НАЦИОНАЛНА СИГУРНОСТ

ЕКОСИСТЕМИ ЗА ОТБРАНИТЕЛНИ ИНОВАЦИИ: МРЕЖОВ МОДЕЛ ЗА ПРЕХОД ОТ НАУЧНИ ИЗСЛЕДВАНИЯ КЪМ СПОСОБНОСТИ



ИВАН ИЛИЕВ
УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ
И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ, СОФИЯ, БЪЛГАРИЯ
АВТОР ЗА КОРЕСПОНДЕНЦИЯ: 9123490-1@UNIBIT.BG

Иван Владимиров ИЛИЕВ *е специалист по информационна сигурност и докторант по национална сигурност в Университета по библиотекознание и информационни технологии. Притежава магистърска степен по бизнес администрация и управление със специализация „Висш мениджмънт“ и бакалавърска степен по планиране и прогнозиране на икономическите системи от Университета за национално и световно стопанство. Професионалният му опит обхваща киберсигурността, стратегическите анализи, управлението на европейски проекти и инвестиционното планиране. Участвал е в разработването и координацията на научноизследователски и иновационни проекти, включително в областта на блокчейн технологиите. Преминал е допълнителни обучения по информационна сигурност, лидерство, международни отношения и публична дипломация*

Резюме: *Статията предлага мрежов модел на екосистема за иновации в отбраната, насочен към прехода от научноизследователски резултати към практически отбранителни способности. Чрез качествен документален анализ и проектно ориентиран синтез е разработена концепция за координационен център, свързващ университети, научноизследователски институти, предприятия и публични институции, без да дублира съществуващата инфраструктура. Моделът определя институционалните отговорности, механизмите за управление и четири последователни етапа на оценка: приемане на потребността, готовност на прототипа, приключване на изпитванията и документирано решение за последващо развитие или внедряване. Разгледани са допълващите се функции на Европейския фонд за отбрана, ускорителя на НАТО DIANA и Иновационния фонд на НАТО, както и ограниченията пред трансграничното сътрудничество. Предложена е рамка за едногодишно пилотно прилагане с показатели за ангажираност на крайните потребители, напредък на изпитванията, решения за преход, административна ефективност и качество на участието. Основният принос е интегрирането на институционалното управление, доказателствата за проектен напредък и оценката на резултатите в общ модел. Практическата му ефективност остава непроверена и изисква пилотно изпитване и последваща оценка.*[1]

Ключови думи: *иновации в отбраната; управление на научните изследвания; технологичен трансфер; технологии с двойна употреба; развитие на отбранителни способности; трансграничното сътрудничество*

DEFENCE INNOVATION ECOSYSTEMS: A NETWORKED MODEL FOR RESEARCH - TO - CAPABILITY TRANSITION

IVAN ILIEV
UNIVERSITY OF LIBRARY STUDIES AND
INFORMATION TECHNOLOGIES, SOFIA, BULGARIA
CORRESPONDING AUTHOR : 9123490-1@UNIBIT.BG

Ivan Vladimirov ILIEV *was born on Aug 11, 1991 in Sofia. He is an information security specialist and a PhD student in National Security Program at the*

University of Library Studies and Information Technologies (ULSIT). He obtains a Master's degree in Business Administration and Management, specialization in Senior Management, as well as a Bachelor's degree in Planning and Forecasting of Economic Systems from the University of National and World Economy. His professional experience encompasses cybersecurity, strategic analysis, European project management, and investment planning. He has participated in the development and coordination of research and innovation projects, including projects in the field of blockchain technologies. He has also completed additional professional training in information security, leadership, international relations, and public diplomacy.

Ivan Iliev speaks English language at level C1.

Abstract: *A documentary study proposes a networked defence innovation hub linking research, industry and public users. It specifies governance, transition gates and evaluation criteria; practical effectiveness remains untested.*

Key words: *defence innovation, research governance, technology transfer, dual use, capability development, cross-border cooperation*

INTRODUCTION

Defence innovation requires more than scientific outputs or technically promising prototypes. Research organisations, companies and public users must agree on the problem, testing conditions, ownership of results and the next step towards use. The issue addressed here is institutional: how can these decisions be connected without creating another isolated research organisation?

The paper combines a research report and its accompanying presentation into a focused conceptual contribution. It proposes a distributed Defence Innovation Ecosystem Hub, a transition procedure and a first-year evaluation framework. These are design proposals, not findings from a completed implementation.

THEORETICAL BACKGROUND AND METHODOLOGY

Innovation-system approaches emphasise interaction between knowledge producers, industry and government. The Quadruple Helix developed by Carayannis and Campbell additionally includes the media- and culture-based public [1]. A structure comprising universities, research institutes, companies and public institutions therefore does not reproduce that framework: two categories remain research organisations, while civil society is not a separate participant.

This paper consequently uses "four-institutional-group model" rather than treating those groups as the canonical four helices. The distinction preserves the manuscript's practical division of work without making an unsupported theoretical equivalence. Public accountability and responsible-use review remain necessary; their effectiveness would require separate assessment.

The study applies qualitative documentary analysis and design-oriented synthesis. The two author-supplied manuscripts provide the design baseline. Academic literature and official programme documents are used to compare institutional functions, support mechanisms, transition requirements and cross-border constraints. No interviews, survey, statistical estimation or causal evaluation are reported.

Comparison distinguishes collaborative R&D funding through the European Defence Fund (EDF) [2], acceleration and testing support through NATO DIANA [3], and venture investment through the NATO Innovation Fund (NIF) [4]. These mechanisms are examined for complementary functions rather than ranked by effectiveness. Official descriptions demonstrate institutional mandates, not successful outcomes in the proposed Hub.

The analytical sequence is: identify the transition problem; allocate institutional responsibilities; specify evidence required at project gates; relate support instruments to development needs; and formulate a testable implementation plan. Outputs are governance rules, a transition pathway and evaluation criteria. The resulting model is intended for national or cross-border adaptation, subject to local legal and resource conditions.

RESULTS: INSTITUTIONAL DESIGN AND TRANSITION GATES

The proposed Hub is a coordination secretariat connecting existing laboratories, research facilities, industrial sites and public testing environments. It should not initially duplicate their infrastructure. Universities contribute knowledge and talent; research institutes provide applied research and technical evaluation; companies undertake engineering and industrial integration; public institutions define needs and retain adoption responsibilities.

A steering council would approve priorities and resources. An end-user board would define problems and acceptance criteria; scientific and industrial reviewers would assess feasibility and integration. Security, legal and ethical screening would precede sensitive work. A professional secretariat would manage agreements, facilities access and progress records. These are proposed functions, not established bodies.

Each project would enter through a Transition and Exploitation Plan naming a user sponsor, the intended application, starting and target technology readiness, test arrangements and a prospective exploitation route. It would distinguish pre-existing intellectual property from new results and specify access, publication and data-use rights. Ownership is contractual and law-dependent; no universal entitlement is assumed.

Four gates structure progression: problem acceptance; prototype readiness; test completion; and a documented transition decision. At each gate, technical evidence and the credibility of the next step are reviewed together. Decisions may continue, redirect, suspend or close a project. A successful test alone does not create a procurement commitment.

Possible routes include licensing, joint development, a research spin-off, a controlled public-sector pilot or funded further research. Selection should reflect technical maturity, user demand, certification needs and lifecycle costs. Civilian revenues may support dual-use development, but civilian suitability does not establish defence suitability. Security, safety, export restrictions and responsible-use conditions require project-specific review.

FUNDING AND CROSS-BORDER COOPERATION

EDF supports collaborative defence research and development [2]. DIANA combines challenge-based acceleration with mentoring, testing facilities and connections to defence users [3]. NIF provides venture investment and operates independently of NATO structures [4]. Their different functions require separate eligibility and financing decisions (Table 1).

Table 1. Support functions and transition needs

Mechanism	Main function	Hub requirement
EDF	Collaborative defence R&D	Plan testing and the post-project route.
DIANA	Acceleration and testing	Define user needs and validation criteria.
NIF	Venture investment	Demonstrate a viable company and growth case.
Public pilot / procurement	Contractual testing or adoption	Confirm lawful procedure, budget and acceptance.

Source: Author's synthesis of [2-4]; the final row is a proposed transition function, not a funding entitlement.

The European Commission identifies legal, administrative and language obstacles, limited access to classified information, security-of-supply requirements, certification and export controls as barriers for defence SMEs [5]. The proposed response is early screening, complementary partner selection and shared project-management support, rather than an assumption that international funding removes these barriers.

Non-classified work packages can widen participation but cannot replace required controls. Consortium agreements should define integration responsibility, access rights and decision deadlines before development begins. A transition review should involve the prospective user, technical reviewer and funding or procurement representative. It should record unresolved conditions rather than interpret programme participation as a promise of purchase.

IMPLEMENTATION AND EVALUATION FRAMEWORK

A first-year pilot should start with one clearly defined, non-classified mission and existing facili-

ties. Initial activities would map partners and infrastructure, agree governance and select two or three priorities. A small challenge call would then support three to five applied teams, subject to available resources. These numbers are planning assumptions, not achieved results or validated forecasts.

During the final phase, teams would conduct controlled demonstrations and document a continuation, redirection or closure decision. Expansion should depend on assessed demand and evidence of manageable delivery costs. No predetermined number of successful procurements is proposed.

Table 2. Proposed pilot monitoring criteria

Criterion	Measurement / evidence
User commitment	Projects with named sponsor and acceptance criteria / supported projects.
Test progression	Projects completing planned tests / projects due for testing.
Transition decision	Projects with documented next-step decision / projects reaching review.
Administrative efficiency	Time and staff effort per agreement and gate review.
Participation quality	Substantive SME work packages and recorded decision roles.

Source: Author's proposed evaluation framework. Ratios require stated denominators and reporting periods; a zero denominator is reported as not applicable.

Baseline records should capture maturity, prior funding, intended users and available infrastructure. Follow-up should include delayed and discontinued projects, expenditure and reasons for gate decisions. A documented closure may demonstrate responsible resource allocation; it should not be relabelled as successful adoption. Before-and-after changes describe pilot experience but cannot alone establish the Hub's causal effect.

DISCUSSION AND CONCLUSION

The contribution is an integrated institutional design connecting responsibilities, transition evidence and monitoring. Its practical value remains unproven: the source base is selective, programme descriptions are not impact evaluations, and local feasibility requires stakeholder consultation and a costed plan.

Defence innovation should be managed as a pathway from an accepted need to a justified next-step decision. The proposed Hub supports that pathway without replacing researchers, suppliers or public authorities. Pilot evaluation should test coordination costs, access to testing and progression towards use, rather than infer success from the establishment of a new institution.

REFERENCES

[1] **E. G. Carayannis, D. F. J. Campbell.** "Mode 3" and "Quadruple Helix": toward a 21st century fractal innovation ecosystem. International Journal of Technology Management, 46(3/4), 2009, 201–234. doi:10.1504/IJTM.2009.023374.

[2] European Commission. European Defence Fund. Programme description, n.d. https://commission.europa.eu/funding-and-tenders/find-funding/eu-funding-programmes/european-defence-fund_en (accessed 20 October 2026).

[3] NATO. Defence Innovation Accelerator for the North Atlantic (DIANA). 1 July 2026. https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana (accessed 20 October 2026).

[4] NATO Innovation Fund. About. n.d. https://www.nif.fund/about/ (accessed 30 October 2026).

[5] European Commission. Defence SMEs. n.d. https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en (accessed 22 October 2026).

1. **Ivan Iliev i**s a doctoral researcher at ULSIT, Sofia, working on national security, cybersecurity, governance and emerging technologies.