management of innovation relating to it. On the other hand, the highest level of program complexity relates to systems integration. In OI models, the role of lead systems integrators does not vanish, but the nature and dynamics of interaction between them and defense organizations changes in meaningful ways with the introduction of new agents of innovation. It is necessary to unlock the full potential of what

each contributor does best, which means lead systems integrators and defense organizations must be able to work together to provide the integrated policy frameworks, working models, and processes that enable new solutions for military programs to be more rapidly absorbed.

In this context, defense organizations must learn to limit their roles to stipulating operational requirements and user needs rather than issuing detailed guidelines and 'wish lists' of technological components for programs (Versailles, 2005). On the other hand, lead systems integrators must adopt and promote modularization and the standardization of interfaces, which can make gains possible in integrating emerging technologies and innovation more flexibly over the lifespan of military programs. Integrating new functions into military equipment generally proves challenging using OI models, with some notable exceptions, such as when open-source solutions make it possible for new players to interact with "old" generations of proprietary software, middleware, and hardware or between different technological generations of components (Le Texier and Versailles, 2009). On the other hand, assessments of trade-offs between the costs of modularization and the benefits of being able to rapidly integrate emerging dual-use technologies must be carefully and continuously considered.

Changing the Approach to Supply Chains

With OI, industrial policies that address the associated risks of supply chains for military programs need to be reshuffled. The DTIB will continue to play a vital role in meeting military requirements, but efforts to preserve critical competencies within it are no longer enough to sustain technological superiority. Firstly, it is imperative to complement traditional DTIBs by accounting for the emergence of new innovation ecosystems with critical dual-use technologies. Secondly, defense organizations must manage the complementarities new innovation ecosystems provide to the DTIB by cultivating commonality and synergy between them on the one hand and ensuring reliability in critical supply chains on the other.

Changing Perspectives on the DTIB

The DTIB typically aggregates a group of industries that are, to varying degrees, dependent on defense spending. Nations depend on their respective DTIB for some degree of self-sufficiency in military production (Dunne et al., 2007). The DTIB is a hierarchical network managed by lead systems integrators and is typically observed as a closed perimeter of actors localized in the domestic market and previously active in defense programs, with specializations shaped and driven by lead systems integrators (Versailles and Merindol, 2019; Versailles, 2005). In this traditional framework, the DTIB is relatively stable, with considerable power and influence concentrated with lead systems integrators and defense organizations, which impose rules around issues such as intellectual property rights and the export of defense articles and equipment. However, defense requirements increasingly cannot be fulfilled entirely by capabilities located within the DTIB, particularly with the accelerating digitalization and exploitation of data technologies in defense. To keep pace with innovation occurring in the civilian space and to enable similarly positive outcomes for defense, the same characteristics of agility and input-driven models need to be replicated.

While it is necessary to open up the boundaries of DTIB to take advantage of dual-use technologies that are relevant and increasingly needed for military purposes, the challenge of OI cannot be solved simply by introducing new R&D streams and technology providers into the DTIB. Adjusting to new realities also stress the need for complementing the DTIB with new innovation ecosystems previously not linked to defense. This may be challenging because the stability of the traditional DTIB contrasts with the dynamics of new innovation ecosystems, which are driven by bottom-up and user-centric needs. Even in the OI context, however, the DTIB and its stability remain vital for adding value, given its deep understanding of military needs, doctrines, and concepts concerning force employment and operational constraints, on the one hand, as well as its proven capacity to work with and manage the vast complexities of military programs (Belin et al., 2018; Versailles, 2005). In OI models for defense, therefore, the traditional DTIB actors still 'own' or control the specific capabilities to integrate new technologies and innovation into military programs but need to provide better linkages to new solutions adapted to defense needs that may not have much in common with civilian applications.

Developing Complementarities

New innovation ecosystems present a two-pronged challenge concerning securing access to critical technologies in the long-term perspective. First, the R&D and industrial capabilities required to produce dual-use technologies may depend on actors or ecosystems outside a nation's traditional military and geopolitical alliance frameworks. Innovation ecosystems tend to have a life of their own, defined by commercial factors and civilian needs, and their composition can be dispersed among various nations. Consequently, the localization of strategic assets may not be primarily driven by the specificities of national alliances and partnerships for commercial players and new innovation ecosystems. For defense, however, localization requires policy coordination between civilian and military industries to create innovation hubs and the competencies relevant to developing particular dual-use technologies within the framework of their international alliances and partnerships.

	Functions	Key Aspects	Localization	Challenges
Defense Technological and Industrial Base (DTIB)	To develop and integrate capabilities without commercial applications into military programs	Hierarchical and stable network	National	Preserving national self-reliance and increasing exportability
New Innovation Ecosystems	To adapt, advance, and exploit dual-use technologies for the defense environment	Heterogeneous and dynamic networks	International alliances and partnerships	Standardizing interfaces, commoditization and localization

Table 2.1: Comparing Defense Technological Industrial Bases and New Innovation Ecosystems

Second, interdependencies between the DTIB and contributors of dual-use technologies can generate uncertainty on issues of long-term access to critical components. Individual components of systems may be complex and high-value but are quite possibly useless on their own – becoming valuable only when they are put to work in a technology or platform. Such efforts require coordination and for risks associated with such sensitive interdependencies to be mitigated

through responses like the standardization of interfaces and commoditization of components or systems (Holgersson et al., 2022). Standardized interfaces can provide design rules to ensure interoperability between different parts of complex systems (Jacobides et al., 2018). Commoditization, on the other hand, can exploit the benefits of substitutability with alternative components and even suppliers.

The localization challenge introduced by dual-use technologies is exemplified by 5G technology, which promises to massively expand bandwidth to unlock the gains from "big data" and AI technologies. 5G is supplied by actors outside the DTIB and requires the development of new modules "hardened" for military use and will require military systems to connect with civilian standards using ad-hoc protocols. To reduce the risks with dual-use technologies such as 5G, governments may mandate that technology providers belong to nations considered strategic allies and partners and ensure the substitutability of commodities or the existence of backup providers. Standardization of interfaces alone is not enough, and defense organizations must consider commoditization early on in acquisition. Uncertainty with dual-use technologies can be managed to some extent by appropriately considering specific constraints of the defense environment but will not vanish entirely. Defense organizations must be prepared to pursue strategies that combine the standardization of interfaces, commoditization, and incentives to rely on industrial relationships within the framework of a nation's global alliances and partnerships.

Implementing New Network Orchestration Models

The strategy for OI in defense must propose a design for network orchestration that serves needs by helping enact renewed collaboration between defense organizations and lead systems integrators. However, this takes work to realize. A significant change in mindsets and ways of working for defense organizations is necessary to achieve new types of trusted interactions with industry partners. The OI model defines the network orchestration function at three levels. First, defense organizations must foster the development of various intermediaries, for example, incubators, accelerators, innovation labs, and defense research agencies, strategically building complementarities and synergy between them. These intermediaries must be able to deploy the necessary mechanisms to foster new connections and interactions into their portfolios, allowing them to

perform as catalysts and enablers for dual-use technologies collaboratively with new innovation ecosystems.

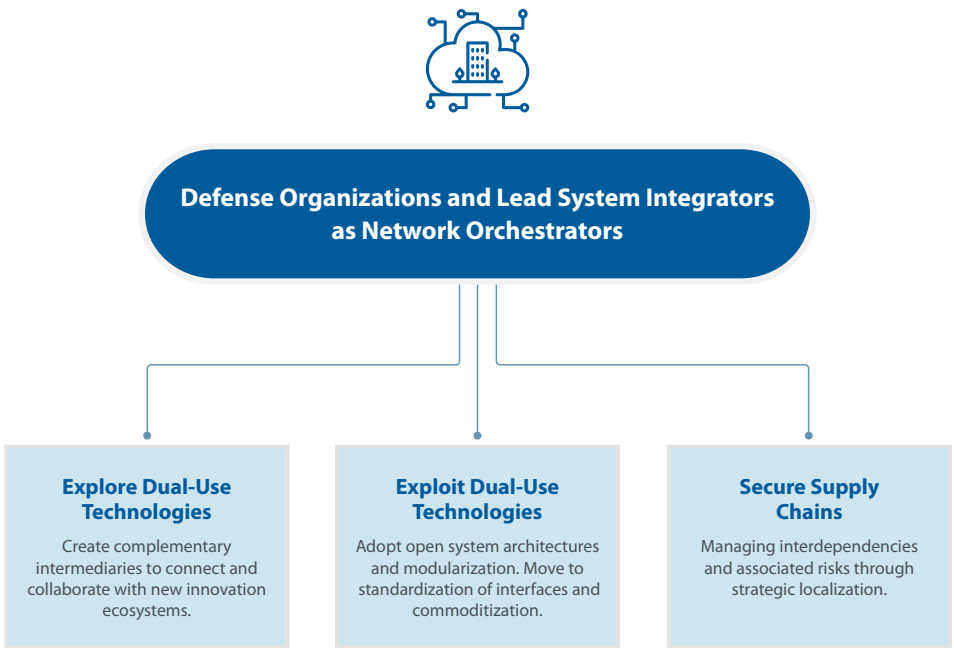

Figure 2.1: Network Orchestration for Open Innovation in Defense

Second, defense organizations and lead systems integrators must work in tandem to design and promote open systems architectures for technologies relevant to military programs. This process has already been developed in open-source software but needs to be expanded across other areas by improving procurement processes and acquisition models (LeTexier and Versailles, 2009). Finally, defense organizations and lead systems integrators must carefully consider the strategic necessity for localization, standardization of interfaces, and commoditization to mitigate long-term risks associated with dual-use technologies developed by internationalized innovation ecosystems. Here, strengthening civil-military coordination to develop future-looking industrial policies can help make the localization of critical technological and industrial assets possible in ways that reflect the makeup of a nation's global alliances and partnerships.

References

Belin, J., Guille M., Lazaric N., and Mérindol V. (2018). Defence firms adapting to major changes in the French RD funding system. *Defence and Peace Economics*, 30(2).

Chesbrough, H.W. (2003). The Era of Open Innovation. *MIT Sloan Management Review*, 44, 3

Dunne P., Garcia-Alonso M., Levine P., Smith E. (2007) « Determining the Defence Industrial Base, *Defence and Peace Economics*, vol.18 (3).

Foray, D. (1997) " Which way to go ? Defence technology and the diversity of "dual use" technology transfer," *Research Policy*, vol. 26 (3), pp. 367-385.

Holgersson, XX, Marcus, B. C., Chesbrough, H., and Bogers, M. (2022). The Forces of Ecosystem Evolution. *California Management Review*, 64(3), 5–23. Available at: https://doi.org/10.1177/00081256221086038

Jacobides, M. G., Cennamo, C., and Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, 39(8), 2255–2276. Available at: https://doi.org/10.1002/smj.2904

Le Texier, Th. and Versailles, D. W. (2009). Open-source software reshaping Defense-related management of technologies. *International Journal of Open Source Software & Processes (IJOSSP)*, 1(2), pp. 14-27.

Mérindol, V. and Versailles D. W. (2010). Dual use as knowledge-oriented policy: France during the 1990-2000ies. *International Journal of Technology Management*, 50(1), 80-98.

Merindol, V. and Versailles, D. W., (2020). *The (r)evolution of Defence innovation models: Rationales and consequences*, Policy Paper #60, commissioned by Ares Group Available at: http://www.iris-france.org/ares.

Versailles, D.W. (2005). Défense, organisation industrielle et réseaux de connaissances. *Revue d'économie industrielle*, 112 (4e trimestre), pp. 11-25.

Versailles, D.W. and Merindol V. (2019). Boundary object as the missing link in resources orchestration: an exploratory study of Dassault Aviation Mirage IV et Rafale programs. *Management International*, vol. 23 N°4, pp. 101-117