POLICY BRIEF

EU DEFENCE, REARMAMENT AND R&D ETHICS

May 2025

www.plusethics.com

CONTENTS

ETHICS ON THE FRONTLINE: RETHINKING EUROPEAN REARMAMENT IN THE AGE OF STRATEGIC AUTONOMY

1. INTRODUCTION: REARM EUROPE AND ITS ETHICAL STAKES

With the announcement of the ReArm Europe Plan[1] in early 2025, the European Union has placed defence and deterrence at the centre of its strategic future. Designed as a comprehensive response to rising geopolitical instability, the Plan introduces an unprecedented scale of investment into Europe's defence capabilities, mobilising hundreds of billions of euros[2]. But as the EU pivots towards military reindustrialisation, critical ethical questions arise: how can such a strategy align with the Union's foundational values of peace, democracy, and human dignity? Can a fast-moving defence agenda truly incorporate meaningful ethical oversight, especially in areas where military goals may conflict with civil liberties and fundamental rights?

At Plus Ethics, we see the ReArm Europe Plan as an opportunity to promote responsible innovation within defence R&D. We recognise the importance of strengthening Europe's strategic autonomy and technological resilience—particularly in an era of complex and unpredictable threats. These challenges increasingly stem not only from regional conflicts, but also from the assertive repositioning of major global actors such as the United States and Russia, whose military agendas and extraterritorial interests have, in different ways, placed pressure on Europe's sovereignty, decision-making autonomy, and security posture. In this context, the EU's pursuit of greater strategic independence is understandable. At the same time, we believe that ethical reflection must be embedded from the outset to ensure these efforts align with the Union's democratic values. Rather than positioning ethics as a constraint, we see it as a resource for guiding innovation in ways that are socially legitimate and legally robust.

[1] European Commission (2025, March 19). *Commission unveils the White Paper for European Defence and the ReArm Europe Plan/Readiness 2030*. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793
[2] European Commission (2025, March 4). *Press statement by President von der Leyen on the defence package*. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673

2. THE STRATEGIC SHIFT: FROM PEACEBUILDING TO DETERRENCE

2.1. THE REARM EUROPE PLAN: OBJECTIVES AND SCOPE

The ReArm Europe Plan represents a historic step in the EU's move towards a more assertive security posture. With a projected mobilisation of up to €800 billion, it introduces a range of measures to stimulate defence spending across Member States. These include the temporary relaxation of EU fiscal rules to allow increased national investment in military capabilities, as well as the creation of the Security Action for Europe (SAFE) financial instrument to provide up to €150 billion in loans for joint defence procurements. The Plan also highlights the need for deeper cooperation among Member States, stronger defence supply chains, and accelerated innovation in key technological areas such as AI & cyber warfare, critical Infrastructure protection, missile defence, and drones and counter-drone systems.

The Plan is framed as a necessary response to real and growing threats, and there is little doubt that Europe must be better prepared to defend its interests. Yet its symbolic and material weight signals a departure from the EU's longstanding self-image as a peace-building project rooted in diplomacy and multilateralism. By placing rearmament and industrial defence capabilities at the heart of its strategic posture, the Union risks shifting from normative power to military actor—normalising a defence-first narrative and relegating ethical and humanitarian concerns to secondary roles. This reconfiguration invites a broader reflection on the tools and safeguards required to ensure that, even as the EU becomes more assertive, its foundational values are not compromised. This transition is particularly evident in the growing role of EU funding instruments that support security and defence innovation.

2.2. THE ROLE OF THE EUROPEAN DEFENCE FUND (EDF) AND HORIZON EUROPE (HE) IN SECURITY R&D

The European Defence Fund (EDF) has already played a critical role in promoting cross-border cooperation in defence R&D. With a budget of nearly €7.3 billion for 2021-2027, the EDF supports joint research and development of defence products and technologies, particularly among SMEs and mid-caps[3]. In fact, the EDF is explicitly opening the door to non-traditional stakeholders—such as SMEs and research organisations previously involved in civil innovation—through dedicated calls like EDF-2025-LS-RA-SMERO, EDF-2025-LS-DA-SME, EDF-2025-LS-RA-SMERO-NT and EDF-2025-LS-DA-SME-NT[4]. These calls aim to foster

[3] European Commission (n.d.). European Defence Fund (EDF) – Official Webpage. Retrieved from: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

[4] European Commission (2025). *EDF 2025 Work Programme*. Retrieved from: https://defence-industry-space.ec.europa.eu/edf-work-programme-2025_en

greater inclusivity and diversification of the defence innovation ecosystem. In addition, bonus mechanisms are in place to increase funding rates for proposals that allocate a significant proportion of eligible costs to EU-based SMEs, further incentivising their participation.

This represents a strategic move to integrate a broader range of expertise and agile innovation capacities into defence R&D. Many of these actors, having worked in areas such as AI, cybersecurity, or situational awareness under civil funding frameworks, now find themselves eligible—and encouraged—to apply their capabilities to defence applications. This transition, however, raises new challenges in terms of ethical preparedness and domain-specific governance. It is crucial that these entrants are supported not only with financial incentives but also with guidance on the specific ethical, legal, and societal expectations that come with defence-oriented innovation.

Notably, several EDF calls in 2025 place a stronger emphasis on ethical, legal, and societal dimensions, reflecting a growing recognition of their relevance in defence innovation. Topics such as autonomous triage and evacuation (EDF-2025-RA-MCBRN-ATE), risk and robustness in autonomous vehicles (EDF-2025-LS-RA-SI-CYBER-3RAV-STEP), and privacy-preserving human-AI dialogue systems (EDF-2025-LS-RA-CHALLENGE-DIGIT-HAIDP-STEP and EDF-2025-LS-RA-CHALLENGE-DIGIT-HAIDO) raise complex questions related to autonomy, human oversight, data protection, and human dignity. Similarly, projects aiming to develop enhanced pilot environments (EDF-2025-DA-AIR-EPE) or next-generation soldier systems (EDF-2025-DA-PROTMOB-SS) have significant implications for human-machine interaction and operational ethics. These calls demonstrate an emerging shift in EDF priorities toward integrating ethical foresight directly into the technological development process. This evolution opens a crucial window of opportunity to embed responsible innovation principles at the earliest stages of defence R&D planning and execution.

Notably, several EDF calls in 2025 place a stronger emphasis on ethical, legal, and societal dimensions, reflecting a growing recognition of their relevance in defence innovation:

- EDF-2025-RA-MCBRN-ATE: *"Autonomous triage and evacuation"*, addressing ethical questions around medical decision-making by machines in crisis contexts and health data monitoring.
- EDF-2025-LS-RA-SI-CYBER-3RAV-STEP: *"Risk, robustness and resilience for autonomous vehicles in military operations"*, involving issues of accountability, human oversight, and operational safety.

- EDF-2025-LS-RA-CHALLENGE-DIGIT-HAIDP-STEP and EDF-2025-LS-RA-CHALLENGE-DIGIT-HAIDO: *"Privacy-preserving human-AI dialogue systems"*, which foreground concerns related to data protection, trust, and meaningful human control.
- EDF-2025-DA-PROTMOB-SS: *"Full-size demonstrators for next-generation soldier systems"*, raising questions around end-user acceptance, human enhancement and ethical deployment.
- EDF-2025-DA-AIR-EPE: *"Enhanced pilot environment"*, touching on cognitive load, autonomy, and responsibility in high-risk contexts.

These calls demonstrate an important shift in EDF priorities toward embedding ethical foresight within the technological development process. They offer a timely opportunity to align defence innovation with principles of responsible research and innovation (RRI), ensuring that technological advancement remains compatible with core European values.

In parallel, Horizon Europe—the EU's main research and innovation programme—has expanded its scope to include more security-driven calls, particularly under Cluster 3 (Civil Security for Society). While Horizon Europe projects remain rooted in civilian frameworks, the increasing emphasis on resilient infrastructure, disaster-resilient societies, cybersecurity, hybrid threats, and border management demonstrates a convergence with defence priorities.

This intersection creates both opportunities and risks. On one hand, it allows for shared innovation and the integration of ethical good practices. On the other, it requires vigilance to ensure that civilian research does not become a backdoor for unchecked militarisation. Ethical oversight in Horizon Europe—while more developed than in defence R&D—must not be diluted as these domains continue to converge. As more civil actors enter the defence domain and as funding mechanisms become increasingly streamlined, the question arises: what happens to ethics in this accelerated landscape?

3. FAST-TRACKING DEFENCE: WHAT HAPPENS TO ETHICS IN EMERGENCY MODE?

Periods of crisis are often marked by a collective suspension of procedural safeguards in favour of rapid, solution-oriented action. In such contexts, ethical scrutiny can appear to many as a secondary concern—less urgent than the technological or operational response itself. Defence, by its nature, tends to operate under similar urgency, often invoking the language of necessity and exception. However, history reminds us that decisions made under exceptional circumstances frequently leave long-lasting normative legacies.

The acceleration of defence R&D under EU funding risks introducing a structural form of ethical minimalism: calls for proposals may demand swift deliverables, ethical oversight may be reduced to basic compliance checklists, and developers may be pushed to prioritise performance over deliberation. This is not unique to the defence domain. During the COVID-19 pandemic, for example, several ethics review procedures were temporarily reduced to expedite biomedical research and technological innovation[5]. While not inherently problematic, these instances highlight a recurring tension between speed and scrutiny, and the importance of recalibrating ethical standards once urgency subsides. In the context of defence, however, this recalibration is rarely straightforward. Technologies such as autonomous drone swarms with lethal capabilities, AI-powered decision-support systems for threat prioritisation, autonomous surveillance platforms, or behavioural analytics tools pose complex questions about responsibility, legitimacy, and the limits of human oversight in defence contexts.

Traditional ethical theory offers several lenses through which to interpret these cutting-edge developments. A deontological perspective might emphasise the inviolability of people, while a consequentialist framework could accept some ethical trade-offs for the sake of greater collective security. Meanwhile, virtue ethics would ask not just what we do, but what kind of organisations we become when security is pursued without reflective restraint. From a governance standpoint, the precautionary principle—long applied in environmental and health regulation—should also be considered in defence innovation. It urges restraint in the face of uncertain or potentially irreversible risks, and insists on the burden of proof being placed on those advocating deployment. This principle is rarely invoked in military R&D but has growing relevance as dual-use and emerging technologies complicate the civil-military divide.

[5] Salamanca-Buentello, S., Katz, R., Silva, D. S., Upshur, R. E. G., & Smith, M. J. (2024). Research ethics review during the COVID-19 pandemic: An international study. *PLoS One. 2024 Apr 16;19(4)*:e0292512. https://doi.org/10.1371/journal.pone.0292512
Sheehy, A., Ralph James, J., & Horgan, M (2020). Implementing a National Approach to Research Ethics Review during a Pandemic – the Irish Experience. *HRB Open Res, 3:63*. https://doi.org/10.12688/hrbopenres.13146.2

The challenge, then, is not to resist urgency altogether, but to build infrastructures that preserve ethical reflection within it. Fast-tracked innovation should not preclude inclusive deliberation, especially when the societal implications are profound. Ethics, in this light, is not an impediment to efficiency but a mechanism for legitimacy and resilience—essential in securing not just borders, but the values those borders are meant to protect.

4. PRIVACY, DUAL-USE DILEMMAS AND TECHNOLOGICAL OVERSIGHT

Technologies developed under defence frameworks increasingly overlap with tools used in civil contexts. AI-driven surveillance networks, facial recognition systems deployed in real-time monitoring, autonomous aerial vehicles used for crowd control, and behavioural prediction algorithms designed for pre-emptive threat detection all illustrate this convergence. These tools can serve both military and civil administration purposes—but dual-use technologies also raise complex dilemmas: should systems originally developed for battlefield situational awareness be repurposed for border surveillance or urban policing? Can predictive models trained on military intelligence datasets be ethically adapted for use in public safety or migration management? And can civilian-facing applications truly uphold privacy and accountability standards if they are rooted in logics of control developed for conflict scenarios? These questions demand ethical scrutiny that moves beyond abstract principles to engage with the real-world challenges of operational deployment, data governance, and institutional accountability.

For example, testing AI-based technologies on soldiers or operational personnel raises concerns about informed consent, long-term effects, and potential coercion. Similarly, integrating end-user feedback—whether from military or civilian actors—must go beyond formal checklists to reflect genuine participatory mechanisms, as in the case of Virtual Reality or Augmented Reality training with soldiers. But to begin with, legal compliance should be seen as a foundational requirement. Adherence to the General Data Protection Regulation (GDPR)[6] is essential even in defence R&D contexts that handle sensitive data. The AI Act[7], now formally adopted, reinforces this obligation by establishing common rules for high-risk AI systems—including many used in defence-related contexts. However, it is crucial to note that the regulation explicitly excludes from its scope

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

[7] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

AI systems developed or used exclusively for military purposes (see article 2). This exemption underscores the need for defence-specific ethical standards beyond the scope of general EU digital regulation

In parallel, the EU has strengthened its position against the misuse of dual-use technologies by tightening export controls[8] and introducing clear restrictions in funding schemes. Publicly funded technologies must not be diverted toward applications that violate human rights, international law, or ethical norms. Yet, in practice, these boundaries can be ambiguous and difficult to enforce without proper oversight.

Plus Ethics' work in EU-funded civil security projects like STARLIGHT, SYNERGISE, UNCOVER or APPRAISE demonstrates that aligning innovation with ethical and legal safeguards is complex even outside the military domain. These projects showed that ethics-by-design, inclusive stakeholder engagement, and transparent governance structures are not optional—they are central to building institutional and public trust. In defence contexts, where information is more tightly controlled and scrutiny reduced, the risks of ethical neglect are even more pronounced. Plus Ethics' contributions in defence R&D projects, such as ECOBALLIFE, ARMETISS or VESTLIFE, exemplify that strengthening ethical governance is therefore not only a normative imperative but also a practical condition for legitimacy and sustainability.

5. THE ROLE OF ETHICS ADVISORY STRUCTURES IN DEFENCE-ORIENTED PROJECTS

The European Defence Fund (EDF) and other EU funding instruments have introduced several procedural requirements to embed ethics into the research and innovation process. These include the mandatory ethics self-assessment[9] at the proposal stage, an Ethics Summary Report (EthSR) for funded projects, and the inclusion of dedicated ethics deliverables within the project's work plan. In addition, for projects dealing with serious and complex ethics issues[10], the European Commission encourages the appointment of independent Ethics

[8] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02021R0821-20241108

[9] European Commission (2021). *How to complete your ethics self-assessment* (Version 2.0). Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf

[10] European Commission (2021). Identifying serious and complex ethics issues in EU-funded research. Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidelines-on-serious-and-complex-cases_he_en.pdf

Advisors or the establishment of Ethics Advisory Boards (EABs)[11]. According to official guidance, these structures are intended to provide ongoing support and critical oversight, helping consortia to manage ethical risks proactively and uphold high standards of research integrity throughout the project lifecycle.

However, the operationalisation of these values remains inconsistent. Ethics sections in proposals are often treated as bureaucratic checkboxes rather than as integral reflections on the risks and societal implications of the proposed technologies. Ethics deliverables, when present, can vary in depth and relevance, and may not keep pace with evolving technical developments or emerging ethical dilemmas. And while the Ethics Summary Report offers a valuable initial framework, its impact depends on how seriously the project consortium engages with it and on the follow-up provided by project officers and external reviewers.

Defence R&D raises unique and pressing ethical concerns that go beyond the scope of standard regulatory compliance. These include, for example, the design of systems for autonomous targeting, the use of predictive models for threat detection, or the deployment of behavioural analytics in high-stakes operational settings. These applications demand sustained ethical attention, not only for legal reasons, but because they shape norms around legitimacy, accountability, and proportionality in future conflicts.

At Plus Ethics, we advocate for the inclusion of ethical and legal expertise in project consortia, for the establishment of independent ethics advisory boards with cross-disciplinary expertise and meaningful oversight roles in defence-oriented projects. Such boards should be embedded from the design phase and remain active throughout project execution. Our work has shown that early ethical impact assessments—when combined with regular risk reviews, adaptive foresight tools, and participatory engagement with stakeholders—create more resilient innovation pathways. These tools can add value without impeding innovation. In fact, these tools improve project legitimacy, reduce reputational risks, and help anticipate potential misuses of emerging technologies.

For ethics structures to be effective in the defence context, they must be dynamic and responsive. Static ethics templates are rarely sufficient for technologies that evolve quickly or may be used in politically sensitive operations. Instead, defence research needs flexible, scenario-based ethical governance that incorporates real-time evaluation, meaningful end-user feedback, and transparency

[11] European Commission (2023). *Ethics Advisors and Ethics Advisory Boards: Roles and Function in EU-funded Projects* (Version 2.0). Retrieved from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/roles-and-functions-of-ethics-advisory-ethics-advisory-boards-in-ec-funded-projects_he_en.pdf

protocols—not just to meet funding requirements, but to preserve public trust in European security innovation.

6. TOWARDS A RESPONSIBLE REARMAMENT: RECOMMENDATIONS FOR ETHICAL INTEGRATION

As the EU commits to expanding its strategic autonomy through defence innovation, it must also address the complex ethical, legal, privacy, and societal challenges that accompany this shift. The nature of defence R&D introduces high levels of opacity, political sensitivity, and technological risk, particularly in domains like autonomous systems, surveillance infrastructure, behavioural modelling, and data-intensive operations. These domains not only challenge existing legal frameworks, but also raise profound questions about democratic control, accountability, and social acceptability.

Public concern around military technologies—especially when developed with public funds—can erode trust if ethical safeguards are perceived as insufficient or superficial. Furthermore, many non-traditional actors entering defence projects (e.g., SMEs or civil research organisations) lack the experience or internal capacity to anticipate and mitigate these ethical risks effectively. In this context, ethics must not be an auxiliary consideration—it must be a core feature of project design, execution, and evaluation.

Based on our work in civil security and ethics-by-design, we recommend the following actions to ensure ethical alignment in the implementation of the ReArm Europe Plan and related funding programmes:

- *Strengthen mandatory ethics components in all defence-related calls, ensuring that self-assessments and Ethics Summary Reports are accompanied by comprehensive risk mitigation plans.*
- *Establish independent Ethics Advisory Boards in all projects dealing with sensitive technologies or fundamental rights implications, with cross-disciplinary and international expertise.*
- *Ensure proportional budget allocation for ethics work packages, enabling continuous assessment and adaptive governance throughout the lifecycle of the project.*
- *Apply legal principles to the fullest extent possible, even in cases where legal exemptions for military use exist—aligning with the spirit, not just the letter, of the law.*
- *Implement dual-use foresight tools and scenario-based ethical impact assessments, especially when technologies are likely to have civilian applications or societal spillovers.*

- *Facilitate meaningful stakeholder engagement, including with civil society, human rights experts, and potential end-users (military and civilian alike), to build legitimacy.*
- *Require dedicated training modules for project partners—particularly within industrial consortia unfamiliar with ethics-by-design approaches—on ethical, privacy, legal, and social responsibility in high-risk innovation.*
- *Create mechanisms for public communication and transparency, including simplified ethics reports or dashboards accessible to non-specialist audiences.*

Only through a systematic, well-funded, and independent ethics infrastructure can the EU ensure that its investments in security and defence innovation do not compromise its values. Responsible rearmament is not a contradiction—it is a necessity. It is what distinguishes the European model of strategic autonomy from others based on opacity, coercion, or militarisation without accountability. Ethics, in this regard, is not an external constraint—it is what makes the entire endeavour sustainable and legitimate.

7. CONCLUSION: RE-ARMING WITHOUT DISARMING OUR VALUES

Europe's renewed defence ambitions are not without justification. The continent faces a turbulent geopolitical environment marked by armed conflict, cyberthreats, and diminishing reliability of traditional allies. These conditions demand coordinated and robust responses—but they must not lead to the erosion of the EU's normative foundations.

This is not a call for idealism in the face of insecurity. Rather, it is a pragmatic recognition that security built on secrecy, opacity, and unchecked technological escalation is fragile. Democracies cannot afford to win the battle for control only to lose the war for legitimacy. A responsible rearmament is one that integrates ethical foresight, safeguards fundamental rights, and fosters accountability from the ground up.

At Plus Ethics, we do not shy away from the complexity of this moment. We understand that defence innovation will play a role in Europe's future, and we recognise the urgency with which such innovation must advance. We also insist that ethical excellence must accompany technical excellence. Our experience in civil security projects positions us to support defence initiatives by ensuring they remain anchored in the values the EU claims to defend. Rearming Europe should not mean abandoning the very principles that distinguish it. Strategic autonomy must be built on ethical autonomy—and that begins with ensuring every innovation, every investment, and every deployment is guided by democratic responsibility and foresight.

Plus ethics

This publication and more information on Plus Ethics are available on our website.

www.plusethics.com