#60

THE (R)EVOLUTION OF DEFENCE INNOVATION MODELS:
Rationales and Consequences

Prof. Dr. Valérie MERINDOL
PROFESSOR OF INNOVATION,
PARIS SCHOOL OF BUSINESS

Prof. Dr. David W. VERSAILLES
PROFESSOR OF STRATEGIC MANAGEMENT AND INNOVATION STUDIES,
PARIS SCHOOL OF BUSINESS

July 2020

The views expressed here are solely those of the author.
They do not reflect the views of any organisation.

Policy Paper

Armament Industry
European Research
Group

ABSTRACT

This article investigates recent evolutions in Defence-related innovation management, and its reorganisation towards joint efforts operating user-centric innovation and open innovation rationales in parallel to more traditional perspectives framed by the (top-down) management of technologies.

It is the introductory paper of a series of policy papers which will focus on the way EU Member States have taken into account the necessity to review their defence innovation policy. The future case study articles will also elaborate on the consequences of such changes for procurement policies and for the management of armament programmes.

New mindsets and ways of working are required to generate more agility, more frugality, tighter time frames for the implementation of solutions, and increased cost-effectiveness. War fighters must be present around the table of the management of innovation from the earliest stages of the projects onwards. Open innovation rationales must be introduced to attract talents and expand the boundaries of communities working for Defence. New intermediaries such as corporate incubators, accelerators, innovation hubs become key players in this framework. We do not minimize the disruption incurred by these elements, most notably in the interaction with the industry and with system integrators. However, we promote the idea that thinking in terms of ecosystems is more suitable to this new perspective than the traditional (and closed) approach in terms of Defence industrial base. The article also illustrates these directions with case studies on DARPA, the US DIU program, French military labs, the UK JHub, and the NATO Innovation Hub.

***Keywords**: open innovation, user centric innovation model, dual use technologies, Defence ecosystems, innovation intermediaries, military capabilities*

TABLE DES MATIÈRES

INTRODUCTION ON OPEN INNOVATION: NEW CHALLENGES IN THE DEVELOPMENT OF MILITARY CAPABILITIES

In the open innovation model, firms and policy makers need to systematically seek for, and combine, internal and external assets to create value and develop new projects (Chesbrough, 2003). It implies a transformation of the ways of working about innovation in all industrial sectors, for private and public actors. The adjective "open" means that ideas and technologies potentially emerge from anywhere, not only from the inside of the companies: knowledge and competences originate from various networks. Digitalization and "deep techs", such as big data and artificial intelligence, accelerate this transformation because they transversally impact most capabilities. They are flexible enough to allow new uses that are not easy to anticipate. They are considered as "diffusing" technologies incurring significant evolutions in sectoral boundaries. New competitors emerge in all industries, both with the advent of start-ups and the diversification of large companies.

Open innovation implies major changes in relation with ways of working and organizational aspects, the governance of networks, individual and collective mindsets, and the rationales of business models. It requires increased agility, an attitude prone to breaking institutional and organizational boundaries, and the introduction of multidisciplinary teams where people with different backgrounds and experiences work (and create) together. The open innovation framework has promoted a new user-centric approach of innovation and creativity (von Hippel, 2005): users locate at the heart of the definition and resolution of problem, and sometimes they actively contribute to find and develop new solutions. The user centric model deeply changes individual and collective ways of working for the development of new products and services.

In Western countries, Defence policy makers need to adapt and reshape the governance of innovation (Bahemia and al, 2018). Open innovation requires to "invent" a brand new model for State-Science-Industry interactions in place to develop military capabilities. This transformation is mandatory to stay in the game of the dynamics of innovation as a focal actor.

For Defence-related policymakers, the stakes are high for two reasons.

Firstly, open innovation and the traditional model of Defence innovation are to some extent in contradiction with each other. Defence policy makers have a constant focus on the control of technologies, the protection of the supply chain and the preservation (management) of capabilities in the Defence industrial base (DIB). Ministries of Defence act as the same time as clients and as regulators; firms active as system integrators represent the key actors for the development of complex military programs (Belin et al. 2010; Versailles et Mérindol 2019; Versailles, 2005b). They develop "techno push" processes implying a verticalisation of the value chain. In this perspective, military services are not absent from the development of complex systems as they represent the final users, but they intervene at formal steps in the development of technologies. It is not expected them to be present at all steps of the process. The starting point of the reasoning about complex military programs always relates to the trade-off between technological superiority and the cost of developing new technologies (for example in France see Becht and Gassilloud, 2018). Countries such as the USA also foster technological superiority as a strategic objective, even if this process incurs very high development and production costs (as illustrated with the F22 and JSF programs). It is now important to introduce more flexibility by combining various models of innovation, and most notably combine the techno push approach and the user centric model. This will support the emergence of ideas and technologies and will give room to various development trajectories (Wilkinson and Jewel, 2017).

Secondly, open innovation draws a new and complex relationship between civilian and military technological innovations. It is important to introduce new ways to manage "dual use technologies" (Merindol and Versailles, 2010). Innovative technologies relevant for the development of military capabilities can emerge from any sector. In the open innovation context, the concept of Defence industrial and technological base (DITB, or DIB) (see Versailles, 2003) loses its relevance because it is most often associated with a closed perimeter of actors active in past Defence programs. DIB exemplifies a closed innovation model. Defence policymakers have now to appropriate at the same time new critical technologies and systems specific to Defence issues, and a wide variety of innovations and technologies not driven by military needs and budgets. Defence policy makers remain the focal actors in the former environments, while they are only one of the

crowd (and not the main influential one) in the latter. The management of innovation for Defence therefore requires new reference patterns, with new ways of working and collaborating with a wide variety of actors.

The open innovation perspective requires a transformation in the management of Defence innovation, at two levels: inside the administrations in charge of military services, and at the level of innovation networks. All countries have initiated transformations to adapt their innovation polices to open innovation contexts. Step by step, they introduce new tools and structures that all share several characteristics, such as putting military users at the centre of the innovation processes, encouraging bottom-up initiatives and working with innovative start-ups... The transformation speed depends on national cultures. This policy paper investigates these new patterns, and elaborates on illustrations selected from France, the United Kingdom and the USA. In a first section, we discuss first the new organizational drivers and processes leading to a new repartition of responsibilities inside ministries of Defence. In a second section, we identify new directions for the interactions between Defence institutions, the industry and the actors of basic and applied research.

NEW ORGANIZATIONAL CULTURES, NEW PROCESSES AND A NEW REPARTITION OF RESPONSIBILITIES

Three main imperatives prevail when ministries of Defence are trying to manage open innovation:

- Change the organizational culture by introducing new mindsets and new ways of working for problem resolution,
- Change innovation and technological processes, and
- Adapt the distribution of responsibilities for processing innovation in military technological systems.

New mindsets and new ways of working for problem resolution

Evolutions of the organizational culture are always a key aspect in the management of innovation. However, they require time. Several issues must be considered.

Processes towards the identification of problems in relation with military capabilities and their resolution require adaptations. In the traditional approach, innovation is driven by the engineers' mindset. In the adapted organizational culture, the starting point of innovation processes does not locate in the technological performance anymore; the whole innovation process revolves around value in use, appraised from the end-user's perspective (most often the war fighter). In this perspective, the systematic search for technological superiority can eventually represent a way to address the issue at stake for war fighters, but it does not lead to an automatic solution (Mérindol and Versailles, 2018). User-centric approaches to innovation do not mean that technologies are not important anymore. They only represent an option to address the search for *operational* superiority, and value creation for war fighters in their actual (tactical, operative, strategic) environments. The user-centric approach is therefore consistent with Iansiti (1997) perspective of technology integration that elaborates on a knowledge-based approach (that is also illustrated in GAO, 2004) but it supposes a separation between the management of innovation and the management of technology. This requires new (and adapted) ways to involve military services (and war fighters) in innovation processes. This relationship should be more informal than in the past. It is important to encourage the war fighters' feedback and to introduce new opportunities for cocreation between military end-users and providers of technologies. It is equally important for the accommodation of breakthrough technologies and the identification of new military uses based on artificial intelligence, and for the "invention" of new ways of working on the battlefield with digital technologies.

In the user-centric approach of innovation, it is important for Defence organizations to be agnostic about the civilian or military sources of technologies, and their funding, provided that the access to technologies is secured on the long run. This requires increased flexibility and the ability to breaking internal and external silos. The traditional verticalization of Defence-related activities used to manage the complexity of military programs tends to curb the emergence and the diffusion of new ideas inside military programs, and to curb the eventual transposition of innovative solutions promoted by civilian users.

The ease of installing organizational adaptations depends on the national culture prevailing in each Defence innovation system. In the USA, for instance, promoting new

innovation management models meets important constraints. Several agencies have already aligned with the precepts of open innovation and taken advantage of the associated ways of working. DARPA, the US Defence agency in charge of the development of disruptive technologies, has always been working with an open innovation approach. DARPA (see focus 1) manages innovative communities outside the ministry of Defence and asks them to address Defence and National Security challenges (Fuchs, 2010; Colatat, 2015; Bonvillian et al. 2019). DARPA easily accommodates a combination of techno-push and user-centric approaches in its activities.

Focus 1 – Combining the techno push and user centric approaches: DARPA and the Strategic Defence Capabilities office of the US DoD

DARPA is unique inside the American military innovation system. Its goal has remained stable over time: DARPA's role is to pick major problems that are not addressed by other military organizations. DARPA accepts financial risks to develop leading and disruptive technologies and propose solutions for these problems. DARPA characterizes with three main organizational features (Van Atta, 2007). It is independent from military services and their R&D centres. DARPA is a flat, agile, idea-driven and outcome-focused organization. It hires talented people as project managers for a defined duration (3 years). DARPA has an average 20% staff turnover each year. These projects managers come from various research public and private institutions and all are acknowledged as senior technologists or researchers in their respective scientific fields.

DARPA project managers facilitate innovative communities to resolve key challenges associated with new technological trends. Their role is to find the most original and relevant ideas and to gather various (scientific, civilian and military) points of view to experiment and develop new prototypes (Fuck 2009).

One of the challenges addressed by DARPA is to break internal and external silos such as the verticalisation of the industries (Bonvillian et al. 2019; Bonvillian and Van Atta, 2011). Managing various communities, offering new opportunities for start-ups or competitors to work differently on an innovative project remains central for the development of disruptive technologies. DARPA is famous for its unorthodox approach. DARPA managers have tested various methods for the management of conception and innovation projects to act as catalysts in the development of disruptive technologies.

DARPA dedicates resources for transitioning the new technologies to civilian and military markets. DARPA project managers always seek sponsors in the military services because new disruptive technologies do not relate to immediate military needs. They require both organizational changes and adaptations in the operational doctrines.

The recent introduction of user-centric approaches inside DARPA represent a new perspective for transitioning disruptive technologies to military organizations faster than it was done in the past.

The user-centric approach of innovation has been introduced through collaboration with the Strategic Defence Capabilities Office (SDCO). Created in 2012, the SDCO is staffed with military staff with different operational backgrounds and positioned at different levels of the hierarchy. The SDCO mission is to appraise technologies developed by DARPA and to assess them with an operational value-in-use perspective. SDCO targets technologies with various degrees of technological maturity and experiments with them in actual environment to elaborate new uses and operational doctrines

They fund prototypes, organize dense feedbacks with the providers of technologies and, in some cases, work with military units in co-creation processes. SDCO was put under the control of DARPA in 2019. The US DoD expects that this reform will densify the ties between military personals and innovation communities hosted by DARPA. Despite the loss of its administrative autonomy, the SDCO's goal remains unchanged: improve the accommodation of disrupting technologies by military services, and increase the opportunities for co-creation processes.

New processes for the management of innovation versus technologies

The traditional approach to military innovation revolves around maturity scales applied to technologies (Technological readiness level or TRL, eventually complemented with Technological maturity assessment, TMA). The entanglement between the management of innovation and of technologies represents a major source of ambiguities (Mérindol, 2015). The assimilation of the management of innovation with the management of technology is totally comfortable with linear processes of innovation. When pretending that these processes cover the very same reality, managers mitigate their risk with decision gates about the generations of technologies to be sequentially introduced into the programs with different "blocks" or "standards". Adopting the user-centric approach of innovation requires new ways of working, new competencies, new mindsets. Evolutions inside the Strategic Defence Capabilities Office, now affiliated to DARPA, illustrates this mandatory transition (see focus 1).

A direct consequence of this evolution locates in the need for a redefinition of dual use policies. This necessary evolution represents another source of difficulties. In many cases, in France, the United Kingdom and in the USA, routines incurred by the traditional linear approach of innovation tend to restraint the emergence of dual use technologies (Mérindol, 2009; Mérindol and Versailles, 2010). This point is typically observed in decisions or policies about dual-use technologies ruled by rationales based on TRLs.

Specific funding schemes promoting dual use technologies focus on the early stages of their development at TRL 1 to 3 (science-based projects). The TRL 3 decision gate is supposed to end the "generic" phase common to civilian and military applications before engineers decide to orient the subsequent developments towards product lines specific to each category of end-user. Such an approach is mainly developed without any active interaction with end-users (either civilian or military). The progression through the next stages of technology maturity does not foresee any sort of connection (or cross-fertilisation) between military and civilian end-users.

Other funding systems promoting dual-use policies target TRLs 5 to 7 (technological and industrial demonstrators). The French RAPID program typically focuses on this target. Results are interesting. Projects brought by start-ups and SMEs have been accelerated both for civilian and military markets (Perrin and Guérini, 2019). However, the number of success cases remains low. In many cases, initial prototypes have been developed for commercial markets and lots of challenges occur to adapt these technologies to military applications. Difficulties obviously arise in the maturation of technologies and the customization for military uses, but also emerge in the rationales of business models, of production schemes, of supply chains, and in the preparation for maintenance activities. These elements are not easy to handle. SMEs or start-ups usually have it difficult to "pivot" and accommodate the constraints of military operational rationales (and the subsequent specifications) when the maturation process has already advanced. In the USA, the Defence Innovation Unit (DIU) illustrates these elements (see focus 2).

Focus 2 – The US DIU Program as an instance of management for dual-use technologies

The Defense Innovation Unit (DIU) was set up in 2015 in order to experiment new technological innovation driven by commercial markets in the military environment. It is headquartered in Mountain View (CA), in the Silicon Valley, with additional outposts in Austin (TX), Boston (MA) and the Pentagon. The DIU goal is to contribute to enhance US military capabilities by introducing leading innovation (in digital areas, AI, etc.) coming from civilian and commercial markets. There are two main challenges. First, attract talented start-ups mainly located in the Silicon Valley to work and adapt their technology to the US military markets. Second, experiment technologies in actual contexts to assess their relevance for military services. The program also contributes to learn about possible interactions between the Pentagon and actors who were not yet related with it.

The DIU effectiveness is a controversial topic (Dougherty, 2018) as only 30% of their technologies were transferred to the military services. DIU was criticized by small firms for lacking agility in decision-making process and in modalities for testing the technologies in military contexts. That is the reason why many companies disregard DIU initiatives and projects. Moreover, when start-ups bring in technologies or projects with high maturity levels, it becomes difficult to adapt them to military needs. Working out a new business model to diversify their activities on Defence markets proves also to be difficult for small companies.

Adapted responsibilities to handle military innovation

In open innovation processes, the adjective "open" means that ideas and technologies potentially emerge from anywhere inside and outside the Defence ecosystem. This evolution implies a redefinition of responsibilities and functions inside Defence-related organizations. This is similar to current transformations of innovation practices and ways of working in large companies (Mérindol, 2016). The affiliation of the innovation function to a specific unit or to a group of specialists is not relevant anymore. Responsibilities must be reshaped and reshuffled throughout the organization.

The first reason for this evolution lies in the fact that innovation processes are not confused anymore with the management of technological maturity. In Defence-related organizations, there is now a tendency to split these two main aspects into a direction of innovation and a direction in charge of technological aspects of program management. In France, the creation of the Defence innovation agency illustrates how the boundaries of responsibilities are reshaped inside the ministry of Defence (Perrin and Guérini, 2019).

The second reason lies in the evolution of the function of innovation director itself. This executive evolves into a facilitator and/or an orchestrator of new forms of collaborations and/or a catalyst of new ideas and projects. He combines techno-push and user centric approaches. He must create a climate of trust, foster bottom up initiatives and make these initiatives visible and appropriable by the rest of the organization.

Open innovation also introduces new motivations to facilitate innovation coming from employees (Chesbrough and al 2006). The creation of open labs as they exist in large companies represents one of the main tools for enhancing theses bottom up initiatives and support intrapreneurship programs (Mérindol et al. 2016). Open labs are physical spaces designed to enhancing creativity and, sometimes, to using fast prototyping tools.

They are staffed with small teams specialized in the facilitation of creativity methods (such as design thinking) that empower employees to "think out of the box". These teams support the development of the user centric approach and foster collaboration with various people inside and outside the organization (such as start-ups and researchers).

Similar initiatives have also emerged in Defence organizations. In the USA, the SOFWERX lab offers a unique platform for collaborating with Special Forces and accelerating digital innovation. France offers several initiatives with the French Army "Battle lab", the French Air Force "Air Warfare center" (CEAM), and the French Navy "Navyl@b" and "Fuscol@b". All these labs illustrate how innovation is distributed throughout the French Ministry of Defence in close vicinity with the war fighters (see focus 3). These labs offer new opportunities for the end-users to explore new ideas, to experiment and test new solutions. They act as catalysts in the user centric approach. As already illustrated in large established companies, fostering these initiatives requires explicit support at the highest levels of the military hierarchies.

Focus 3 – The development of military labs in France to focus on experimentation with war fughters

The Battle Lab of the French Army (launched in 2019), the N@vy Lab and the Fuscol@ab of the French Navy (launched since 2018) and the evolution of missions for the French Air Warfare Centre (initially created in 1933 as "Centre d'experiences aériennes militaires" with a focus on the elaboration of doctrines and the reception of materials, now "Centre d'expertises aériennes militaires") all orchestrate the direct involvement of war fighters in the innovation process. These initiatives also connect with universities and start-ups through the "participative innovation program" run by the French Defence procurement agency DGA to fund prototypes (Perrin and Guerini, 2019). They contribute to spreading out the user-centric innovation approach inside the French Ministry of Defence. The French Innovation Agency and its Defence lab will develop complementarities and networked activities with these labs in the future. Future will tell about the density of these connections.

The French Army aims at providing an appropriate environment to test and experiment with actual operational staff. To encourage war fighters to contribute to the activities, the lab's team is setting up a network of "contact persons for innovation" inside the French Army operational units. Human resources management make it now also possible to position officers from the operational staff in the Battle lab for specific periods of time. The French Army also prepares an educational program to develop entrepreneurial mindsets towards innovation.

The Navyl@b is located inside the Centre d'expertise des programmes navals (CEPN), the unit in charge of technico-operational studies. It supports the experimentation of new ideas coming from the French Navy operational units in relation with the development of new digital technologies for tactical issues. Candidate projects are selected according to three criteria. The inventor must be able to devote time to the project (with validation by the hierarchy). Second, the proposed solution shall be brand new. Third, the l@b assesses the trade-off between development costs and the value in use of the new solution. The Navyl@b also runs yearly hackathons in collaboration with THALES and Ecole 42, and different engineer schools. The Fuscol@b is entirely dedicated to innovation projects proposed by, and developed for, the French Navy green berets and special forces.

As a technico-operational centre, the CEAM or Air Warfare Centre contributes to the validation of complex systems for the French Air Force (Mérindol, 2009). It hosts 23+ teams and more than 700 experts. The recent attention devoted to bottom up initiatives materializes with informal exchanges among Air Force experts at international level. The challenge is to develop new warfare scenarios and develop the subsequent experimentations in using creativity protocols such as hackathons.

NEW INTERACTIONS BETWEEN DEFENCE INSTITUTIONS, THE INDUSTRY AND (BASIC AND APPLIED) RESEARCH

Open innovation reshapes the governance of innovation networks present in the development and production of military capabilities. The challenge is threefold:

- Redefine roles and relationships between system integrators and Defence institutions as clients to develop and produce complex military technological systems.
- Change the approach to assess the criticality of industrial and technological capabilities related to militaries capabilities. This point implies a shift from the concept of Defence Industrial and Technological Base (DITB) to an analysis in terms of Defence ecosystem.
- Encourage the emergence of a variety of (innovation) intermediaries to enlarge the range of actors and competences present in the projects and align strategies and interests.

New interactions between system integrators and Defence clients

Due to the importance of digitalisation, machine learning, AI and data fusion, the development of military programs has become more complex than ever. This implies the integration of a wide variety of innovations. One of the issues at stake is to install system integrators in the dynamics of open innovation. This requires renewing both their roles and interactions with military end-users and Defence institutions. This aspect is a key for the transition of new technologies from the exploration to the exploitation phase.

"Smart" Defence clients and system integrators must gain in flexibility in order to combine the techno-push and user centric models. The goal is to enhance the capacity to easily introduce new technological components coming from various actors and networks. In this perspective, "smart" Defence clients and system integrators should work in tandem to foster transversal approaches inside complex programs that are still mainly organized in a vertical techno-push way (Mérindol and Versailles, 2018). They should take advantage of interdependencies with other programs and activities to promote modularity and design open technological architectures. These elements are in line with recent comments by Taylor and Louth (2020) about the difficulty at integrating new solutions coming from start-ups into large programs (and at finding out solutions to welcome start-ups into integration networks), and the difficulty at adapting start-ups to the specific culture and ways of working of Defence procurement agencies. This requires adaptations for Defence policy makers and the industry in the traditional management of technology. The role of ministries of Defence should for instance lead to stipulating operational specifications and not to listing technological contents for the programs (Versailles, 2005a; b) as was often the case in France (Betch and Gasilloud, 2018). This also requires adaptations in the management of innovation. Recent evolutions seem to go in the right direction as suggested with the recent organisational instructions ("IM 1618" that replaced in January 2019 the "IM 1516") that shifted the organization of innovation-related activities from programs to capabilities. Time will tell whether mindsets and practices follow.

New interactions between Defence and system integrators should contribute to reshaping collective strategies for identifying intersections between civilian and military needs. The

user-centric approach makes it possible to identify the dual potential of technologies at the early stages of the development of programs (Yeong Ng and al. 2018).

In another research (Mérindol and Versailles, 2018), we have explored large established firms that develop horizontal diversification strategies to operate smooths transfers of technologies between adjacent markets. This is typically the case with THALES at the crossroads between Defence, aerospace, Security and transportation sectors. It is easy to illustrate these aspects with components (such as GNSS sensors) or sub-systems such as air surveillance radars that can be easily adapted either to military non-cooperative environments or to civilian air traffic management. THALES runs in-house resources to identify opportunities for this "global dual-use" strategy, and negotiate adaptations with each category of clients (including the downgrading of "nice-to-have" specifications in exchange for significant reductions for the total cost of possession). They also know how to handle the coordination between programs, their respective tempos and timelines. Similar instances can be found with tier 1 and tier 2 major suppliers.

We have identified several barriers blocking smooth application of this new approach leveraging on the full potential for dual-use rationales: this strategy is only easy to install when it does not lead to reconsider the nature of interdependencies inside the supply chain, or when it does not generate a new repartition of value along the value chain. This means that the typical repartition of value, influence and power between system integrators and their main suppliers shall be considered here as both an opportunity and a limitation to this potential "global dual-use" strategy (Mérindol and Versailles, 2018). Who will negotiate with the "smart" client? How will the "smart" client react to such options? Who will contribute to the governance of the program on the industry side?

Transitioning from Defence industrial "bases" to Defence ecosystems

From the end of the Second World War onwards, the concept of "Defence industrial base" (DIB) has represented a key approach for developing industrial policies related to Defence issues (Dune, 1995; Versailles, 2003). The concept refers to a closed model of innovation: the perimeter of critical industrial and technological competences necessary for the development of military capabilities is mainly defined (and nurtured) by direct financial links between the industry and ministries of Defence. The DIB identifies clear

and explicit boundaries around these critical competences. Managing these networks in a long-term perspective has always been a key issue (Versailles, 2005b).

The analysis in terms of DIB shows the direct influence of Defence policy makers on the structure of the industry and on the trajectories for innovation (Matelly and Lima, 2016). These elements also apply to the European Defence Fund (EDF). Its 2021-2027 multi-annual framework notably materialise with support to cross-border competitive collaborative projects covering "the entire R&D cycle" and incentivise the elaboration of projects and consortiums including SMEs. Open questions relate to the transformation of exploration projects into actual acquisition and production programs, to related public procurement procedures, and to the evolution of governance at national and European levels Defence- and Security-related programs. The limits inherently associated with public policies related to the DIB emerge when (legitimately) bridging with other public policies in relation with innovation. In the EDF case, the links with other European initiatives (PESCO, European Peace Facility, and Horizon Europe) automatically open questions about the management of dual-use technologies and competences.

Boundaries have blurred with the technological evolutions linked to the digitalisation. This is the reason why the open innovation model is required today. Firms and research centres working directly with ministries of Defence represent a part of critical industrial and technological competences required for the elaboration of future programs, but they do not represent the whole network of competences required for developing the military capabilities anymore. Digital technologies, machine learning and data fusion, robotics, artificial intelligence are partly and/or completely developed outside the boundaries of the DIB. They emerge from new ecosystems and from start-ups born in these ecosystems. International industrial leaders in these areas locate (partly or completely) outside the direct influence of Defence innovation networks and of Defence policymakers in Western countries. At the minimum, it is necessary to point out that exploration activities in these areas are not driven by military issues anymore. However, significant efforts are required to access to new competences and attract new actors. This represent one of the greatest challenges for Defence policy makers as shown by the initiatives launched in the United Kingdom (see focus 4). Taylor and Louth (2020: 16) explain that traditional Defence-related actors miss the entrepreneurial attitude towards risk typical of start-ups unless it is mitigated with (public) financial resources and fast public procurement decisions. They

identify issues with risk management rationales for organizations and individuals, with implications about the reliability of the conclusions of the innovation process. We zoom out from their considerations to point out the difficulty at handling at the same time the discrepant mindsets and attitudes typical for each sector.

Open innovation implies a new vision to appraise critical competences required for developing military capabilities and take them from different worlds. The concept of ecosystems becomes more relevant than the DIB approach. It offers opportunities to appraise networks with flexible boundaries that depend on economic and technological ties, and on the degree of interdependencies between actors during the creation and capture of value (Adner, 2017; Jacobides, 2018). Multiple ecosystems relate to Defence issues. They represent a mix of networks with small and large firms, research centres and academic stakeholders. These ecosystems characterize with strong and direct ties with Defence clients (Mérindol and Versailles, 2018). The centrality of dual-use technologies varies in these ecosystems. Sometimes, system integrators operate in several ecosystems at the same time, where their influence and degree of autonomy to build innovation strategies vary. In some of these ecosystems, they operate as orchestrators of the value chain. In others, they do not have much influence and cannot frame any collective strategy. All these aspects create new constraints and opportunities for the development of new technologies for military capabilities.

Focus 4 – The British Ministry of Defence as orchestrator of new ecosystem on Defence issues

In the United Kingdom, the Ministry of Defence has recently launched two initiatives to develop new Defence ecosystems: the UK JHub and the Defence and Security Accelerator (DASA).

The UK Jhub aims at creating direct links between military end-users and providers of technology, especially start-ups that have never worked with the Ministry of Defence before. It offers opportunities to experiment and develop new concepts. It organizes as an open and friendly coworking space, located near the British tech city, with various visualisation tools and creative rooms. The agile structure interacts with 200 start-ups specialized in bitcoin technology, artificial intelligence, robotics, etc. They consider themselves as “scouts” rapidly assessing the solutions proposed by start-ups and identifying how to create value with them for Defence issues. They also appraise how to rapidly transfer these solutions throughout the Defence institution. The UK Jhub can also be involved in cocreation processes with the start-ups to adapt solutions to military needs, and launch tests and experimentations. In this case, the management of IP preserves the opportunity for start-ups to freely exploit these solutions for

civilian purposes, but restrictive clauses prevail for exploitation in military environments. Priority is then granted to British military services.

The Defence and Security Accelerator (DASA) was launched in 2016 with a staff of 50 people. It is co-located with DSTL, the RD agency of the British ministry of Defence and is also connected with 11 regional based innovation partners (mainly universities, such as Cranfield University). The DASA focuses on the creation of new networks for military issues by encouraging new entrants. It aims at changing mindsets and ways of working between the British MoD and suppliers of technological solutions (traditional and non-traditional suppliers of the British Defence). DASA also funds projects where SMEs and universities collaborate to develop new ideas and accelerates the transition to military capabilities. Large companies play a key role as partners of DASA initiatives.

New intermediaries connecting Defence with actors not usually active in military programs

In the open innovation context, intermediaries play a central role and become focal actors. They help connect heterogeneous competencies together, develop shared meanings, and align interests. Various intermediaries are present in the ecosystems. They do not necessary focus only on technological interfaces but they encourage the emergence of new formal and informal relationships between two categories of economic actors: the ones traditionally active in military programs, and the ones who are not typically active in these networks (scientists, students, start-ups, etc.).

Several agencies and units representing Defence institutions act as intermediaries. We offer key illustrations for public intermediaries in this paper. All facilitate the emergence of new communities to complement their respective national frameworks. All elaborate on open innovation to support Defence organizations to think "out of the box" and attract talented start-ups. DARPA (cf. focus 1) focuses on disruptive technologies. The NATO Innovation Hub (cf. focus 5) builds (virtual) communities fostering new ideas and concepts for developing new militaries capabilities inside the Alliance. The French Defence Innovation agency orchestrates new relationships between the French MoD, Defence firms and research centres that are not traditionally present in Defence ecosystems. These intermediaries are staffed with open minded individuals who have also a strong culture about Defence operations and institutions. They often behave as boundary spanners who contribute to build bridges between military organizations and

actors not yet related to Defence, and progressively build together some common understanding suited for innovating together.

Focus 5 – NATO Innovation Hub: Open innovation to foster new ideas and concepts for NATO capabilities

The NATO Innovation Hub was created in 2013 inside the ACT command. Today, it runs two activities. First, it hosts virtual international communities to foster the development of new ideas and design new concepts for NATO military capabilities. This represents its initial activity. Second, it runs a lab to develop software applications for NATO operational uses. NATO Innovation hub is staffed with 20 people with strong military background.

Open innovation and frugal innovation have always been key references for the NATO Innovation Hub. It is designed as an agile structure missioned to think "out of the box" and deliver rapidly new ideas and concepts by collecting expertise outside Defence organizations. It focused at the beginning on new training tools. The NATO Innovation Hub now addresses diverse topics, depending on the agenda of the Transformation Command. Recent activities have been dedicated to foresight studies on warfighting at the horizon 2040

The NATO Innovation hub locates in a friendly space inside the University of Norfolk. Its position inside the university offers easy contacts with start-ups, faculty members and students. They often offer internships for Master students in different areas (graphic artists, engineers, political science, etc.). As the Hub's main activities organize around the animation and facilitation of international and virtual communities, only a small volume of networking activities take place in the physical space itself.

The Hub hosts virtual communities about innovation to enrich NATO vision and analysis. It animates 3 communities, for a total of more than 3,500 members: "end-users" (expressing operational needs), "providers" (from basic research, the academia and the industry), and "capability designers" (who translate the providers' contributions into solutions meeting the end-users' needs). 40% of these members are military staff from NATO countries and the other 60% are scientists located all around the world. Scientists are the most active "givers" in the community. Most scientists were not previously connected with Defence networks and topics before joining the Hub's community. The NATO Innovation Hub also mobilizes new structures to enrich foresight analysis. As an illustration, it has recently connected with the "IHEDN jeunes" network, a French specific education program dedicated to students addressing Defence and international security challenges.

The NATO Innovation Hub organizes Innovation challenges and generates opportunities for start-ups to connect with NATO operational issues. It runs innovation challenges and hackathons on a regular basis. Each year, one of the NATO countries hosts an international challenge. A new topic is jointly selected by the hosting country and by NATO Transformation command. The goal is to motivate the participation of inventors, small companies and start-ups.

The challenge runs as another instance of agility and frugality. Topics are promoted on social networks and social media. Candidates first apply with one-page long presentations, eventually complemented with videos, photos and/or slideshows. On this basis, a committee with technical experts then selects about 10 projects (per event). The selected teams then have 3 months to prototype their solution with regular support by the Hub's staff to ensure better understanding of the military specificities and help the teams focus on the operational issues at stake. In the final round, the teams pitch in front of an international committee (either face to face, or via videoconference) and the best solutions are acquired for NATO capabilities through national procurement budgets.

on aerial imagery. The Hub's hackathon generates lots of interest among start-ups as previous winners leveraged on this visibility to raise their series A and B funding rounds. As an illustration, Dataiku was awarded 2 of the 3 prizes in the 2018 hackathon for its solution to the challenge using deep learning for object detection on aerial imagery. This was a major step in their journey to become a "unicorn" and a Gartner 2020 "leader". As a consequence of winning NATO Innovation Hub's hackathon, Dataiku was under contract with the US Air Force to develop its solution further. NATO Transformation Command announced in Feb. 2020 that they selected Dataiku as the reference platform for machine learning and the development of operational uses of AI throughout NATO member nations. Both NATO Transformation Command and Dataiku publicly acknowledge that this journey started with interactions and acculturation efforts developed during the 2018 hackathon.

Beside public intermediaries affiliated with Defence institutions, private intermediaries play a key role to renew the management of innovation inside ecosystems and support the elaboration of new business models. These intermediaries attract and encourage the development of start-ups addressing military issues. For ministries of Defence and system integrators in the industry, collaborating with start-ups has become now mandatory to accommodate emerging and disrupting technologies such as artificial intelligence and other "deep techs". Such collaboration carries its own challenges. *First*, the focus on Defence markets is not automatically a safe bet for start-ups because these markets have their own barriers to entry and their specificities. The Defence and aerospace industry is structurally steered by large firms and 1st tear suppliers in charge of the integration of complex systems that are enforcing the specific standards issued by Defence institutions. These companies remain reluctant to encourage new entrants because start-ups may disrupt their own technological strategies and their business models. *Second*, there is a cultural gap between Defence organizations and aerospace leaders on one side, and the world of start-ups on the other side. Differences in size, resources, and agility make it difficult to find appropriate ways to collaborate. The main obvious features materialize in

decision making processes: start-ups exhibit rapid reactions while ministries of Defence and system integrators, as any large established organization, are structured with long, formal and complex decision-making processes.

Specific intermediaries such as corporate incubators and accelerators are run by large companies to address these challenges. The Airbus group runs its BizLab to promote the search for aeronautic applications with digital start-ups. This corporate accelerator has locations in France, Germany and India. THALES also launched an accelerator dedicated to cybersecurity and located inside Station F facilities in Paris. Rolls Royce launched an accelerator program steered by its "Data lab" located in India. In collaboration with large companies, private actors act also as new intermediaries and contribute to renew Defence and aerospace ecosystems. Other initiatives focus on acceleration and business development for the private sector: Starburst launched its Accelerator to support the development of start-ups active in "deep techs" and provide new solutions for Defence and aerospace markets at international level (cf. focus 6). This accelerator shows the importance of the intermediation function to overcome the shortcomings of the traditional ways of managing innovation. The perspectives illustrated in France with Starburst, the ASD industry and Defence administrations show the importance and relevance of organizational intermediaries to handle these issues. Lots of institutional, cultural and organizational issues still exist.

Focus 6 – Starbust: The importance of organizational intermediaries for Defence and aerospace ecosystems

The focus on intermediation roles for innovation represents Starburst distinctive originality. Starburst was created in the early 2000s. This firm has progressively focused its activities on the ASD sector. Starburst currently combines two activities: consulting services on the management of innovation for large firms, the initial activity of the company; and the acceleration of start-ups in Defence and Aerospace ecosystems. In the future, they expect to install incubation and pre-incubation activities, and to detect technological inventions in research labs. They also prepare activities in venture capital. Starburst scouts start-ups with already available technological demonstrators (after TRLs 5-6). They work with 50+ industry leaders that commit as partners (initially in Paris, France: with Thales, Safran, or Airbus Industries; now all over the world, with offices in Munich, Los Angeles, San Francisco, Tel Aviv, Abu Dhabi, Seoul and Singapore). All these companies commit to be present in the maturation of technologies with experimentation, upon matching proposals introduced by the Starburst team. Projects focus on deep techs and on enabling technologies (sensors, machine learning, cybersecurity,

robotics, AI, etc.) making a difference for future military capabilities. Starburst works in direct connection with large Defence companies for a quick appraisal of the value of technological solutions for military markets. Experimentations make it possible to appraise the business potential, and the integration into business and technological portfolios operated by the established companies present in the ASD sector. The acceleration program has a 12-month duration, with senior coaching and mentoring, and support to series A fundraising. It is based on service for equity rationales, negotiated on a case by case basis with each start-up.

They have partnerships with more than 30 aerospace and Defence companies and 100 labs and universities, mainly located in Northern America and in European countries. More than 5,000 start-ups are in Starburst's radar today: 45% of them locate in Northern America, 40% in Europe and 15% in the rest of the world. Between 2015 and 2019, 21% of the start-ups in the acceleration program successfully raised series A rounds. In 2019, this proportion reaches 50%, thus showing the importance of making the connection between start-ups and established companies already present in the ASD sector.

The Starburst Accelerator case is interesting to illustrate the importance of intermediation. It operates in an ecosystem of companies embedded in complex co-opetitive relations: all of them compete against each other and cooperate together at the same time. This implies the ability to manage at the same time bilateral relationships with corporate partners and with an international portfolio of start-ups. Fostering open innovation initiatives does not mean that activities are open to anything and to anybody. The intermediation challenge locates in the ability to find the proper balance between collaboration and openness, and to introduce the relevant negotiation about property rights and business control. Starburst and their industrial partners offer a great illustration of the capacity to manage various degrees of openness in the ecosystems build around each industrial actor of the aerospace and Defence sector. Another challenge lies in the ability to develop a climate of trust with Defence-institutions (MoDs, military staff, procurement agencies) and common understanding about tendencies and priorities for the future. The intermediation role also manifests in France with the animation of the Defence Lab for the French Defence Innovation Agency, and of the associated coworking space dedicated to start-ups, to meetings, and to the organization of events relevant for the whole ecosystem.

CONCLUSION: REDESIGNING DEFENCE INNOVATION POLICIES IN THE OPEN INNOVATION CONTEXT

Other recent policy papers have already stressed the importance of introducing more "agility" in Defence administrations (Taylor and Louth, 2020). We support their

conclusions, but our points develop much beyond the boundaries of closed innovation models and of the existing "Defence industrial base".

Open innovation implies to reshape Defence industrial policies by defining various tools to empower for openness (with various openness degrees) to actors not yet related to Defence. Defence needs to gain in flexibility in managing strategic ecosystems and to develop a dynamic vision of interdependencies among actors. These aspects impact the ways of working in open innovation, and the management of openness. This transformation is a mandatory step towards the preservation of leading capabilities.

However, this process takes time because it implies cultural changes, the adoption of new practices and a new vision of innovation networks. The new design of Defence innovation policies will elaborate on three dimensions:

- Systematic introduction of a user centric approach for managing innovation and complex programs.
- Diversification of public policy instruments to both attract new talents and secure the access to critical suppliers. This implies constant trade-offs between tools and perspectives fostering network openness and controlling key technologies for military capabilities.
- Promotion of new intermediaries inside and outside Defence organisations.

The conceptual elements described in this paper do not discuss the resources required for the installation of a sustainable industrial policy in relation with Defence and Security issues. Two "elephants" have been sitting in the room for decades: the eventuality of an autonomous Defence industry for Europe, and the actual strategy framing interactions and cooperation between European and American Defence industries. Current European initiatives to foster the appropriation of Defence programs and fund innovation all represent interesting opportunities for the future. However, prudence dictates to acknowledge that thinking in terms of Defence ecosystems and operating open innovation rationales both remain agnostic as regards these two "elephants". Transitioning from closed Defence industrial bases to open ecosystems will therefore have to clear, or adapt to, very old – yet vivid – strategic challenges. ■

REFERENCES

Adner, R. (2017). Ecosystem as Structure: An Actionable Construct for Strategy. *Journal of Management*, *43*(1), 39–58.

Bahemia H., Sillience J, Vanhaverbeke W. (2018). The timing of openness in a radical innovation project, a temporal and loose coupling perspective, *Research Policy*, 47 (10), 2066-2076

Becht O. et Gassilloud T. (2018). *Les enjeux de la numérisation des armées*, Rapport d'information n° 996, France : Assemblée Nationale.

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

Bonvillian W. B., Van Atta R., Windham P. (2019) *The DARPA model for transformative technologies: perspectives on the US Defense Advanced Research Projects Agency*, Washington: Open book publishers

Bonvillian W.B. and Van Atta R. (2011), ARPA –E and DARPA: applying the DARPA model to energy evaluation, *Journal of Technological Transfer*, 36, 469-513.

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

Colataa P. (2015). An organizational perspective to funding science: collaborator novelty at DARPA, *Research Policy*, 44 (4), 874-887.

Dougherty G.M. (2018). Promoting disruptive military innovation: Best practices for DoD experimentation and prototyping programs, *Defense ARJ*, 255(1-2), 2-29.

Dugan R.E. and Kaigham J., Gabriel J. (2013). Special forces innovation: How DARPA attacks problems., *Harvard Business review*, Oct.

Fuchs E. (2010). Rethinking the role of the State in technology development: Darpa and the case for embedded network governance, *Research Policy,* 39(9), 1138-1147.

GAO, (2004) 'Best Practices: Using a Knowledge Based Approach to Improve Defense Acquisition', Washington DC, January 2004.

Hippel Von, Eric v. (2005). *Democratizing innovation*. Cambridge, Mass.: MITPress,

Iansiti, M. (1997). *Technology Integration: Making Critical Choices in a Dynamic World,* Cambridge, MA: Harvard Business School

Jacobides, M. G. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39* (March), 2255–2276.

Matelly S. and Lima M. (2016). The influence of the State on the strategic choices of Defence companies: the cases of Germany, France, and the UK after the Cold War, *Journal of Innovation Economics and Management*, 2(20), 61-88.

Mérindol V. (2009). *Gestion des compétences et gouvernance de l'innovation* : *la Défense dans l'économie fondée sur la connaissance.* Collection « Recherche en gestion », Paris : Economica.

Mérindol V. (2015). Technologie de l'information et variété des formes de co-création : vers un nouveau paradigme pour la Défense américaine, *Gérer et comprendre,* 119 (mars).

Mérindol V. (2016). *Innover en entreprise : de l'incantation à l'action, des secteurs dits traditionnels à la nouvelle économie*, Rapport de l'Institut de l'entreprise, Paris (http://www.newpic.fr)

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

Mérindol V. et Versailles D. W. (2018). Construire les interdépendances entre business models dans une stratégie de diversification reliée, *Finance, Contrôle et Stratégie*, numéro spécial « Du Modèle d'affaires à l'Ecosystème », NS-1.

Mérindol. V., Bouquin N., Versailles D. W., Aubouin N., Capdevila I., Le Chaffotec A. (2016). *Livre blanc des open labs en France. Quelles pratiques ? Quels changements* ?, Paris, Chaire newPIC de Paris School of Business et plateforme Futuris de l'ANRT.

Perrin C. et Guérini J.-N. (2019). *L'innovation et la Défense,* Rapport d'Information n°655, Sénat, France.

Taylor, T. and Louth, J. (2020). *The challenge of change. Acquiring technologies for Defence in the UK*. RUSI Occasional paper, March, ISSN 2397-0286.

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

Versailles D.W. (2005b). La nouvelle gouvernance des programmes de Défense : les relations entre l'Etat et l'industrie, *Revue d'économie industrielle*, 112 (4è trimestre), 83-105.

Versailles, D. W., (2003). Le concept de base industrielle et technologique de Défense: époques, approches, acteurs, chapitre 1, pp 9-36 in Versailles D. W., Mérindol, V. et Cardot P. (2003), *Recherche et technologie, Enjeux de puissance*, Paris: Economica.

Wilkinson M., Jewell S. (2017). *UK Defence Innovation – Design and Implementation of a system to realize value through exploitation of novelty"*, London*:* Niteworks White Paper, November

Yeong Ng J.C., Wen Song K., Tan Q. (2018). Expanding the scope of application of user innovation theory – a case study of the civil-military integration project in China. *International Journal of Innovation Studies*, 2, 33-41

#60
Policy Paper

THE (R)EVOLUTION OF DEFENCE INNOVATION MODELS: Rationales and Consequences

Valérie MERINDOL is Full Professor of Innovation at Paris School of Business where she jointly heads the newPIC chair with David W. Versailles since 2014 specializes in the management of innovation and creativity. Recent projects relate to the management of open innovation laboratories and of innovation platforms, with recent field research on deep techs, biotechs, and healthcare. Valerie is also a founding partner in the Luxembourg-based consulting company ISK Consulting SA, specialized in the management of innovation, in the management of knowledge, in corporate strategy and in the elaboration of business models / *vm@newpîc.fr*

David W. VERSAILLES is Full Professor of strategic management and innovation studies at Paris School of Business where he jointly heads the newPIC chair with Valerie Mérindol since 2014 specializes in the management of innovation and creativity. David W. Versailles is also a Visiting Full Professor at Luxembourg School of Business since 2019. In parallel to his academic positions, David W. Versailles is also today a Founding Partner and the CEO of the Luxembourg based consulting company ISK Consulting SA, specialized in the management of innovation, in the management of knowledge, in corporate strategy and in the elaboration of business models / *dwv@newpic.fr*

July 2020

The views expressed here are solely those of the author. They do not reflect the views of any organisation.

ARES GROUP

The Armament Industry European Research Group (Ares Group) was created in 2016 by The French Institute for International and Strategic Affairs (Iris), who coordinates the Group. The aim of the Ares Group, a high-level network of security and defence specialists across Europe, is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.

CONTACT [Pilots]:
Jean-Pierre Maulny, Édouard Simon, Olivier de France, Sylvie Matelly
ares@iris-france.org
+33 (0)1 53 27 60 60

www.iris-france.org/ares
#AresGroup