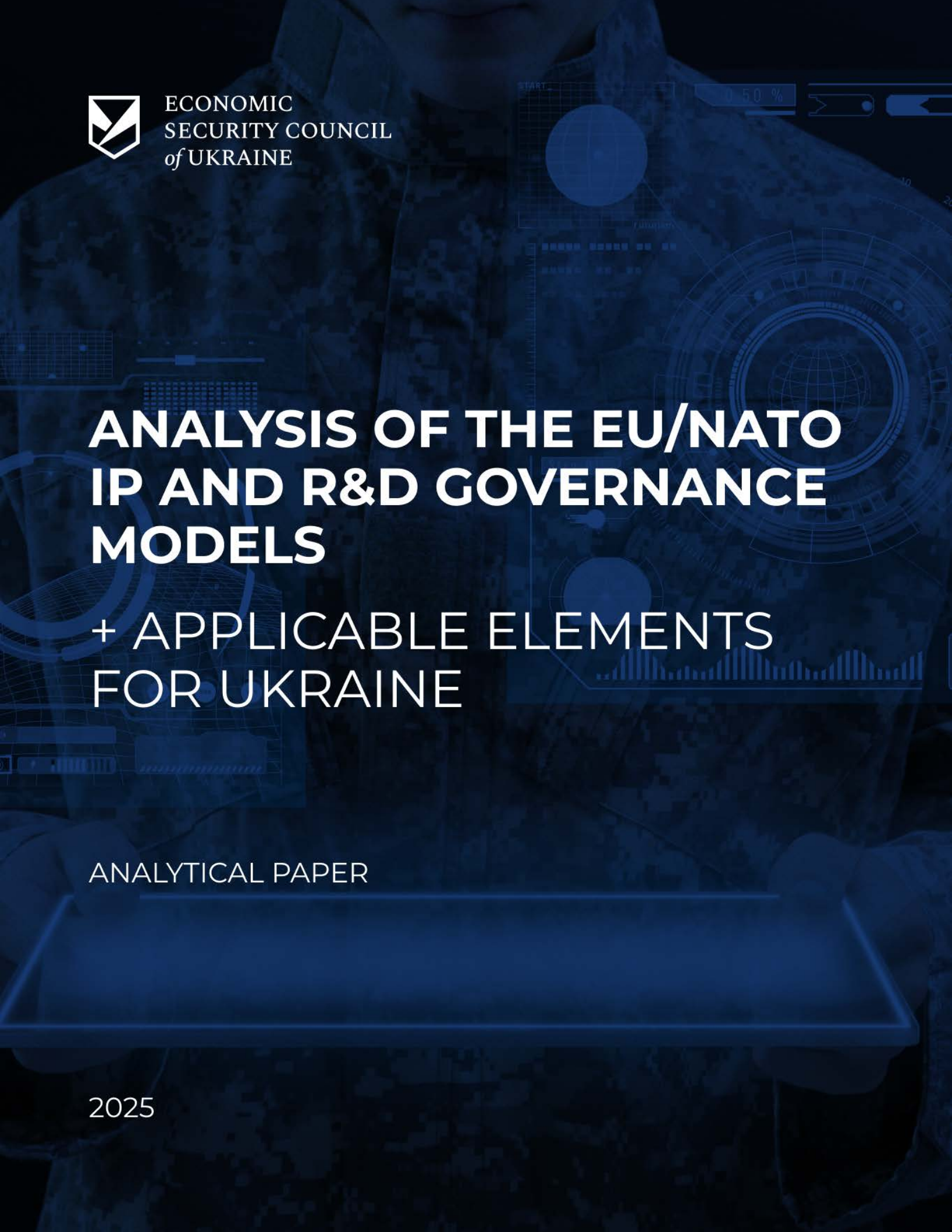


ECONOMIC
SECURITY COUNCIL
of UKRAINE

ANALYSIS OF THE EU/NATO IP AND R&D GOVERNANCE MODELS

+ APPLICABLE ELEMENTS FOR UKRAINE

ANALYTICAL PAPER

2025

CONTENTS

ABBREVIATIONS:

ACT/SACT – Allied Command Transformation / Supreme Allied Commander Transformation (NATO)
AFU – Armed Forces of Ukraine
CSO – Collaboration Support Office (NATO STO)
DMP – Data Management Plan
DIANA – Defence Innovation Accelerator for the North Atlantic (NATO)
EC – European Commission
EDA – European Defence Agency
EDF – European Defence Fund
EU – European Union
IP – Intellectual Property
IPR – Intellectual Property Rights
MoD – Ministry of Defence
NCIA – NATO Communications and Information Agency
NSPA – NATO Support and Procurement Agency
OCCAR – Organisation for Joint Armament Cooperation (multinational procurement agency)
PCP – Pre-Commercial Procurement
PPI – Public Procurement of Innovative solutions
R&D – Research and Development
STO – Science and Technology Organization (NATO)

1. EXECUTIVE SUMMARY

The European Union employs an innovation-driven and market-oriented approach to defence R&D and IP governance, whereas NATO prioritises security, interoperability, and unrestricted operational access for Allies. The two models differ in terms of culture and mechanics, yet they are complementary in terms of strategic effect.

In the context of EU programmes, such as the European Defence Fund (EDF) and Horizon Europe, project participants maintain ownership of newly developed technologies, with the European Commission refraining from asserting claims over the outcomes of these endeavours.

For instance, the European Commission's Horizon Europe programme has allocated €7.9 billion for the 2021-2027 period to research and development initiatives. These grant agreements explicitly guarantee the beneficiaries ownership of the results generated from these actions (Article 16 of the EDF Model Grant Agreement). In recent calls, EU consortia have delivered joint prototypes such as the Eurodrone and collaborative unmanned systems demonstrators, all governed through shared foreground IP rules.

This approach fosters the commercialisation of industry and the dissemination of R&D outcomes on a broad scale. Conversely, NATO structures regard technology as a strategic asset. In instances where NATO common funds finance development, the Alliance typically assumes responsibility for securing the intellectual property rights (patents, data, etc.) for the Alliance.

It is evident that NATO R&D initiatives frequently place significant emphasis on the dissemination of information within a select community, such as among member governments, along with the implementation of classification controls. This is indicative of the organisation's prioritisation of security concerns. Recent innovation programmes initiated by NATO, such as DIANA, signify a paradigm shift in the field. These programmes offer financial grants to nascent enterprises without the expectation of equity or intellectual property rights being transferred, thereby enabling innovators to maintain complete ownership of their ideas and innovations. This approach aligns with practices observed in the European Union, where a similar policy is in place to encourage the development of cutting-edge solutions.

The NATO model, however, employs a distinct rationale. STO conducts approximately 140 collaborative research activities on an annual basis, engaging over 3,500 scientists. These activities culminate in the production of technical reports, which are subsequently made available to the entire Allies community. In the context of NATO-funded contracts, agencies such as NCIA have been observed to employ systematic methodologies to secure unlimited-use rights to software, data and technical information. This approach is undertaken to ensure full operational freedom across the Alliance. DIANA is representative of a controlled exception within the NATO ecosystem: it encourages early-stage innovators by guaranteeing full IP retention, while still enabling secure testing, evaluation, and follow-on adoption through NATO's operational structures.

For Ukraine, the optimal path is a hybrid governance model:

– EU-style clarity on IP ownership, background/foreground structure, licensing, and contractual discipline;
– NATO-style protection of sensitive technologies, unrestricted government-use rights, and alignment with interoperability and export-control norms.

Such a combined approach would ensure both industrial competitiveness and secure integration into Euro-Atlantic defence frameworks.

1.2 KEY FINDINGS

- **Institutional Models:** The EU operates through formalised, regulation-based structures (European Commission, EDA, OCCAR), which provide legal clarity, uniform rules, and predictable funding mechanisms. NATO relies on decentralised, nation-driven structures (ACT, STO, NCIA/NSPA), where cooperation is voluntary and operationally focused.

- **Funding Logic:** The EU deploys large-scale, multi-annual grants (e.g., EDF, Horizon Europe) that reward collaboration, ensure foreground IP ownership by participants, and encourage industrial exploitation. NATO uses limited common funding and primarily coordinates national contributions, supplemented by new innovation tools such as DIANA grants and the NATO Innovation Fund.

Implication for Ukraine: develop grant-based incentives for domestic innovation and mirror NATO's practice of securing government-use rights in fully state-funded projects.

- **IP Ownership & Rights:** EU projects distinguish background vs. foreground IP – participants must share background needed for the project and jointly manage new "foreground" results. IP generated ("results") is owned by the creators or consortium, not by the EU. In NATO procurement or common projects, the default is Alliance ownership or at least broad user rights for all Allies if they paid for development. This ensures interoperability and access, but can limit industry's commercial exploitation.

- **Data Management & Security:** EU frameworks encourage dissemination of research results and data (with exceptions for security/classified projects), aiming for civilian spin-off benefits and transparency. NATO emphasizes controlled dissemination: research within NATO's Science & Technology Organization (STO) leads to publications often restricted to member defense communities, aligned with NATO security classification. Handling of classified or sensitive R&D outcomes is stringent in NATO, whereas the EU tends to avoid classified projects or uses national security exceptions sparingly.

- **Export Control & Sovereignty:** The EU model builds in sovereignty safeguards by excluding non-EU control over project IP (EDF mandates no third-country entity can control foreground IP). NATO's model must navigate multi-national export control regimes (especially US ITAR regulations) on a case-by-case basis, which can complicate technology sharing among Allies.

- **Contracts & Agreements:** EU programs use grant agreements and consortium contracts with detailed IP clauses (e.g. joint ownership rules, mandatory exploitation or dissemination plans, dispute resolution via arbitration or national courts). NATO efforts often rest on Memoranda of Understanding between governments or NATO agencies' contracts, with bespoke clauses for each project and disputes handled through arbitration under NATO procurement rules or bi-national agreements.

- **Culture & Incentives:** EU governance seeks to incentivize innovation through competition, prizes, and intellectual property rewards (companies benefit commercially from EU-funded R&D). NATO's collaborative culture in R&D is built on burden-sharing and standardization-nations contribute knowledge to collective projects for mutual benefit (e.g. 140+ STO activities yearly with 3,500 scientists sharing research), often without direct commercial reward, focusing instead on improving collective capabilities.

Applicable Elements for Ukraine.

From these findings, several practical elements can be adopted in Ukraine's defence R&D governance:

- **IP Policy Framework:** Implement clear rules distinguishing state vs private IP in defense projects (mirroring EU "foreground" concepts and NATO nations' practice of state-owned service inventions). Fast-track the pending legislation on service

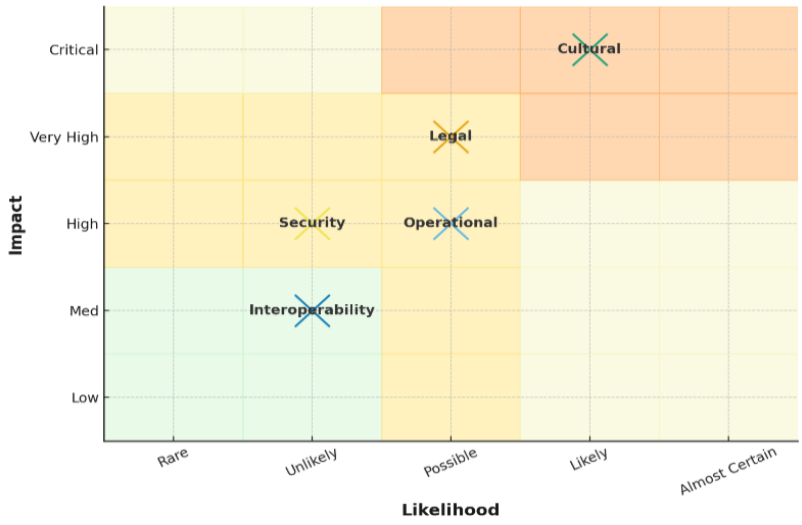
inventions to firmly vest MoD with ownership of military R&D results while crediting and rewarding inventors.

- **Data & Classification Management:** Develop a protocol for deciding early whether a defense innovation will be patented and published or kept classified (akin to NATO nations' approach). Accompany this with a Data Management Plan template for each R&D project to specify handling of sensitive information (who can access, what can be published).
- **Contracting Models:** Introduce model R&D contract clauses that balance innovation incentives with state interests – e.g. similar to EU PCP contracts where companies retain IPR but government obtains free usage licenses. Also consider NATO-style clauses for projects fully funded by government: if MoD pays for a development, MoD should have rights to use/modify across the Armed Forces. Standard IP clauses for defense procurement contracts will reduce ambiguity and disputes.
- **R&D Process & Collaboration:** Establish processes for collaborative projects with allies that mirror EU/NATO best practices: use MoUs or agreements that address joint ownership and info security upfront. For example, adopt NATO's practice of a Technology Transfer Working Group to handle IP terms with foreign partners, ensuring Ukraine can both protect allied IP and share its own innovations appropriately.
- **Governance & Institutional Setup:** Empower the new MoD IP Directorate as the central authority to oversee IP in all defense R&D. Set up an interagency "IP Board" or coordination committee (MoD, economy, justice, strategic industries) to align policies – a lesson from NATO's need for cross-cutting coordination among commands and agencies.
- **Financing & Incentives:** Leverage financing instruments that encourage innovation – e.g. small innovation grants or prizes for soldiers and engineers (following EDA's innovation prize model) to surface new ideas. Create a defense innovation fund or partner with allied funds (like NATO's Innovation Fund) to co-finance Ukrainian startups, ensuring IP stays in country but with pathways for NATO interoperability.
- **Interoperability & Standards:** Align definitions and standards with EU/NATO to ease cooperation. For instance, adopt NATO-compatible classification levels for technical data, use STANAG-aligned data formats, and follow EU standards for research ethics and IP reporting. This will make it easier to plug Ukrainian R&D projects into EU or NATO programs in the future.
- **IP Due-Diligence in External Procurement & Cooperation:** Introduce a formal IP due-diligence procedure for all cases where Ukraine procures technologies from private suppliers or receives systems from allied nations. This should include a systematic review of licensing terms, export-control constraints, and any third-party patent rights embedded in the solution.
- **Expert Review of Imported or Jointly Developed Technologies:** Establish a dedicated IP expert review mechanism to verify clean title of rights, assess compliance with licence conditions, and confirm "freedom to operate" for the Ministry of Defence. This team would also evaluate potential vulnerabilities related to foreign components subject to ITAR-like restrictions or proprietary subsystems controlled by external actors.
- **Protection Against Downstream Legal and Export Risks:** Integrating such due-diligence into the R&D and procurement workflow would safeguard Ukraine from litigation, inadvertent violations of export-control rules, and future obstacles to re-export or international cooperation involving the resulting systems.

Together, these findings demonstrate that neither the EU nor NATO model is sufficient on its own for Ukraine's current wartime and transition context. A hybrid framework is required – one that ensures secure state control over defence-critical technologies, while enabling industry-led innovation, scalable licensing, and alignment with Euro-Atlantic cooperation mechanisms.

1.3. RISK HEATMAP OF THE IMPLEMENTATION OF THE IP REFORM

This section provides an analytical overview of the key risk factors affecting the implementation of the Defence IP Governance Reform. The assessment identifies and prioritises systemic, operational, and cultural risks that may hinder the reform's effectiveness. The document is exclusively concerned with the identification, scoring, and prioritisation of risk. The assessment is indicative of the wartime operating environment; however, it also identifies elements to be adapted for the transition and peacetime phases.



Risk Heatmap

In implementing these changes, Ukraine faces several risks that vary in severity and likelihood:

- **Legal risk (Medium–High):** Adoption of new laws may be delayed, or conflicts with existing regulations could slow progress. Moreover, the current reform package in the MoD addresses only *service inventions by military inventors*, leaving broader regulation of intellectual property rights in defence (e.g. involving civilian contractors, joint ventures, or private companies) unresolved. This gap could undermine coherence of the system and create disputes in multi-actor projects.
- **Operational risk (Medium):** The MoD's new IP processes may not be uniformly applied at first, and institutional capacity gaps remain. Units and agencies might interpret policies differently, leading to inconsistent protection of innovations and potential loss of valuable IP.
- **Cultural risk (High):** Shifting the entrenched mindset from secrecy and individual ownership to structured sharing and state stewardship will encounter significant resistance and inertia. Inventors may remain hesitant to disclose ideas if they distrust the system or fear losing recognition.
- **Security risk (Medium):** Stronger IP disclosure mechanisms, if not paired with robust classification protocols, could inadvertently expose sensitive information. The balance between dissemination for innovation and secrecy for security must be carefully managed.
- **Interoperability risk (Low–Medium):** If Ukraine's reforms are not fully aligned with NATO and EU norms, there is a danger of developing isolated practices. This could complicate collaboration with partners or exclude Ukraine from multinational projects.

Heatmap interpretation: Cultural change and legal adoption appear as the "hot" zones requiring the closest attention. Operational and security risks are "warm" but manageable with

targeted capacity-building and improved classification protocols. Interoperability risks remain at the lower end but must still be monitored to avoid divergence from Euro-Atlantic standards.

1.4. MULTI-CRITERIA RISK ASSESSMENT FOR DEFENCE IP GOVERNANCE REFORM IN UKRAINE

The methodology employed in conducting the risk assessment involved the utilisation of the Multi-Criteria Risk Assessment (MCRA) model. The MCRA model is utilised to evaluate risks in the present wartime operational environment.

It is possible that a peacetime weighting configuration will be introduced at a later date, reflecting different institutional priorities (e.g. a stronger compliance and governance focus).

At present, all weights and thresholds are reflective of the necessity for accelerated decision-making and diminished bureaucracy under wartime conditions.

Criteria Description

Each risk is evaluated according to seven scientific and operational criteria, capturing strategic, operational, economic and international dimensions:

Code	Criterion	Description	Evaluation Logic	Relevance (Wartime)
P – Probability	Likelihood of the risk materializing	How often or how easily the negative event may occur	1 = Very low, 5 = Very high	high wartime relevance
I – Impact	Strategic and operational consequences	Measures severity: operational losses, capability gaps, reputational harm, financial cost	1 = Negligible, 5 = Catastrophic	high wartime relevance
V – Velocity	Speed of impact realisation	How fast the consequences harm defence capability if the risk occurs	1 = Slow, 5 = Immediate	high wartime relevance
D – Detectability	Detectability / warning capability	How difficult it is to detect the risk before consequences occur	1 = Easy to detect, 5 = Almost invisible	higher relevance during transition
R – Recoverability	Ability to restore situation	Cost and time needed to mitigate consequences once they appear	1 = Quick recovery, 5 = Nearly impossible to recover	higher relevance during transition
E – Export & Regulatory Effects	Exposure to international IP/export control constraints (ITAR, 3rd-party control)	Higher values indicate greater dependency and strategic vulnerability	1 = No effect, 5 = Very severe restrictions	stable across both
A – Alliance Alignment	Compliance with NATO/EU rules and	Higher score = greater misalignment and	1 = Fully aligned, 5 = Non-aligned	

	cooperation standards	risk of reduced cooperation		

These criteria are specifically designed to cover **defense-unique factors**: secrecy, dual-use constraints, allied interoperability and technological sovereignty.

Weighting and Formula

Importance weights were assigned based on expert judgement focused on defence operational mission priorities.

Criterion	Weight (wi)
Probability (P)	**0.20**
Impact (I)	**0.25**
Velocity (V)	**0.15**
Detectability (D)	**0.10**
Recoverability (R)	**0.15**
Export Effects (E)	**0.10**
Alliance Alignment (A)	**0.05**

Weighted Risk Score:

$$RS = \sum(w_i \cdot x_i)$$

Total RS is within **1.0-5.0 scale**.

Interpretation Thresholds

Score Range	Risk Level	Category	Required Action
4.0–5.0	Critical	Red Zone	Immediate management & strategic intervention
3.0–3.9	High	Amber Zone	Leadership-level mitigation & continuous monitoring
2.0–2.9	Medium	Yellow Zone	Targeted control measures
1.0–1.9	Low	Green Zone	Periodic monitoring

1.4 Risk Assessment Results *(Scores represent consolidated expert judgement).*

A. Governance, Legal & IP Management Risks

Risk #	Risk Description	RS	Level
1	Loss of state control over publicly funded IP	4.10	Critical
2	Production blocked due to unresolved IP disputes	3.85	High
4	Excessive secrecy limiting commercialisation	3.40	High
6	Inventors conceal innovations; ideas disappear	3.45	High
9	Private ownership blocks military exploitation	3.55	High
10	Legal disputes delay capability fielding	2.95	Medium
11	Lack of legal/IP expertise in MoD structures	2.90	Medium
14	Corruption in IP registration or contracting	3.55	High
15	Misclassification of information	3.40	High
16	Licensing failures block serialisation	3.85	High

18	No centralised defence IP registry	3.15	High
22	Grey-zone privatisation of defence IP	3.45	High
23	Legal gaps in software/data rights	4.10	Critical
24	"Prototype graveyard": no transition to serial production	3.85	High
29	"Valley of death" due to unclear IP status	3.90	High

B. Operational & Strategic Risks

Risk #	Risk Description	RS	Level
3	Leakage of critical technologies to hostile states	4.60	Critical
7	Non-alignment with EU/NATO standards	3.95	High
12	Low trust from partners in MoD IP governance	3.95	High
15	Misclassification of information (operational effect)	3.40	High
17	Dependency on foreign components/IP	4.05	Critical
19	Lack of transparency causes industry–MoD conflicts	3.20	High

C. Industrial & Economic Risks

Risk #	Risk Description	RS	Level
5	Lack of economic incentives for industry participation	2.95	Medium
13	Ineffective compensation mechanisms	2.85	Medium
20	Insufficient resourcing of MoD IP Directorate	3.35	High
21	IP lost due to personnel turnover	3.05	High

D. Cyber & Information Security Risks

Risk #	Risk Description	RS	Level
26	Cyber attacks / leaks compromising IP registry	4.30	Critical
15	Misclassification of sensitive info (cross-cutting)	3.40	High

E. Human Capital & Organisational Culture Risks

Risk #	Risk Description	RS	Level
27	HR risks: burnout, rotations, language gaps, knowledge loss	3.50	High
25	Violation of inventors' moral rights	2.90	Medium

F. International, Regulatory & Export Control Risks

Risk #	Risk Description	RS	Level
8	ITAR / foreign IP restrictions	4.25	Critical

28	Foreign ownership/control in consortia	4.00	Critical
17	Foreign component/IP dependency (cross-cutting)	4.05	Critical

Short Summary of the Critical Risk Cluster

1. **Leakage of strategic defence technologies to hostile states (RS 4.60)**
Immediate security threat: loss of operational advantage, exposure of sensitive capabilities, and accelerated adversary adaptation.

2. **ITAR and foreign-controlled IP restrictions (RS 4.25)**
Limits Ukraine's ability to deploy, modify, export or co-produce critical systems; creates long-term operational dependency.

3. **Loss of state rights to publicly funded IP (RS 4.10)**
State cannot control or scale what it pays for, leading to blocked serialisation, legal conflicts, and strategic vulnerability.

4. **Legal gaps in software and technical data rights (RS 4.10)**
Modern systems are software-defined; unclear rights prevent upgrades, integration, lifecycle management and NATO interoperability.

5. **Dependence on foreign components and IP in key capabilities (RS 4.05)**
Creates supply chain vulnerabilities, export-control exposure, and inability to sustain or scale production independently.

The aggregated risk picture indicates that Ukraine's most critical vulnerabilities lie in legal fragmentation, export-control exposure, and insufficient government rights over defence-critical technologies. These risks directly affect serialisation, operational deployment and Euro-Atlantic cooperation. Addressing them early will create a stable foundation for the full Defence IP and R&D governance reform.

2. BACKGROUND, PURPOSE & SCOPE

Effective intellectual property governance in defense R&D is a critical enabler for innovation, commercialization, and security. In modern warfare – exemplified by Ukraine's experience – technological innovation from drones to software can be as decisive as troops on the ground. IP governance determines who owns these innovations, who can use them, and how they can be shared or protected. Without clear IP rules, valuable defense innovations risk being lost, underutilized, or misappropriated.

Ukraine's Current Pain Points: Until recently, Ukraine's MoD had virtually no formal IP management. This resulted in fragmented ownership of innovations and perverse incentives. For example, between 2013 and 2023 the MoD itself registered **zero** patents, while individual researchers and even officials involved in projects privately registered hundreds. Inventions developed with state funds often ended up under personal ownership, leaving the state unable to scale them or control their dissemination. There were **no standard IP clauses** in defense contracts, so each R&D effort handled rights ad hoc or not at all. The legal status of "military service inventions" was a grey zone – unlike a civilian employee, a soldier or officer had no clear law stating whether an invention they create belongs to them or the government. This ambiguity allowed some to claim IP for themselves (even for battlefield innovations), undermining the state's interest. At the same time, a culture of secrecy prevailed without mechanisms to patent or license technologies; many innovations stayed classified or in unit-level use only, never transitioning to broader adoption. This highlights a **secrecy vs. dissemination dilemma** – excessive secrecy can impede wider exploitation of useful tech, but lack of controls can leak sensitive know-how. Another major issue was the **procurement vs.**

R&D gap: the MoD had no framework to take a prototype invented in the field and contract a company to mass-produce it because the MoD held no rights to that invention. The absence of an IP licensing mechanism meant even proven innovations could not be legally manufactured at scale for the forces. These pain points made it clear that Ukraine needed a robust IP governance model for defense.

Purpose of this Paper: This brief paper aims to analyze how the EU and NATO govern intellectual property and R&D in the defense context, and to extract practical elements that Ukraine can apply in the short to medium term. By comparing the EU's and NATO's models, we identify best practices, pitfalls to avoid, and concrete steps for aligning Ukraine's emerging system with Euro-Atlantic standards. The goal is to provide Ukrainian MoD leadership and supporting international partners with an advisory roadmap to establish an IP and R&D governance framework that both protects national security and stimulates innovation.

Scope: The analysis covers institutional roles, processes, contractual frameworks, data rights policies, classification handling, and export control considerations in EU and NATO contexts. It looks at how contracts and programs are structured, how IP ownership and usage rights are allocated, and how results are disseminated or protected. Specifically, it examines EU mechanisms such as the European Defence Fund, Horizon Europe, the European Defence Agency's projects, and OCCAR's joint procurement programs; and NATO mechanisms including Allied Command Transformation initiatives, the Science & Technology Organization's collaborative research, the NATO Communications and Information Agency's projects, and Bi-SC directives governing procurement. The focus is on governance elements relevant to defense R&D (from basic research to prototype development). This paper also touches on data rights and classification (how sensitive information is managed), and export control rules that impact technology sharing. Broader issues like general patent law or civilian IP regime are not covered except where they interface with defense R&D. The timeframe focus is on near-term implementable changes (next 3–24 months) in Ukraine's defense sector. All recommendations consider Ukraine's ongoing reforms and the need for compatibility with EU and NATO standards.

3. METHODOLOGY

This analysis was conducted as a comparative study of EU and NATO intellectual property governance models, using a combination of policy document review, case studies, and input from subject-matter experts.

Comparative Framework: We identified key dimensions of IP and R&D governance – institutional setup, funding mechanisms, contract types, IP ownership rules, data rights, security classification, export controls, dissemination practices, and dispute resolution. We then examined each dimension in the EU context and in the NATO context, allowing a side-by-side comparison (summarized in the comparative matrix in Section 7).

Sources: The study drew on official policy documents and agreements (for example, EU grant agreements and NATO directives), as well as secondary analyses. EU sources included the EDF general conditions, Horizon Europe model agreements, European Commission communications on innovation procurement, and guidelines from EDA/OCCAR. NATO sources included the Bi-Strategic Command Directive 060-070 on procurement (for NATO's stance on IP in contracts), documentation on NATO Science & Technology Organization activities, and public information on new programs like DIANA. We also reviewed case studies of specific programs: e.g., how an OCCAR-managed project handled joint IP, or how a NATO STO panel publication was disseminated. Additionally, we consulted interviews and surveys (summarized in Annex) with Ukrainian defense officials and legal experts engaged in the current IP reform,

to gauge practical challenges and needs. These interviews provided on-the-ground perspective to validate which foreign practices are most applicable to Ukraine.

The comparative analysis was qualitative, focusing on identifying strengths and weaknesses rather than quantitative metrics. However, where available, data points (such as number of projects, patents, or timeline durations) are cited to illustrate points. All sources of information are referenced in footnotes for transparency. For proprietary or sensitive insights from interviews, we provide anonymized summaries in Annex B rather than direct citations.

By triangulating policy review with case examples and expert input, the methodology ensures that the recommendations are grounded in both theory and practice. The focus throughout was on extracting actionable insights – governance elements that have been proven in EU/NATO contexts and that align with Ukraine's strategic direction (e.g. closer EU integration and NATO interoperability). All findings have been fact-checked against official documents where possible, to ensure accuracy and relevance as of late 2025.

4. LANDSCAPE & CONTEXT

Why IP Governance in R&D Matters.

In both the EU and NATO, effective IP governance is seen as essential to fostering innovation and maintaining strategic advantage. Proper IP rules create a balance between encouraging developers (companies, research institutions, even individual inventors) and safeguarding the interests of the funding stakeholders (governments and taxpayers). In the defense sector, this balance is particularly delicate: on one hand, defense R&D thrives on innovation which often comes from open exchange of ideas and collaboration (sometimes requiring dissemination of results to the broader industry); on the other hand, military technologies can be sensitive or classified, requiring restrictions on information sharing. A sound governance model ensures that when governments fund R&D, they either retain rights or obtain sufficient access to use the results (so national security isn't compromised), while still rewarding innovators and enabling commercialization where appropriate. The EU leans toward innovation and market impact – it treats defense R&D outputs as something that should eventually strengthen the European industrial base and economy. NATO leans toward security and interoperability – it treats R&D outputs as assets to be shared among Allies for collective defense, often with controlled access. Both perspectives highlight that IP is not just a legal technicality; it's a tool of strategy, deciding who can make and deploy a new technology.

Ukraine's Challenges in Context: Ukraine historically inherited a Soviet-style approach where defense innovations were state secrets by default, with little concept of intellectual property incentives. This led to a stagnation in formally captured innovation – people didn't bother to patent or document because it was either secret or not rewarded. As described earlier, this resulted in a fragmented landscape: individual claims and no central ownership. Additionally, Ukraine's defense R&D has been underfunded and ad-hoc, with many innovations emerging informally during the war (e.g. frontline soldiers hacking together drone modifications). The lack of an IP framework meant those grassroots innovations stayed at the tactical level. Now, as Ukraine strives to modernize and integrate with Western practices, it faces the task of building an IP governance system from scratch in the middle of an ongoing conflict. The current reform momentum – the new MoD IP Directorate, new draft laws, pilot projects – is effectively Ukraine catching up on two fronts: aligning with EU's innovation-driven model and with NATO's security-driven expectations. Both EU and NATO partners are keen to see Ukraine improve IP protection, as it affects cooperation: allies need assurance that any tech they share will be handled properly (e.g. not leaked, but also possibly not locked away unused). Likewise, donors and industry partners want to know that if they help develop a technology in Ukraine,

there are clear rules on ownership and usage. Ukraine's candidacy for EU membership also adds impetus – the EU acquis (body of law) on intellectual property and innovation must be met, and strong IP protection is viewed as a driver of investment and collaboration.

Key Issues to Address: Several specific issues form the landscape that Ukraine must navigate, drawing lessons from EU/NATO:

- **Fragmented Ownership:** Without clear rules, multiple stakeholders (inventors, units, private firms) claim pieces of IP. EU projects solve this by consortium agreements clarifying ownership up front, and NATO often establishes in MOUs who will own what. Ukraine will need to formalize ownership in every project (the draft service IP law will make the state the default owner for military inventions, simplifying this).
- **Absence of IP Clauses:** Historically no IP clauses in contracts meant uncertainty. Both EU and NATO never embark on R&D without an agreement on IP (e.g., the EDF grant agreement devotes an entire article to IP rights). Ukraine's defense contracts will need standard IP clauses inserted, and MoD directives to enforce their use.
- **Secrecy vs Dissemination:** EU practice shows that not all defense R&D needs to be secret – many projects publish results or at least share them across Europe to maximize usage. NATO practice shows that some results must remain classified for coalition use only. Ukraine must develop criteria to decide which innovations to openly patent (thus disseminating knowledge but protecting via legal IP) and which to keep classified for national security. The new procedure in the draft law requiring a decision within 4 months to patent or classify is a direct attempt to emulate best practice and avoid paralysis.
- **Procurement–R&D Gap:** EU and NATO both recognized the "valley of death" problem between prototypes and adoption. EU addresses it with initiatives like PCP/PPI bridging procurement with R&D, and NATO's Rapid Adoption Service under DIANA aims to fast-track promising tech to military use. Ukraine similarly is piloting a licensing mechanism to let MoD license inventions to manufacturers. The context is that, to fight a war effectively and rebuild after, Ukraine cannot afford R&D that languishes – every good innovation must find a path to deployment. Governance must link the innovator in the lab or field with the procurement official and industry, through IP licenses and contracts.
- **International Collaboration:** Ukraine's defense is now heavily intertwined with partners (weapons aid, joint projects). Lack of an IP framework was a gap that could scare off partners – but by establishing legal rules, Ukraine sends a signal that it will respect allies' IP and also assert its own where appropriate. NATO countries typically have arrangements among themselves for co-development (like US and European allies often sign project agreements covering IP). Ukraine is not yet in those frameworks formally, so it has to be proactive in setting bilateral IP terms. This paper's context analysis suggests borrowing NATO-like templates for tech exchange: e.g. if a NATO country shares a prototype, have an agreement that Ukraine can use it under license. Conversely, if Ukraine develops a new capability, ensure it can license or share it with allies without losing control.

Conclusion of Landscape: Ukraine stands at a crossroads where it can design a hybrid IP governance model drawing on the best of both worlds – the EU's openness and innovation incentives and NATO's focus on security and equitable access. The landscape review underscores that IP governance is not an abstract legal issue; it directly affects military effectiveness, alliance cooperation, and defense industrial growth. By understanding how the EU and NATO handle these issues, Ukraine can avoid re-inventing the wheel and instead leapfrog to a modern, robust system. The following sections delve into those EU and NATO models in more detail, before converging on what Ukraine should adopt.

5. EU MODELS OVERVIEW

This section reviews the European Union's models for IP and R&D governance in the defense domain, focusing on key institutions, funding instruments, IP rules, and contract types.

5.1 INSTITUTIONS AND PROGRAMS

European Commission & EDF: The European Commission plays a central role via the European Defence Fund (EDF), a flagship program since 2021 to fund collaborative defense research and development among Member States. The EDF is managed by the Commission (DG DEFIS) and supports projects through competitive calls. It has both "research actions" (100% grant-funded R&D projects) and "development actions" (co-funded projects for prototyping). The Commission sets the rules and evaluates proposals, ensuring that projects align with EU capability priorities. Another Commission-led program relevant to dual-use R&D is **Horizon Europe**, the EU's civilian R&D framework (2021–2027). While not defense-specific, Horizon has security research strands and innovation ecosystems that defense actors can leverage. The Commission's Horizon rules on IP are similar in structure to EDF's (given EDF's MGA – Model Grant Agreement – is largely based on Horizon templates with some stricter conditions for defense).

European Defence Agency (EDA): The EDA, an EU agency, facilitates cooperative defense R&T among member states. EDA runs projects where a few interested countries agree to jointly fund R&D (often called Category B projects), and it also launched the **Preparatory Action on Defence Research (PADR)** in 2017–2019 (which piloted EU defense research funding ahead of EDF). The EDA provides templates for project arrangements among nations and offers an **IPR Helpdesk** to advise on intellectual property in those cooperative projects. While the EDA does not disburse large grants like the EDF, it is a forum to coordinate multinational projects and advise on best practices, including how to handle IP among the contributing nations and industries.

OCCAR: The Organisation for Joint Armament Cooperation is not an EU institution but a multilateral agency (involving several EU nations) that manages collaborative armament programs (e.g. the A400M transport aircraft, Eurodrone, etc.). OCCAR's model is relevant as it has its own established conventions and procedures for contracts. Within OCCAR-managed programs, participating nations usually sign a Memorandum of Understanding that covers intellectual property and technical information rights. OCCAR then places contracts with industry on behalf of those nations. For example, OCCAR's standard contract conditions (OMPs – Organization Management Procedures) include specific clauses on Background Technical Information and foreground IPR use rights. Typically, industry must grant to the participating governments a royalty-free license to use any background IP needed for the program purpose, and foreground IP from the contract can be used by those governments for defense use (while companies might retain the right to commercialize externally with consent). OCCAR essentially embodies a European approach to joint development that ensures all partners can use the results.

Other EU Initiatives: The EU also supports innovation via **prizes** (e.g. EDA's Defence Innovation Prize which awards funding to novel concepts – winners keep their IP but commit to further development) and via regional programs. Additionally, NATO-adjacent EU initiatives like the **Permanent Structured Cooperation (PESCO)** projects sometimes involve collaborative development with their own governance (often leveraging EDF for funding). The institutional landscape is multi-layered but generally, the European model involves formal frameworks with defined roles: the Commission for funding and rule-setting, agencies like EDA and OCCAR for

facilitating and managing projects, and member states aligning via EU mechanisms to avoid duplication.

5.2 FUNDING INSTRUMENTS AND MECHANISMS

Grants (100% or Co-Funded): The core of EU R&D funding is through grants. Under EDF research actions, the EU provides essentially full funding for early-stage research. For development (e.g. building a prototype), the EU might cover up to e.g. 20-80% with the rest co-funded by industry or participating states, to ensure buy-in. The grant approach means that participants (often industry consortiums with academia) agree to EU grant conditions, including on IP and results. A key feature: eligibility criteria require that entities are EU-based and not controlled by third countries – ensuring EU strategic autonomy in technology. Also, using grants allows the EU to require **collaboration** (minimum 3 entities from 3 countries, etc.) to foster integration.

PCP/PPI (Procurement mechanisms): Pre-Commercial Procurement (PCP) and Public Procurement of Innovative Solutions (PPI) are special instruments the EU promotes (often via Horizon or structural funds) to bridge the gap between R&D and uptake. In **PCP**, a group of procurers (e.g. defense ministries or agencies) jointly fund several companies to develop and test prototypes in stages. The unique aspect is risk-benefit sharing: the companies retain the IPR of what they develop, but the government buyers get license rights to use and can require certain conditions (like the right to license to third parties under fair terms). PCP explicitly allows procurers to not take full ownership so that companies can later commercialize the solution widely (including to other countries), while the procurers keep enough rights to deploy the solution. **PPI** is when procurers directly purchase a limited batch of a new solution that is already developed but not yet scaled – in PPI, IP is usually with the supplier unless negotiated, but since it's an actual procurement, the authority could negotiate ownership or an exclusive license if critical. These instruments have seen limited use in defense so far, but conceptually Ukraine could use PCP for, say, soliciting multiple UAV prototypes from local firms, and allow those firms to keep IP (so they can export later), while MoD gets to use the product. The EU's endorsement of PCP/PPI shows a flexible approach to IP – sometimes the state doesn't need to own the patent, as long as it can use the tech and the market can grow the innovation.

Prizes: The EU (and EDA) have used prize competitions to stimulate innovation (e.g. the EDA's annual innovation prize on specific topics like AI, materials, etc.). A prize is essentially a reward for achieving a technical goal. Typically, the winner retains their IP; the prize giver may ask for a license to use or a commitment that the idea will be developed within Europe. Prizes can bring in non-traditional actors (startups, individuals) who might not engage in formal procurements. For Ukraine, a similar scheme could encourage inventors in the military or small companies to propose solutions to defined problems, knowing they won't lose their IP but will gain recognition and funding.

Co-funding and National Programs: EU also encourages nations to co-fund projects. PESCO projects, for instance, often pool national funds and may receive EDF co-funding. Those arrangements need agreement on IP too (often falling back on either EDF rules if EDF money is involved, or a bespoke agreement if purely national funds). The common theme is that funding is tied to collaboration and sharing – the EU rarely funds a purely national project; it's always about cross-border partnerships.

5.3 IP RULES IN EU PROJECTS

Background vs Foreground IP: EU projects rigorously define these terms. **Background** is any pre-existing IP or info that partners bring to the project (e.g. a company's proprietary tech needed to perform the work). Each partner must list what background they are willing to share

for the project, and they remain owner of it. However, they must grant access rights to the others if that background is needed for the project execution or for exploiting the project results. This ensures no partner can block the project by denying use of some essential know-how. Access rights to background are typically royalty-free for project execution, and either royalty-free or fair terms for exploitation depending on what's agreed in the consortium.

Results/Foreground: Ownership of results (foreground) in EU projects stays with the participant(s) who generated them – the EU Commission explicitly "does not obtain ownership". If an outcome is created by one entity, it owns it. If created jointly by multiple beneficiaries and their contributions can't be separated, they have **joint ownership** by default. Under Horizon/EDF rules, joint owners must either reach a joint ownership agreement or abide by a default: any joint owner can use the result themselves royalty-free, and can license it to others (outside) but must compensate the others and get their consent. This default pushes consortium members to negotiate custom terms to suit their situation. Often, they agree in the Consortium Agreement on how they will handle joint IP (for example, one partner might take lead in patenting and license to the others).

Dissemination and Exploitation: EU rules strongly encourage that results be disseminated (made public through papers, conferences, etc.) unless it would harm the protection of the results (e.g. patent filings come first) or there are security considerations. Even in defense research, the expectation is to publish non-sensitive findings to advance general knowledge. Beneficiaries must also commit to exploit results (either themselves or by licensing to others or via further research) – the EDF, for instance, requires a plan for how the new technology will be taken up into actual use by militaries or industry. If a participant fails to exploit, the Commission can require them to find someone else who will (or even assign the IP to a capable entity), though this is rarely enforced strictly.

Specific EDF Conditions: The EDF, being defense-focused, adds a few special IP constraints mainly about sovereignty: any background or foreground used in an EDF project must not be subject to control or restriction by a non-EU entity. This means if, say, a company in the project had licensed US technology (ITAR-controlled) as background, and that license forbids sharing with others, it would violate EDF rules. Similarly, the foreground (new IP) arising cannot be in a situation where a third country could veto its use or export. This is to ensure that Europe can use the results freely within Europe. Practically, participants might have to sign declarations about this and design projects to use "EU/associated country technology" only. For Ukraine, aligning with this principle is important, as Ukraine will want freedom to operate with its defense tech without undue foreign veto, while also respecting allies' secret tech.

Contract Types in EU R&D: The legal instruments are typically:

- **Grant Agreements:** binding contracts between the consortium and the Commission. They incorporate standard clauses (like Article 16 on IP) and any project-specific modifications in annexes. They reference an **Annex 5** in EDF which likely contains additional IP terms, e.g., if some open-source approach is used or if ethical/security requirements impose restrictions.
- **Consortium Agreements:** an internal contract among project members (not seen by Commission) where they sort out additional details: e.g. how they'll share IP, who will patent what, how costs and profits are split, publication review procedures, etc.. The Commission mandates having such an agreement for multi-beneficiary projects (to avoid conflicts later).
- **Procurement Contracts:** If an EU agency like EDA or an OCCAR program funds a company via a contract (as opposed to a grant), then the terms are negotiated but usually follow similar logic: e.g. in an OCCAR development contract, there will be clauses on government rights to use and on the contractor's rights to further exploit. These often mirror what's in the MoU among the governments for that program.

Summary: The EU model provides a **structured, legalistic framework** where IP rights are clear and codified upfront. It tries to create win-win situations: companies get to own and profit from IP (incentive to innovate), while states ensure they can access and use the technology (through licenses or jointly owning if needed). The emphasis on dissemination and avoiding external restrictions aligns with the EU's broader goal of strategic autonomy – the EU wants a strong internal market for defense tech and reduced dependency. For Ukraine, adopting EU-style rules would mean embracing this transparency and market orientation: standardizing how consortia share IP, encouraging patents and publications (except where classified), and thinking about exploitation from the start of any project.

6. NATO MODELS OVERVIEW

This section examines how NATO as an alliance handles IP and R&D governance, noting the key institutions, mechanisms for collaboration, and approaches to intellectual property and data.

6.1 INSTITUTIONS AND GOVERNANCE

Allied Command Transformation (ACT): ACT, led by SACT (Supreme Allied Commander Transformation), is NATO's strategic command in charge of fostering innovation, concept development, experimentation, and training. ACT (based in Norfolk, USA) often sponsors R&D-related activities such as technology demonstrations, war-gaming new concepts, and coordinating NATO's Science & Technology work. While ACT doesn't have a large discretionary R&D budget like the EU's EDF, it does set priorities and manages programs like the NATO Innovation Challenge (a biannual contest) and, in conjunction with Allies, the new DIANA accelerator and NATO Innovation Fund. ACT issues guidance (with ACO, the operations command) in the form of **Bi-SC Directives** – for example, the Bi-SC Directive 060-070 on procurement policy covers how NATO bodies should conduct acquisitions, including R&D contracts and associated IP principles.

Science and Technology Organization (STO): The STO is NATO's network for collaborative defense science. It comprises the **Office of the Chief Scientist**, a **Collaboration Support Office (CSO)** in Paris, and the **Centre for Maritime Research and Experimentation (CMRE)** in La Spezia. The STO has a set of technical panels (seven panels like AVT, IST, etc., as listed in section 4) that organize research activities (studies, experiments, data exchanges). These activities are typically called "research task groups," "working groups," or "specialist meetings." Importantly, the STO operates on the principle of voluntary national contributions: nations offer their scientists' time and sometimes facilities; NATO STO coordinates and publishes results. There is usually no transfer of funds in these projects – each nation covers its own participation costs, making it a cost-effective model (NATO provides the secretariat and meeting support). The governance for STO research is through the Science & Technology Board (with representatives from nations). STO results often feed into NATO standardization or concepts. The IP aspect here is that whatever a nation contributes remains that nation's property, but by participating, nations agree that the group's collective output (like a technical report or database) can be used by all NATO members. If proprietary technology is involved, they manage it via agreements within the group (e.g. they might operate under a memorandum that restricts further sharing beyond the group). The culture is one of trust and professional exchange rather than contracts.

NATO Agencies (NCIA and NSPA): NATO's agencies also engage in R&D through procurement. The **NATO Communications and Information Agency (NCIA)**, for instance, may contract companies to develop new software prototypes or cyber defense tools for NATO. The

NATO Support and Procurement Agency (NSPA) can manage procurements for multinational projects including possibly development of equipment. These agencies follow NATO procurement rules (like the Bi-SC directives) and implement programs on behalf of groups of nations or NATO common funding. In such cases, NATO (through the agency) acts as the buyer. For example, NCIA might issue an RFP for an "innovation challenge" contract to build a prototype in AI; the contract will include clauses ensuring NATO has rights to use the deliverable in all NATO systems (an example of IP clause: "NATO will have unlimited rights to use, modify, reproduce the software for its purposes, while the contractor retains ownership and can commercialize outside NATO as long as security is respected" – specifics vary but that spirit is common).

Bi-SC Directives and Policy: NATO's formal stance on IP is encapsulated in procurement policy: as noted, the principle "if NATO pays, NATO retains the IP rights". This is a high-level rule to protect NATO's investment and ensure no vendor locks in a capability. It doesn't mean NATO will patent things itself (NATO is not a commercial entity), but rather NATO will either own the deliverables or have irrevocable licenses. Another relevant policy area is **Standardization Agreements (STANAGs)** – some of these relate to data formats, etc., which can involve IP if they incorporate proprietary tech. NATO tries to prefer open standards or get permission to use certain tech standards across Allies (sometimes negotiating alliance-wide licenses for things).

Cultural Aspects: NATO governance is consensus-driven among 32 nations. There is an inherent cautiousness about IP because of the diversity of national laws and sensitivities. For example, European NATO members might be comfortable sharing certain tech among themselves, but the U.S. may impose restrictions (ITAR) on high-tech components. Thus, NATO often sticks to the lowest common denominator – focusing on areas where sharing is possible and steering away from where IP issues would cause friction. This is a reason why NATO itself didn't historically fund much proprietary R&D – it left that to nations, except in common projects. Now with DIANA and the Innovation Fund, NATO is venturing into funding dual-use startups and projects. These are governed by their own charters (the NATO Innovation Fund is an independent investment fund with allies' contributions; DIANA is governed by a Board of NATO nations). In those, they explicitly avoid taking IP or equity to remain attractive.

6.2 COLLABORATION MECHANISMS (POW, TASK GROUPS, EXPERIMENTATION)

Programme of Work (PoW): NATO STO uses an annual Programme of Work – essentially a list of approved research activities (each proposed by nations or NATO commands). The PoW spans many topics (from materials science to AI to human factors). This mechanism allows nations to plug into whichever projects interest them. The PoW is more of a coordination tool than a funding program. The output of a PoW activity could be a **Technical Report**, **Technical Memorandum**, or even a demonstrator. Because funding is decentralized, IP arrangements are usually handled within the activity. If, say, a multi-nation experiment yields a piece of software code jointly developed, the team would likely agree that each nation can use it for defense but not release it publicly without consent – such details would be minuted in the group or handled by a limited distribution marking (e.g. "NATO SECRET").

Task Groups and Panels: Each STO panel's task group is like a mini consortium but without a formal contract. Participation is governed by the STO operating procedures. The assumption is that by contributing, you can also benefit from others' contributions. Often these groups avoid generating patentable inventions (the focus is usually research papers, reference data, feasibility studies). If any patentable idea did emerge, typically it would be pursued by the individual inventors through their national institutions, while NATO/STO might publish the general findings. There have been cases where NATO research collaborations led to follow-on development projects handled by nations or OCCAR, which then formally address IP in that next stage.

Experimentation and Exercises: NATO (especially ACT) conducts concept experiments and technology demonstrations (e.g. CWIX – Coalition Warrior Interoperability eXercise – where new tech is tested for interoperability). During these, companies might participate with their products. NATO ensures confidentiality of those proprietary products while integrating them in tests, and companies retain their IP; NATO gains insight and maybe data to set requirements or standards. There is an unwritten understanding that if you bring your tech to a NATO exercise, NATO won't steal it, but NATO also isn't giving you IP – instead NATO might later issue a requirement influenced by what it saw. So the IP governance here is ensuring NDAs and proper handling of proprietary info.

Notable New Mechanisms: The NATO Innovation Accelerator (DIANA) and the NATO Innovation Fund deserve mention as novel mechanisms:

- **DIANA:** As noted, it runs challenge calls and provides grants and acceleration services to startups working on dual-use tech. It explicitly guarantees participants keep their IP and NATO takes no ownership, which is a departure from the classic "NATO pays = NATO owns" for good reason (to encourage participation).
- **NATO Innovation Fund:** This is a venture capital fund (multinational) investing in early-stage companies in emerging tech. It will acquire equity stakes in startups. It's independent but NATO-affiliated. IP from those startups remains with them, but the Fund (and indirectly NATO nations investing) hope to guide those companies to produce tech useful for Allies. There may be side agreements or expectations that companies will not sell out sensitive tech to adversaries – that is more handled via investment terms (e.g. golden share conditions, compliance with export laws). It reflects NATO countries' recognition that to not fall behind, they must engage with commercial innovation.

6.3 IP AND DATA GOVERNANCE IN NATO

Background/Foreground in NATO Context: NATO doesn't formally use these terms in the way EU does for its projects, but conceptually:

- In NATO collaborative projects (multiple nations), each nation's prior contributions are its background; new joint results are often treated as joint property of those nations or of NATO if it's an official NATO project.
- In NATO procurement contracts (NATO buys from a vendor), the contract will stipulate that any deliverable (technical data, software, etc.) can be used by NATO. The contractor's background tech used in the deliverable might remain theirs, but NATO likely gets a license for its use. For instance, a software delivered might contain contractor-owned modules – NATO would negotiate rights to use and even modify within NATO. The Bi-SC procurement directive likely requires the CO (contracting officer) to include appropriate clauses so NATO isn't handcuffed by proprietary claims.

Classification and Dissemination: This is a cornerstone of NATO data governance. All information in NATO R&D efforts is assigned a classification or handling level (ranging from NATO Unclassified, to NATO Restricted, Confidential, Secret, etc.). Many STO publications are NATO Unclassified and even public, but if they involve sensitive tech, they may be classified. When something is NATO Secret for example, its "distribution" is limited to people with clearance in NATO countries – this effectively means the IP or knowledge is ring-fenced to the alliance. NATO has strict rules that anything classified cannot be shared with non-NATO entities (or even with NATO partner nations) without approval. This contrasts with EU projects which, except in rare cases, are unclassified and publishable. So NATO's default is need-to-know, whereas EU's default is disseminate unless told not to. Ukraine, aiming to join NATO's info-sharing, has to be capable of handling such classified info similarly.

That said, NATO also has an interest in dissemination within the alliance. Through STO, valuable research results are published as STO technical reports which are often shared widely among member states' research labs (if unclassified). If classified, they still reach all Allies' authorized personnel. This means a researcher in, say, Canada can learn from results of a project led by Italy, via STO channels – a form of dissemination albeit limited to NATO.

Data and Technical Information Rights: NATO contracts often define **"Technical Data" rights** – e.g., the right for NATO to use data delivered. If a contractor marks data as proprietary, NATO might still have rights to use it internally, but NATO would agree not to disclose it outside. For example, NCIA sometimes procures software under licenses that allow all NATO bodies to use it, but not to distribute to the public. In multi-nation projects outside NATO structures, countries sign **Data/Info Exchange Agreements** to share technical data without fear of losing control (commonly used bilateral or multilateral agreements to exchange R&D information, where each side agrees not to further disclose or use the info without permission).

Comparison with EU: The NATO model is more restrictive in dissemination but more generous in internal sharing. EU model might result in a patent (public disclosure but legal protection) whereas NATO model might result in a classified document (secret but physically protected). NATO's focus on classification is a double-edged sword: it protects secrets but can hinder the collaboration with external partners or industry that lack clearance. NATO tries to mitigate this by having unclassified "public release" versions of some research when possible.

Export Control Considerations: Since NATO includes major arms exporters with strict laws (U.S. ITAR being notable), any tech that goes through NATO channels must respect those. E.g., if a U.S. technology is involved in a NATO project, the U.S. will often impose conditions that it not be shared with certain other nations or that end-use assurances be signed. NATO has internal procedures to manage this, but effectively it means certain advanced research might exclude some allies who are not authorized. The EU avoids this by excluding third-party tech in EDF. NATO can't exclude its own members, so it relies on case-by-case negotiation and often keeps such projects bilateral or in smaller groups under NATO umbrella but not involving everyone. For Ukraine, integrating into this means its IP governance must track origin of technology (so it doesn't accidentally violate an export/license condition when sharing or selling something). The analysis of NATO shows the need for strong record-keeping of what restrictions come with which technology – something Ukraine's new IP registry can incorporate.

NATO vs EU Differences Highlighted: Summarizing the differences in IP/data handling:

- NATO approach: more **collectivist** internally (all allies share the benefits) but **restrictive externally** (protect from others), often by classification.
- EU approach: more **competitive** internally (consortia of some countries, not necessarily all) and **open externally** at least within the single market (results ideally diffuse to all EU industry, and even published globally unless it harms EU interests).
- NATO sees IP through the lens of strategic control and unity (no ally left without access), EU sees IP through economics and innovation (no company left without incentive). Ukraine's strategy should hybridize these: ensure MoD and all relevant national security actors have access to any defense innovation (like NATO would), but also ensure companies and inventors are rewarded and can spin off products (like the EU model).

7. COMPARATIVE MATRIX

Below is a comparative summary of key aspects of EU versus NATO IP and R&D governance models, followed by analytical commentary on their respective strengths and weaknesses. (See Table 1 in the Executive Summary for a condensed version).

Governance & Institutional Setup: The EU establishes formal programs with clear legal bases (EDF under EU regulations, Horizon Europe under EU law) and dedicated management by the European Commission or agencies. Decision-making is top-down (calls for proposals, evaluation, grant awards) with Member States providing oversight through committees. NATO's governance is intergovernmental: initiatives are approved by committees of national representatives (e.g. NATO S&T Board, or North Atlantic Council for big programs) and execution is often bottom-up (nations decide their participation). There isn't a single "NATO R&D authority" in the way the Commission is for EU – various bodies share responsibility. This means the EU can enforce uniform rules across all projects, whereas NATO must persuade nations to adopt common guidelines. For Ukraine, the implication is that an EU-like approach could bring order and predictability (via laws and MoD directives that apply to all projects), but a NATO-like approach reminds that flexibility and voluntary buy-in are needed (especially when working with multiple partners).

Funding & Scale: EU funding for defense R&D has grown (the EDF budget is €7.9 billion for 2021-27). It's significant and project-driven. NATO common funding for R&D is comparatively tiny (outside of new innovation initiatives, NATO largely relies on what nations volunteer). However, NATO's strength is in pooling in-kind efforts – many millions worth of research hours contributed by nations. EU's approach can inject money to drive specific outcomes (like a call on drone swarms under EDF will yield many proposals, one gets funded to build a demo). NATO's approach relies on identifying shared needs and hoping nations contribute; it can suffer if nations are preoccupied or if the benefit isn't immediately clear. For Ukraine, tapping into EU funds (eventually, as an EU member or through EDF partnerships) could be a game-changer for resources, while NATO avenues might offer more in expertise exchange and standard-setting. In the short term, Ukraine should align with EU funding practices to attract grants and with NATO practices to join joint experiments (even as a partner nation in STO activities).

Contractual Approaches: As described, EU uses formal contracts/grants with detailed terms. NATO uses either multi-nation agreements or contracts via its agencies. One notable difference is how disputes or enforcement are handled: in EU grants, the Commission can suspend funding or demand repayment if terms (including IP obligations) are breached. That threat ensures compliance. In NATO, if a nation breaches an informal agreement (like misuses shared info), it becomes a diplomatic issue – trust might erode but there's no central enforcement. With contractors, NATO agencies include arbitration clauses since NATO bodies can't be sued in national courts. So NATO's system is based on trust and mutual interest to a larger extent. Strength: it encourages consensus and goodwill; weakness: it relies on it. The EU system's strength is clarity and enforceability; weakness: rigidity. Ukraine will want clear enforceable contracts internally (to prevent misunderstandings with local industry) – that argues for EU-style. But when dealing with allies informally (like receiving some tech info), it will need to lean on trust and reciprocal courtesy, NATO-style.

IP Ownership & Exploitation: Perhaps the starkest difference: EU projects aim for commercialization – the owners of IP are encouraged to patent and market the product (the EU even measures success by patents filed, products launched). NATO collaborations aim for capability enhancement – success is measured by a concept adopted in NATO or a technology fielded in multiple armies, not by patents. In fact, patents from NATO STO work are rare (those that do occur are owned by individuals or nations outside NATO context). NATO tends to produce collective knowledge (often publicly publishable science or NATO confidential tech

data). One isn't inherently better: EU's model can produce dual-use tech that benefits economy and defense (e.g. new materials that a company can sell widely, while militaries buy it too). NATO's model can produce things like common standards (which aren't patentable but extremely valuable, e.g. a data link protocol used by all Allies). For Ukraine, both are needed: it wants a defense-tech industry selling globally (EU model outcome) *and* it wants interoperability with allies (NATO model outcome such as adopting standards). The joint ownership concept in EU is interesting to Ukraine's situation: if a Ukrainian entity co-develops with a foreign entity, rather than tussle, they could agree on joint IP with mutual freedom to use – something EU consortia often do. Meanwhile, if Ukraine fully pays for an R&D, it might follow NATO logic to keep the IP.

Data Rights & Security: EU consortia might produce open data sets or publish algorithms openly (unless participants decide to keep some trade secret). NATO research often produces classified data sets (for example, sensor readings from trials that are NATO Secret). This means NATO accumulates a lot of information in secure repositories, whereas EU tends to push info out to the public domain or at least to the market. The strength of NATO's way is security and controlled access; the weakness is it can limit innovation because fewer minds (only cleared personnel) can work on the problem. EU's open way can harness academia and industry broadly, but can also inadvertently reveal capabilities. A recent trend is EU and NATO trying to balance: EU has some projects requiring security clearance for participants now, and NATO tries to release more unclassified findings to broaden impact. For Ukraine, the lesson is to implement a tiered approach: some defense R&D outputs should be classified and only shared with those with a need-to-know (especially if they reveal vulnerabilities or countermeasure specifics), whereas other outputs can be unclassified and shared with industry to get solutions. An internal classification guide for IP (as part of the MoD's new instruction) will be vital.

Export Control & Third-Party Influence: EU's exclusion of third-party IP control is directly relevant to Ukraine as it integrates with EU-Ukraine will need to ensure, for instance, that if it uses a Turkish or Israeli component in a system co-developed with EU funds, it has rights to use/export it in the EU. NATO doesn't have such a formal rule but deals with it case by case (e.g. maybe avoid using a component that one ally can't share with another). In Ukraine's context, dealing with both Western and legacy Eastern tech, tracking origin and licensing will be important. This comparative point suggests Ukraine establish an "export control check" step in R&D project planning: mimic EU by favoring tech with clear, unrestricted licensing for Allies, and be aware of NATO members' rules so as not to violate any when sharing results.

Dispute and Enforcement: In EU, if a dispute over IP arises between partners, they ideally solve via the Consortium Agreement mediation; if not, courts/arbitration as per the contract's governing law (often Belgian law for EDF grants). In NATO context, disputes are more likely resolved through negotiation at NATO committees (because going legal is complicated when dealing with multiple national jurisdictions). For example, if two countries in a NATO project disagree on who can license an invention, they will have to talk it out or escalate to the political level. One advantage NATO has is an established habit of consultation and finding consensus; the downside is it can be slow. For Ukraine's system, having a clear legal pathway (arbitration board or designated IP dispute committee) is advised so disagreements (say between a private firm and the MoD) don't stall projects for long.

Strengths & Weaknesses Analysis: (Already partially integrated in table) – to summarize:

- EU model strengths: structured, incentivizes innovation, produces economic benefits, legally clear. Weaknesses: can be slow/bureaucratic, not always directly aligned to specific military needs (industry-led sometimes), risk of IP being held by private sector away from state use if not carefully managed.
- NATO model strengths: focuses on military utility, ensures knowledge is shared among those who need it in forces, handles classified tech appropriately, builds coalition interoperability and trust. Weaknesses: minimal commercial exploitation (misses dual-

use opportunities), less formal means potential gaps in IP protection (relies on goodwill), slower to initiate projects due to consensus.

For Ukraine, these translate into a need to combine strengths: create formal rules and incentives (EU style) to kick-start innovation, while embedding security and sharing principles (NATO style) to ensure defense needs and alliance obligations are met. The weaknesses to avoid are: over-bureaucratization that stifles frontline ingenuity (an EU pitfall) and lack of enforcement that could re-create a vacuum of accountability (a NATO pitfall).

In conclusion, the comparative analysis shows that EU and NATO models, though different, are complementary. A hybrid approach for Ukraine is not only possible but desirable – taking EU's drive for innovation and NATO's discipline of security. The next section will propose specific elements from both that Ukraine can implement.

8. APPLICABLE ELEMENTS FOR UKRAINE

Building on the comparative insights, this section groups key recommendations for Ukraine under thematic areas. These are concrete elements drawn from EU/NATO practices that Ukraine can adapt in its own IP and R&D governance, focusing on what is feasible in the near term.

- **IP Policy:** Establish a comprehensive MoD IP Policy that clearly defines ownership and rights for all defense R&D outputs. This policy should codify that inventions made by servicemembers or with defense funding are owned by the state (as per law #13110/13111), while guaranteeing inventors recognition and fair compensation. It should also set rules for private industry contributions (e.g. if a company develops something with MoD funding, MoD gets a license or co-ownership). Essentially, Ukraine's policy can mirror the EU notion of foreground IP (state or joint ownership for results of defense projects) and background IP (respecting what companies bring in), combined with NATO's expectation that the government secures rights if it pays. This policy should be public and used as the basis for all contracts and internal procedures, much like NATO nations have their defense IP policies and the EU has its framework in grant agreements.
- **Data Rights:** Implement a framework for data and technical information rights management. Borrowing from NATO's playbook, Ukraine's MoD should introduce classification guidelines for R&D information – e.g. categories like "For official use (sensitive but unclassified R&D data)", "Confidential" or higher for military-significant tech. Any project should produce a Data Management Plan (DMP) that states what data will be open, what will be restricted, and who has access. From the EU side, incorporate the practice of requiring each project to identify background data being used and securing permission for it. From NATO, incorporate the need-to-know principle for sensitive data – for example, if a prototype's technical specs are classified, ensure only those with clearance in the project can access it. Also, ensure MoD's rights to use data: e.g., all R&D contracts should include a clause that the MoD has the right to use and reproduce any data or reports delivered for government purposes (similar to NATO and U.S. contracts). This means even if a company holds IP, MoD can internally use the know-how freely across units – a critical point to avoid silos.
- **Contract Models:** Develop and roll out **model contract clauses** for different R&D scenarios, as a toolkit for procurement officers. These should include:
    - *Grant-like contracts* – for instances when MoD gives a grant to a research institute or a small business (e.g. innovation contests), using EU-style terms

(beneficiary owns results, MoD gets license to use, obligation to report and exploit results).

- *Joint development agreements* – for projects with international partners or multiple Ukrainian stakeholders, using a consortium agreement template (defining contributions, ownership shares, access rights akin to EU consortium agreements).
- *Procurement contracts (full ownership)* – when MoD fully funds a development, include NATO-style clause: MoD retains/reverts all IP rights including patents, data, etc., though the contractor may be allowed to use the technology for other purposes with permission.
- *Licensing agreements* – templates for the new pilot licensing mechanism, whereby MoD as IP owner can license to a manufacturer (including clauses on royalty, duration, sublicensing, quality control, export restrictions if any, etc.).Each model clause set should be standardized and cleared by legal authorities so that individual departments don't have to reinvent terms. This echoes EU's practice of standard grant conditions and NATO's standard clauses in procurement directives.

- **R&D Processes:** Introduce structured **R&D process governance**. This means from project initiation to completion, IP considerations are integrated. For example, when an R&D project is proposed (whether by a military unit or an external call), a quick IP review is done: what background tech is involved? Who will own what? Will results be publishable? NATO's practice here is instructive: before nations start a joint project, they agree on these things in an MoU. Ukraine's MoD could require an "IP terms sheet" for every R&D project internally. Additionally, adopt the EU practice of mid-term and final reporting that include sections on IP status (any patents filed? any disclosure that needs protection?). Leverage the **"single window" innovation portal** being launched – build into it an IP submission form where inventors must fill fields like "co-creators, prior art, classification recommendation". In essence, bake IP tracking into the innovation pipeline. Another process: establish a **technology transfer workflow** for cooperation with foreign entities, as the MoD IP directorate has proposed. For instance, if a foreign partner shares tech, have a standard review and agreement (NDA or license) in place via the Office of Defence Technology Transfer (as planned).
- **Governance (Institutional):** Strengthen and formalize governance bodies. The new **MoD IP Directorate** should be fully empowered as the central node. Emulate NATO's coordination by creating an **IP Steering Committee** that includes representatives from General Staff, procurement agencies, intelligence (for classification input), and the national IP office. This committee would review major IP decisions (like whether a breakthrough invention should be patented or kept top-secret, akin to NATO committees deciding on dissemination of sensitive STO findings). Also consider forming an **IP Advisory Board** with external experts (e.g. from industry, academia, allied advisors) to periodically review Ukraine's defense IP strategy – similar to how the European Commission convenes expert groups for EDF or how NATO engages advisory groups. The goal is to ensure cross-stakeholder visibility and buy-in, preventing the IP regime from becoming siloed.
- **Financing:** Increase and diversify financing for defense R&D with IP incentives. Allocate a portion of the defense budget or aid funds to a **"Defense Innovation Fund"** that can issue small grants or contracts to promising projects with clear IP frameworks (even possibly co-invest with NATO's Innovation Fund in Ukrainian startups, if feasible). Encourage public-private partnerships: for instance, if a Ukrainian tech firm invests in developing a product for the military, offer matching funds or milestone payments, and in return negotiate shared IP or long-term supply agreements. Additionally, set up

innovation prizes in specific priority areas (like secure communications, drone countermeasures) to reward solutions – ensure rules say winners must grant MoD a license for military use, but they keep ownership otherwise (so they can commercialize, an EU approach). Financing mechanisms should be tied to IP outcomes; e.g., bonus payments for a project that results in a granted patent or a NATO-standard contribution. This mimics EU programs that incentivize exploitation, and NATO's increasing use of seed funding to attract non-traditional players.

- **Interoperability:** Align Ukraine's IP and R&D processes to facilitate interoperability with EU and NATO partners. On a technical level, require that any defense R&D project consider NATO standards (if relevant) from the get-go – e.g., if developing a new radio, ensure it aims to comply with NATO waveforms (so referencing STANAGs). On a legal level, whenever entering a project with EU funding or NATO involvement, use the established frameworks rather than custom Ukrainian ones. For example, if Ukraine joins an EDF project, adopt the standard EDF agreement terms and just ensure Ukrainian law can accommodate them. If doing a bilateral project with a NATO ally, propose using a template similar to those the ally uses (many Western countries have standard bilateral R&D MoU templates). This avoids a patchwork of incompatible agreements. Also, language interoperability: ensure all IP documentation (patent filings, licenses) can be produced in English when needed – NATO works in English and French, EU mainly in English for technical matters, so Ukraine should maintain dual-language records for ease of cooperation.

By implementing these grouped recommendations, Ukraine would effectively create a bridge between its nascent system and the established EU/NATO best practices. Many of these elements can be initiated within 3–12 months (as requested for near-term): for instance, drafting model clauses and policies can be done in a few months; forming committees and embedding IP steps into processes can likewise be quickly ordered by MoD directive. Some elements (like financing mechanisms or fully staffing the IP directorate) may take up to a year to mature but can start now. The overall outcome will be a defense R&D ecosystem where innovation is encouraged and protected (EU-style) and where military and state interests are safeguarded (NATO-style). Table 2 in Annex A provides a checklist mapping these recommendations to specific EU/NATO references as further reading.

9. LEGAL & ORGANISATIONAL ADJUSTMENTS

Implementing the new governance model will require specific legal reforms and organizational changes. This section outlines those necessary adjustments:

Legal Reforms: The cornerstone legal change is the adoption of the **"service inventions" legislation**. Once passed, these will amend the Civil Code and related laws to explicitly recognize intellectual property created during military service as property of the state (with the inventor's moral rights and compensation safeguarded). This reform updates Ukraine's legal framework to match practices in many NATO countries (e.g., the U.S. and UK have long had provisions assigning military inventions to the government). Beyond this, additional legal moves include:

- **Amendments to Procurement Law:** Update the public procurement legislation or MoD procurement regulations to mandate inclusion of IP clauses in defense R&D and procurement contracts. This could be a simple clause added to the standard contract conditions used by the MoD's procurement agency, reflecting the new MoD IP policy (for example, "All intellectual property deliverables shall be handled in accordance with MoD Instruction X/2025, and the supplier agrees to MoD's rights as specified therein.").

- **Classification & Secrecy Laws:** Review the law on state secrets and defense information to ensure it aligns with R&D needs. Specifically, the law should allow for secret inventions to still be recorded in an internal register. Many NATO countries have a process for **patent secrecy** (e.g., filing a patent but then keeping it secret by government order). Ukraine may consider adding provisions for a "secret patent" mechanism, or at least clarifying how classified technical information can be protected (so that inventors trust disclosing it internally). If needed, amend regulations to allow the MoD to issue a confidentiality order instead of public patenting, as envisaged in the 4-month decision process.
- **Export Control Harmonization:** Align Ukraine's export control lists and regulations with those of the EU and key NATO countries so that when Ukrainian innovations reach a point of potential export, the rules are clear. This could involve updating the control lists (many of which are based on the Wassenaar Arrangement that NATO/EU follow) and ensuring the new IP law references export control compliance (for example, an inventor's obligation to not file patent abroad or export tech without permission). Establish in law or regulation the role of MoD's IP Directorate in liaising with the Export Control Authority when licensing technology abroad – so that one office coordinates both IP and export approvals for defense tech, streamlining the process (a lesson from EU/NATO where fragmentation between IP and export agencies can cause delays).
- **Dispute Resolution Mechanism:** Consider a legal provision (perhaps in the MoD internal regulations or even a law on military technical cooperation) to create a specialized **Arbitration Panel or Mediation Board** for IP disputes arising from defense contracts. This could serve as a faster, confidential way to resolve issues than going through civilian courts. NATO and OCCAR often rely on arbitration for disputes; Ukraine can mirror that by empowering a small panel (maybe including an independent expert or a retired judge) to handle, for instance, a case where a contractor contests the MoD's claim to an invention or an inventor disputes the compensation amount.

Organisational Adjustments:

- **MoD IP Office Structure:** As noted, the IP unit was established under the Military Justice Directorate, with plans to elevate it to a full Directorate by 2025. This elevation should be carried out, making the IP Directorate report directly to a Deputy Minister (as already planned). Organizational charts should reflect this, giving the IP head (Illia Kostin as per news) authority to enforce IP policy across all MoD branches. The Directorate should ideally have divisions within it, e.g., one for "Invention & Patent Management", one for "Contracts & Licensing", one for "International Technology Transfer". This specialization will help manage the workload.
- **IP Coordination across Government:** Defense IP doesn't exist in a vacuum – so Ukraine should designate liaisons in related institutions. The Ministry of Economy (which handles intellectual property policy nationally and oversees the patent office) should have a contact point for defense IP to coordinate on patent filings and economic incentives. The Ministry of Strategic Industries or State Defense Industries Concern (if such exists) should integrate IP management in how they deal with industry R&D. Possibly form a **joint working group** between MoD and the national IP Office (UANIPIO) to handle defense patent applications smoothly (maybe even expedite them given national security, or handle secrecy). This inter-ministerial cooperation echoes how NATO nations unify defense and IP offices in decision-making (for example, in the U.S., the DoD works with the USPTO on secrecy orders).
- **IP Board / Committee:** As recommended, set up an **IP Board** with members from MoD (IP Directorate, procurement, R&D units), Ministry of Justice (for legal aspects), Ministry of Economy/IP office, and Security Service (for classification oversight). This Board would oversee policy updates, major contentious cases, and ensure all organizational

stakeholders are aligned. Formally charter this committee by a MoD order or Cabinet instruction, meeting quarterly.

- **Integration with R&D Project Management:** Create an **R&D Program Management Office (PMO)** within the MoD or under the General Staff that looks holistically at R&D projects (this could be part of an existing Armaments development unit). This PMO should include IP management as one of its functions. For instance, if the PMO supervises a portfolio of projects (drones, electronic warfare, etc.), it should coordinate with the IP Directorate to track IP issues in each project. The recommendation stems from EU practice where program officers monitor exploitation, and from NATO where ACT monitors progress of defense innovations across projects.
- **Human Resources and Culture:** Update job descriptions and performance criteria for project managers and researchers in the military to include IP responsibilities (like "must ensure any innovation is reported to IP Directorate" or "evaluate IP potential of project deliverables"). Possibly assign "IP Officers" at major military research units or commands – analogous to how some NATO commands have an innovation or technology officer. These officers act as the link between the field and the MoD IP Directorate, ensuring organization-wide coverage.

In summary, the legal changes ensure that Ukraine's laws underpin the new IP regime (so it's not just policy but enforceable rules), and the organizational changes ensure there are dedicated people and structures to carry it out. The creation of an MoD IP Office is already a huge step; building on it with coordinating bodies and embedding IP in project management will complete the picture. A final note: while making these adjustments, it's beneficial to document everything (e.g., a Defense IP Handbook capturing all new laws, policies, org charts and workflows) – this could even be published for transparency to international partners, showing Ukraine's seriousness in aligning with best practices.

10. MONITORING, RISKS & MITIGATION

Implementing a new governance model requires careful monitoring of progress and proactive risk management. This section proposes key performance indicators (KPIs) to track, identifies major risks across categories, and suggests mitigation measures for each.

Key Performance Indicators:

- **Percentage of R&D projects with IP plans:** Track what portion of defense R&D initiatives (including those with external partners) have an IP management plan or clauses from the outset. Goal: 100% of new projects by end of next year have IP terms documented.
- **IP Assets Registered:** Number of defense-related IP assets formally registered in the MoD's IP registry – including patents filed, trade secrets documented, or copyrighted software recorded. A rising count indicates the system is capturing innovations. (For example, if in 2023 it was near zero, target maybe 50+ by 2024, 200+ by 2025, noting that even classified ones should be counted internally.)
- **Inventor Compensation Paid:** How many inventors (servicemembers) have received rewards under the new law. This gauges whether the incentive mechanism is functioning. Aim to process compensation cases within a set time after invention disclosure.
- **Licenses Issued to Industry:** The count of licensing agreements from MoD to companies for production. This KPI speaks to bridging the R&D-procurement gap.

Target a steady increase – e.g., at least a handful in the first year, growing as more inventions come in.

- **Disputes Resolved:** Number of IP-related disputes (e.g., an inventor contesting ownership, or a company disputing a clause) and the resolution time. Ideally, disputes are few and resolved amicably/quickly. If disputes spike or drag on, it flags issues in contract clarity or policy acceptance.
- **International Cooperation Cases:** How many tech transfer agreements or joint projects with allies have been executed that include IP arrangements. This will show improved trust – e.g., an ally willing to co-develop a tech with Ukraine because IP terms are sorted.
- **Compliance Audits:** Results of any audits (the MoD launched an IP audit under its Anti-Corruption Programme). If audits show reduction in "leakage" (like fewer cases of private patenting of MoD-funded inventions), that's a positive sign.

These KPIs should be reported to the IP Coordination Board and possibly up to defense leadership regularly to ensure accountability.

Risks and Mitigations:

- **Legal Risks:** One risk is delays or setbacks in passing the necessary laws (political or bureaucratic hurdles). **Mitigation:** Engage Parliament committees early and use the broad support already shown (first reading passed with majority) to ensure final approval. Also, prepare contingency: if laws delay, enforce via internal MoD orders as an interim measure. Another legal risk is conflicts with existing laws (for example, a contradiction between civilian IP law and new defense IP rules). **Mitigation:** Have legal experts do a thorough review and if needed, include amendments to any conflicting statutes in the legislative package. Also consider an interim regulation by Cabinet if Parliament is slow, to give MoD authority to act (some countries do that under national security needs).
- **Operational Risks:** This includes the MoD's capacity to implement – e.g., too few skilled staff, or units ignoring the new procedures. **Mitigation:** Ramp up training and possibly bring in external advisors (NATO/EU mentors) to work with the IP Directorate in the initial year. As a mitigation, tie compliance to budget: e.g., MoD could stipulate no release of R&D funds unless the IP Directorate signs off that IP terms are in place (basically using budget control to enforce). Another operational risk is IT systems – the IP registry or portal might face technical issues. **Mitigation:** Use existing systems (they are building on the Armed Forces innovation portal which is smart to reduce development risk) and have backup manual processes if IT is delayed (like at least keep Excel logs of inventions until a database is ready).
- **Cultural Resistance:** This is arguably the highest risk. Soldiers or engineers used to the old way may be skeptical or fear that sharing their idea means losing personal benefit or getting in trouble (especially if it involves classified info). Likewise, some officials who had personal gain in the old chaos might quietly resist. **Mitigation:** Strong leadership messaging from the top is needed – e.g., the Defense Minister and top generals endorsing this initiative as critical for war effort and Euro-Atlantic integration. Highlight success stories of inventors being rewarded to set positive examples. Also implement a safe channel for reporting inventions to alleviate fear (the single window helps by allowing anyone to submit, even bypassing chain of command if necessary). Over time, as compensation payouts and recognition events (like awards for best military invention of the year) happen, the culture should shift towards seeing IP as a positive-sum game. To tackle any entrenched interests misappropriating IP, use the anti-corruption angle: conduct periodic audits and if someone is found patenting illicitly,

enforce consequences (this requires coordination with law enforcement potentially, but making a public example of a violator can deter others).

- **Secrecy vs Transparency Risk:** There's a risk of leaning too much one way: either over-classifying (which could hide innovations from those who could develop them) or under-protecting (which could leak sensitive info). **Mitigation:** Institute a review panel for classification decisions on inventions – include intelligence and technical experts to weigh the pros/cons. The 4-month rule in the draft law forces a decision; ensure that panel is equipped to make quality decisions within that time. If in doubt, a mitigation could be using provisional patent applications filed under secrecy (some legal systems allow secret patents). Also, do regular sweeps to ensure nothing that should be patented is sitting unpatented beyond the decision deadline – the IP Directorate can flag and escalate any indecision to the Deputy Minister so it gets resolved.
- **Overlap and Coordination Risks:** Introducing an IP regime may overlap with other initiatives (like general innovation programs, or defense industry reforms). There's risk of duplication or working at cross-purposes. **Mitigation:** The IP Coordination Board (or similar interagency mechanism) is key here – it should interface with any defence industry reform task forces, the digital transformation team (if a "single window" for broader innovation exists, clarify roles), etc. Also clearly delineate tasks: e.g., if Ukroboronprom (state defense industry) has its own R&D, ensure they follow MoD IP rules when state-funded.
- **Compliance and Enforcement:** A risk is that even with rules, people might circumvent them (e.g., not report an invention and secretly sell it, or a company not honoring license terms). **Mitigation:** Create an enforcement capacity – perhaps the MoD IP Directorate can coordinate with the Military Law Enforcement or inspectorate to investigate such cases. Also leverage the legal changes: once it's law that service IP belongs to state, any unauthorized patent filing can be challenged legally (the MoD already did challenge one private patent for uniforms). Set up a watch on patent databases to spot if someone tries to patent something related to military tech outside the official channel, so MoD can act (this is a modern need – EU countries use their patent offices to flag military-related filings for security review, Ukraine can do similarly in cooperation with UANIPIO).

For each risk above, a mitigation owner should be assigned (e.g., IP Directorate for most, but also General Staff for cultural enforcement, etc.) and contingency plans ready.

In sum, while the reform's benefits are significant, success hinges on diligent monitoring (with KPIs shining light on progress) and agile mitigation of risks. By anticipating these issues now – legal delays, operational bottlenecks, cultural pushback, security mishaps – Ukraine's MoD and its partners can navigate around them, ensuring the new IP and R&D governance not only exists on paper but truly takes root in practice.

11. COMMUNICATION & CULTURE CHANGE

Technical changes alone won't suffice unless accompanied by a shift in awareness and behavior within the defense community. Building an IP-conscious culture in the Ukrainian Armed Forces and MoD is paramount. This section covers the communication strategies and educational measures to facilitate that culture change.

Awareness & Education ("Cheat-Sheets"): One of the simplest yet effective tools is to create concise reference materials for personnel:

- **Program Manager's IP Cheat-Sheet:** A one-page guide for any officer or official managing an R&D project, listing the key things to remember: e.g., "Have you involved the IP Directorate at project kickoff? Did you include the IP clause in the contract? Are inventors documenting their contributions?" Using a checklist style (NATO loves checklists for compliance), this can greatly help new PMs incorporate IP steps as routine.
- **Inventor's Guide Card:** A small flyer or digital infographic for soldiers and engineers titled "I invented something – what next?" which outlines the steps: (1) Don't disclose publicly yet; (2) Submit to Single Window; (3) Your idea will be evaluated – if it's new and useful, MoD will protect it; (4) You will be credited and may receive a reward; (5) Keep security in mind – mark info as secret if needed and share securely. This demystifies the process and emphasizes that using the system will benefit them. Possibly include a hotline or email for questions.
- **Commanders' Brief:** A short memo or presentation for unit commanders to explain why this matters. Commanders need to encourage their subordinates to participate. The brief can use examples: "If your unit builds a better drone and we patent it, MoD can mass produce it and you get credit – if you hide it or let an outsider patent it, our forces lose out." Tie it to patriotism and mission success, values military folks resonate with.

Training Modules: Develop short training modules integrated into existing military education:

- At the Defense University or officer courses, include a module on "Innovation and IP management in the Armed Forces". Not heavy law detail, but principles and case studies (maybe from the war, like how a field invention saved lives and how IP helped scale it).
- For procurement specialists and lawyers, do targeted workshops on drafting and negotiating IP terms. Possibly invite experts from NATO countries or EU lawyers who have done defense contracts to share experiences (partners would likely volunteer given interest in Ukraine's reform).
- E-learning: If feasible, put a short course on the MoD's intranet or e-learning platform covering the basics of the new IP procedures. This can ensure even those in field can access when convenient.

Consultation and Support Channels: Establish channels for advice and questions:

- **IP Help Desk:** Within the MoD IP Directorate, create a help desk function (even if just one officer assigned) to answer queries from units or partners. This mimics the European IPR Helpdesk but focused on defense context. It could be an email or phone line advertised on MoD internal communications.
- **Regular Q&A Sessions:** Hold periodic "IP hour" webinars or in-person sessions where anyone can bring questions or propose ideas. This also provides feedback on what issues people are facing on the ground trying to implement the policy.
- **Mentorship:** Pair inventors or project leads with a mentor from the IP Directorate for critical projects, ensuring they feel supported in navigating patent filing or licensing. NATO's collaborative spirit can be invoked – it's all about teamwork to get innovation forward.

Recognition and Incentives (Cultural Reinforcement): Use recognition as a communication tool:

- Publicly celebrate successes – e.g., when the first patent under the new law is granted to MoD, issue a press release or MoD news story naming the inventor (if not classified) and how they were rewarded. Similarly, highlight any allied cooperation where

Ukraine's good IP practice made a deal possible. This positive reinforcement builds pride and buy-in.

- Create an award (yearly "Defense Innovator Award") given by the Minister to the top inventor or project team that exemplified innovation and good IP management. This mirrors some NATO nations' practices (e.g., US DoD has annual innovation awards). It sends the message that contributing ideas and going through the proper channels is commendable and career-enhancing, not extra paperwork hassle.

External Communication: While primarily internal, it's also important to communicate to external stakeholders – foreign partners, industry, the public – that Ukraine is making these changes. Given this paper is aimed at international stakeholders as well, the narrative should be shared through:

- Briefings to donor coordination groups (like the Ukraine Defense Contact Group) on IP reform progress, emphasizing that Ukraine will protect shared tech (to reassure them, as mentioned in Section 1 about trust).
- Engaging local defense industry via forums to explain the new IP regime and how it will actually help them (ensuring companies understand they won't just lose IP; rather they get clarity and a potential market via MoD licensing).
- Perhaps sharing simplified updates on social media or MoD's website (non-sensitive aspects) to show the public and expert community that Ukraine is innovating not just on the battlefield but in governance.

Summary: Changing culture is a gradual process. The key is consistent messaging that IP governance is not a bureaucratic imposition but a combat multiplier and a pathway to NATO/EU. Over time, as people see that using the system yields results (like their invention gets fielded or they get a bonus), attitudes will shift from skepticism to engagement. NATO's experience suggests that culture follows policy when leadership consistently prioritizes it – e.g., NATO had to instill a culture of multinational cooperation and did so by continuously messaging "we are stronger together". Similarly, Ukraine should foster a culture of "our innovations are valuable – let's protect and share them properly so they serve Ukraine and our allies." Communication and education are the tools to embed this mantra into daily practice.

12. CONCLUSIONS & NEXT STEPS

Ukraine's endeavour to reform IP and R&D governance in its defense sector comes at a critical juncture. The ongoing war has underscored the ingenuity of Ukraine's people and the strategic importance of rapidly harnessing that ingenuity for defense. At the same time, Ukraine's path toward EU membership and deeper NATO integration demands that it modernize and standardize its practices. This paper has analyzed the European Union's market-driven, innovation-centric model and NATO's security-focused, interoperability-centric model, finding both to offer valuable lessons.

Key Takeaways: Ukraine should pursue a **hybrid governance approach** that combines EU and NATO strengths. From the EU side, embrace transparency, competitive funding, and industry incentives – ensure that inventors and companies see opportunity in working with the MoD because they can benefit from IP rights and commercialization. From the NATO side, embed security considerations and collective access – ensure that any technology developed for defense can be shared appropriately within the Armed Forces and with allies for maximum effect. The hybrid model means Ukraine will, for example, patent or license technology (EU style) but might restrict its dissemination to allies only if sensitive (NATO style); it will allow industry to own or co-own IP in some cases to spur innovation (EU), but will always secure

government-use rights (NATO). This balanced approach will transform what was once a gap into a strategic asset: a robust, modern innovation ecosystem for defense.

Concrete Next Steps: To realize this vision, several immediate steps stand out:

1. **Formalize the Framework:** Finalize and issue the MoD IP Instruction (or Policy) as soon as possible, codifying the new rules so that everyone in the defense establishment has clear guidance to follow.
2. **Empower the IP Directorate:** Provide the new MoD IP Directorate with the authority, staff, and resources it needs. This includes completing its elevation in organizational status by making it a direct report to senior leadership, and ensuring it has a direct line into every R&D program (possibly via assigned IP liaison officers in major projects). Early budget support for hiring patent lawyers or contracting patent services will pay off in number of protected innovations.
3. **Launch the Registry and Portal:** Proceed with launching the IP registry system and the Single Window portal for submissions in Q1 2025. These tools will be the workhorses of the new system, capturing IP at source. Ensure they are user-friendly and secure (especially for classified submissions).
4. **Pilot and Scale Licensing:** Identify a couple of pilot projects where the new IP model can be demonstrated – for instance, pick one internally developed tech to patent and one to keep classified but licensed, and execute those processes. Use the outcomes to refine templates and build confidence. Then expand, with more projects in 6 months, showing an increasing trend of MoD-managed IP deals.
5. **Engage Allies and Donors:** Communicate Ukraine's IP governance improvements to international partners proactively. For example, propose an info session to NATO's Partnership Support groups or an EU defense advisory body to show what Ukraine is doing. This could unlock technical assistance (like training from EDA's IP experts, or exchange with NATO countries' patent offices) and assure allies that Ukraine is ready for deeper collaboration. It also sets the stage for Ukraine to possibly join programs like EDF as an associate in the future, since respect for IP is a prerequisite.
6. **Monitor and Adjust:** Establish a review at the one-year mark (late 2025) to evaluate the implementation against the KPIs and milestones set. In that review, include external observers – perhaps an EU representative or NATO advisor – to give feedback. Be prepared to issue an updated directive or action plan based on the findings, addressing any shortcomings (for example, if uptake by inventors is low, maybe the compensation scheme needs boosting; if industry is hesitant, maybe standard contract terms need tweaking).

Final Thought: By instituting a strong IP and R&D governance system, Ukraine is not only solving an internal problem but also sending a message internationally: that it is a country that values innovation, respects the rule of law in intellectual property, and is ready to be a reliable partner in high-tech development. This will encourage more foreign defense companies to collaborate, knowing their IP will be respected in Ukraine, and conversely encourage Ukrainian innovations to be shared with allies, knowing there is a clear path to mutual benefit. In essence, Ukraine will transform its defense innovation culture from one of ad-hoc heroics to one of systematic excellence. The journey will require sustained leadership attention and adaptability, but with the plan outlined in this report, Ukraine has a clear roadmap to achieve a modern, NATO-standard and EU-compatible IP governance model within the coming two years.

Ukraine's forces have shown the world their ingenuity on the battlefield; now it's time to cement that ingenuity through policies and institutions, so that every bright idea can be captured, protected, and turned into a force multiplier for the country's defense and security. The recommendations and plan presented here aim to do just that – ensuring that intellectual

property becomes a cornerstone of Ukraine's defence innovation and a bridge to greater cooperation with its European and NATO partners.

ANNEX A

COMPARISON OF EU VS NATO IP AND R&D GOVERNANCE.

Aspect	EU Model (e.g. EC/EDF, Horizon, EDA, OCCAR)	NATO Model (e.g. ACT, STO, Agencies)
Governance Structure	Centralized program management by EC/EDA; formal regulations and calls. OCCAR manages joint projects on behalf of member states.	Alliance-wide coordination; strategic commands (ACT) or agencies lead efforts by consensus; nations volunteer projects.
Funding Mechanisms	Grants and co-funding (EDF, Horizon) – EU budget subsidizes R&D. Also innovation prizes and PCP/PPI procurements to spur industry.	Primarily national funding coordinated through NATO STO "programme of work". Some common funding for NATO R&D (limited). New ventures like DIANA accelerator and Innovation Fund pool allied funds.
Contract Types	Grant agreements (multilateral consortium contracts) with obligations for results exploitation and dissemination. Public procurement for development via PCP/PPI where supplier keeps IP.	Project agreements or MOUs between governments; NATO agency contracts for capabilities. If NATO funds a contract, standard terms ensure NATO usage rights or ownership. Emphasis on security clauses and export control.
IP Ownership & Rights	Participants own foreground IP; EU does not take ownership of results. Joint ownership applies if results are generated together (co-owners can use freely for R&D, and license externally with consent). Background IP remains with original owners, but must be made available to the project.	NATO (as an organization) asserts ownership or irrevocable usage rights when it sponsors development. In collaborative research (STO panels), each nation/author retains IP of contributions but grants rights to other Allies for defence use. Recent programs (DIANA) let companies keep IP entirely to encourage participation.
Data Rights & Security	Default towards open dissemination of results (public reports, conferences) except classified projects. Research data management plans often required; civilian-military dual-use results encouraged to transition to market. Security reviews in EDF to avoid unauthorized transfer (no non-EU control of IP).	Emphasis on classification: results are often NATO-restricted or national secret. Tech data sharing is internal to Allies/partners on a need-to-know basis. Publications through STO can be public or classified; much technical info stays in NATO databases. Data rights often include clauses for government-purpose use across all Allies.
Export Control	Subject to national export control laws; EDF projects avoid third-country IP dependencies to ease intra-EU collaboration. Export of defense R&D results (if sensitive) needs member state approvals; EU has common arms export guidelines but not a unified regime.	Strongly linked to member nation controls (e.g. US ITAR for US-origin tech). NATO must respect the strictest common denominator – certain technologies shared in NATO cannot be transferred to non-NATO without originator consent. NATO standardization efforts help identify what can be commonly shared; sensitive projects may exclude some nations or partners.
Dissemination & Use	Broad dissemination encouraged: publish results, share with all EU countries' industries to strengthen the European Defence Technological and Industrial Base. EDF requires exploitation plans for results. OCCAR and EDA projects may share results among participating nations' industries.	Controlled dissemination: results meant for improving interoperability and capabilities of members. Shared through NATO channels, standards (STANAGs) or classified exchanges. Focus on using R&D results in military exercises, doctrine, and equipment standards rather than commercializing them. Public communication is limited, highlighting only high-level outcomes due to security.

Dispute Resolution	Formal legal frameworks: disputes in EU grants can be taken to arbitration or national courts under the grant agreement law. Consortium agreements have internal escalation and then legal remedy. OCCAR has its own dispute arbitration mechanisms under its international agreement.	In NATO context, disputes are managed through negotiation at steering committees or via arbitration clauses in project agreements. Contractors dealing with NATO agencies agree to international arbitration (since NATO entities have immunity from national courts). Consensus politics often resolve issues informally; legal disputes are rare due to diplomatic management.
Strengths	*Strengths:* Fosters innovation and industry growth; clear IP rules give companies confidence to invest. Multi-country projects build scale. Transparent processes and civilian oversight. Market-driven exploitation yields dual-use benefits (spin-offs).	*Strengths:* Ensures collective access to critical tech for all allies; security-first approach protects sensitive innovations. Unified standards (via STANAGs) and interoperability focus. Leverages pooled expertise (burden-sharing) – e.g. collaborative R&D yields 10-100x return in value for nations. Fast adoption by militaries due to direct involvement.
Weaknesses	*Weaknesses:* Process can be bureaucratic and slow (complex proposals, compliance). IP owned by firms means governments may not automatically get rights to use tech in defense without further contracts. Risk of fragmentation if national interests diverge; not all EU states participate equally. Security concerns if results are published (need balance).	*Weaknesses:* Limited budget for R&D – NATO relies on voluntary contributions, so funding is smaller and uneven. Heavy security classification can stifle wider innovation or commercial spin-off. Complex consensus needed among nations for projects. Potential legal ambiguities due to reliance on MoUs (not as clear-cut as EU law). Reluctance of industry if terms seem to limit profit (hence new initiatives like DIANA to attract them).