BREAKING FRAGMENTATION:

Advancing Secure Cross-Border Digital Interoperability in European Defence

DIGITALEUROPE

Preface

Disclaimer
This study was developed in the context of DIGITALEUROPE's Defence Working Group, which brings together a broad cross-section of Europe's defence, digital and dual-use industry. The analysis reflects insights from companies engaged in multinational defence programmes and in deploying digital technologies across the European defence ecosystem. The views expressed in this study are those of DIGITALEUROPE and do not necessarily reflect the positions of its individual member organisations or contributors.

Europe's defence ambition will not be realised by strategy alone. It will depend on whether Europe's defence ecosystem can work across borders with greater speed, trust and security. As digital technologies increasingly underpin military capabilities and the protection of critical infrastructure, the ability to deploy secure digital systems across national boundaries has become a decisive enabler of effective defence cooperation.

Yet the very digital infrastructures that should support such cooperation often expose a deeper structural weakness: fragmentation. Similar security objectives are interpreted and implemented through different national accreditation procedures, certification requirements, cloud rules and technical security practices. This is no longer simply a regulatory issue. It is becoming a constraint on Europe's ability to deliver capabilities at the pace required by today's security environment.

Consider a simple but common scenario. Two companies from different Member States collaborate on a multinational defence programme using a shared digital platform. Even where that system has already been accredited in one country, it may still be required to undergo a separate certification process in another. These repeated procedures are not exceptional; they are systemic. They increase costs, delay deployment and slow the adoption of critical digital capabilities across European defence programmes.

At a time when recent and ongoing conflicts in Ukraine and the Middle East show that operational advantage increasingly depends on how quickly new technologies can be developed, validated and fielded, such delays carry strategic consequences. Artificial intelligence, cyber capabilities, secure connectivity, cloud infrastructures, robotics, satellites and data-driven systems are reshaping defence. As defence systems become more software-defined and interconnected, regulatory frameworks must evolve to enable faster cooperation and trusted cross-border deployment.

This study examines one important dimension of that challenge: the regulatory fragmentation affecting digital systems handling RESTRICTED-level sensitive information in multinational defence programmes. Drawing on industry experience, it identifies the practical barriers companies face and sets out pragmatic, sovereignty-respecting recommendations. These include stronger mutual recognition of national security controls, more interoperable and federated digital architectures and more predictable and efficient accreditation pathways for multinational programmes.

Reducing fragmentation affecting RESTRICTED-level sensitive information is therefore not merely a technical necessity. It is a precondition for Europe's defence readiness, technological resilience and capacity to act collectively.

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

Executive Summary

Europe cannot build defence readiness on fragmented digital foundations

Across multinational defence programmes, digital systems that are already accredited in one trusted environment can still face additional certification, hosting or security validation in another. That duplication delays capability deployment, raises costs, fragments collaboration and weakens Europe's ability to scale trusted digital and dual-use technologies at speed. At a time when defence systems are becoming more software-defined, data-driven and dependent on secure cross-border cooperation, this is no longer a technical inconvenience. It is a strategic constraint.

This DIGITALEUROPE study examines one of the clearest manifestations of that problem: the deployment of digital systems handling RESTRICTED-level sensitive information in multinational defence programmes. Within this space, fragmentation is especially visible in cloud hosting, accreditation, encryption, facility and personnel clearances, system certification and the exchange of engineering and operational data. The result is repeated compliance effort, avoidable delay and weaker interoperability across European defence cooperation.

DIGITALEUROPE identifies one immediate policy priority: Europe needs stronger mutual recognition of accredited systems, validated security controls and equivalent assurance mechanisms across trusted EU and NATO environments, where comparable levels of protection can be demonstrated, for multinational programmes handling RESTRICTED-level sensitive information.

That should be the immediate policy priority

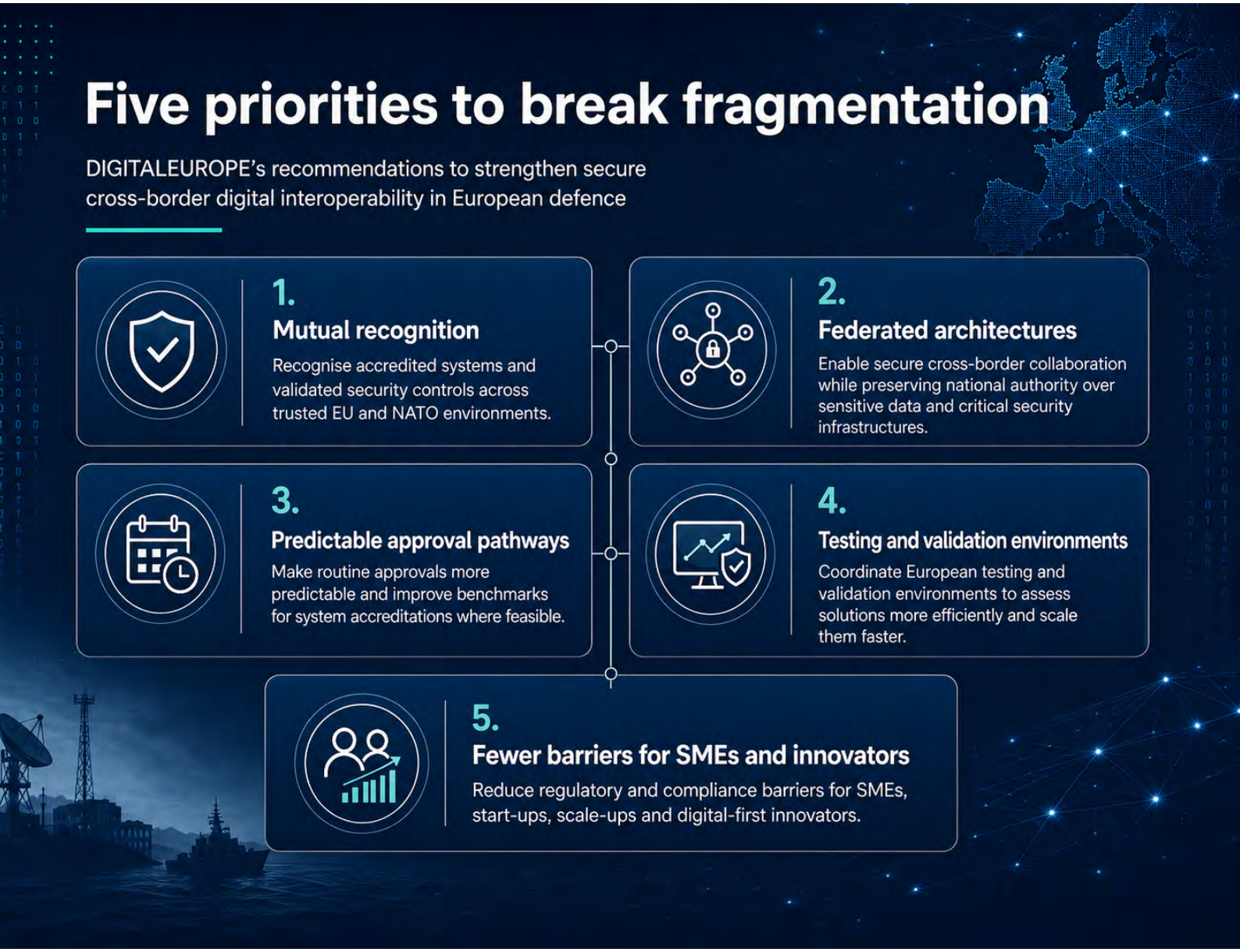
Europe does not need full harmonisation of national security systems. That is neither feasible nor necessary. What Europe needs is pragmatic regulatory convergence: practical steps that preserve national sovereignty while reducing duplication, improving predictability and enabling trusted systems to move across borders faster. DIGITALEUROPE's contribution is to bring the operational reality of industry into this debate. The study is grounded in the experience of companies deploying digital and dual-use technologies across multinational defence programmes and translates that experience into realistic policy action.

Europe should now act on five priorities:

- **Establish project-based mutual recognition of accredited systems:** Participating Member States should be able, on a voluntary and project-based basis, to recognise security controls, certifications and accreditation outcomes already validated in another trusted EU or NATO environment. This is the fastest and most practical way to cut duplication, reduce repeated certification and accelerate deployment while keeping justified national safeguards in place.

- **Build secure interoperability through federated and layered architectures:** Europe should support federated and layered digital architectures that allow nations to retain authority over sensitive data and national security infrastructures while enabling secure cross-border exchange, shared services and modular collaboration. This is the structural answer to fragmentation. It improves interoperability without forcing a single centralised model and creates a realistic foundation for cloud, AI and software-defined defence capabilities.

- **Introduce faster and more predictable accreditation pathways:** Europe cannot ask industry to innovate at commercial speed and then wait through open-ended approval cycles. Where feasible and without prejudice to national security assessments, routine personnel and facility approvals should move towards more predictable timelines, for example, **60–90 days** for routine cases; system accreditations, which can vary more significantly in complexity, should also benefit from clearer predictability, including indicative benchmarks where feasible and appropriate. For rapidly evolving digital and dual-use technologies, procurement and deployment timelines should aim to move closer to **4–6 months** where appropriate. Without measurable improvements in speed and predictability, Europe will continue to lose time where time matters most.
- **Strengthen coordinated testing and validation environments:** Europe should support a limited number of trusted, high-capacity testing and validation environments where digital solutions can be assessed once and then scaled more easily across national contexts. This is essential to reduce repeat validation, build confidence between authorities and help mature technologies move from pilot to operational use.



- **Reduce barriers for SMEs, start-ups and digital-first innovators:** Regulatory fragmentation falls hardest on the companies Europe most needs to bring in. SMEs, start-ups, scale-ups and academic actors often lead in AI, cyber, cloud and secure software, but they have far fewer resources to manage repeated certification, divergent hosting rules and overlapping compliance demands. A more predictable and interoperable framework would not only improve efficiency. It would broaden Europe's innovation base and strengthen the resilience of Europe's defence technological and industrial base.

Delivering these priorities will also require clearer national guidance, more strategic use of European and international standards and stronger pathways from simplification to operational deployment. Together, these measures would reduce uncertainty, improve interoperability and help trusted digital and dual-use technologies move more quickly from development to use across multinational European defence programmes.

The message is simple: Europe does not have to choose between national sovereignty and digital interoperability. It needs practical mechanisms that allow trusted systems to move across borders with more speed, more confidence and less duplication. That is how Europe will strengthen defence readiness and scale digital and dual-use innovation across multinational programmes. **DIGITALEUROPE is ready to help drive that agenda by bringing forward the operational experience of the companies building these technologies across Europe.**

Acknowledgements

This study was developed by DIGITALEUROPE in collaboration with members of its Defence Working Group, whose operational experience and expertise across the defence and digital ecosystem provided important input to the analysis.

DIGITALEUROPE also acknowledges the insights shared by participants in European collaborative initiatives, including the AEROSEC pilot project, as well as by experts engaged in European standardisation activities, including within CEN and CENELEC.

These perspectives informed the study's analysis of regulatory fragmentation and its practical recommendations for strengthening secure digital interoperability across European defence programmes.

Table of Contents

Chapter 1
Introduction

This DIGITALEUROPE study examines the regulatory divergences that affect the deployment of digital systems handling RESTRICTED-level sensitive information in multinational defence programmes. It focuses on an area where fragmentation is especially visible and operationally significant, particularly in relation to accreditation, certification, cloud deployment, secure data exchange and cross-border engineering workflows. For this study, the term "RESTRICTED" is used as a reference point for restricted-level sensitive information across national, EU and NATO frameworks. It supports the comparative analysis of cross-border challenges without implying legal equivalence between national classification systems or security frameworks. Further clarification is provided in Annex 1. Terminology Clarification.

Within this scope, the study considers how regulatory divergence affects not only cross-border cooperation between Member States, but also the participation of SMEs and digital-first companies in European defence programmes. It also recognises the supporting role that European standards can play in improving interoperability. By helping to align technical requirements across Member States and by linking European stakeholders to international standardisation processes through established cooperation mechanisms such as the Vienna Agreement (CEN–ISO) and the Frankfurt Agreement (CENELEC–IEC)[1], European standards can help reduce divergence in technical implementation while preserving national security prerogatives.

The analysis is intended to support practical policy action within the existing legal and institutional framework. In this context, it is relevant to current EU efforts to strengthen defence readiness and simplify cross-border cooperation, including the Defence Readiness Omnibus package[2] and the planned revisions of the Transfer Directive and the Defence Procurement Directive[3], which seek to simplify intra-EU transfers and modernise defence procurement.

More broadly, the study's findings align with the EU Defence Industry Transformation Roadmap: *Unleashing Disruptive Innovation for Defence Readiness,*[4] which emphasises rapid digital deployment, agile capability development and deeper integration of SMEs and new defence actors. It also reflects broader work on secure cloud- and edge-based collaboration for European defence programmes, including the functional requirements developed by the Aeronautics and Security Working Group of the European Alliance for Industrial Data, Edge and Cloud, which serves as the basis for the AEROSEC pilot programme.[5]

Reducing fragmentation affecting RESTRICTED-level sensitive information is therefore an important enabler of a more coherent, secure and interoperable European defence ecosystem.

1 CEN & CENELEC. (2026). *International cooperation.* https://www.cencenelec.eu/european-standardization/international-cooperation/

2 European Commission. (2025). *Defence Readiness Omnibus* (COM(2025) 820 final). https://defence-industry-space.ec.europa.eu/document/download/b2bcc9a0-5259-4543-9e1c-3af1dde8fbec_en?filename=Defence-Simplification-Omnibus.pdf

3 European Commission. (2025). *Proposal for a directive amending Directives 2009/43/EC and 2009/81/EC* (COM(2025) 823 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0823

4 European Commission. (2025). *EU Defence Industry Transformation Roadmap: Unleashing disruptive innovation for defence readiness* (COM(2025) 845 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0845

5 AEROSEC. (2025). *The project.* https://www.aerosec-securecloud-dep.eu/the-project/

1.1 Aim and objectives of the study

The **study aims** to support a more **coherent, secure** and **interoperable regulatory environment for cross-border defence programmes** and **industrial collaboration in Europe.** It focuses specifically on regulatory divergences affecting the deployment of digital systems that handle RESTRICTED-level sensitive information, where misalignment most directly hinders cloud deployment, secure data exchange, engineering workflows, and joint capability development.

In this context, the study pursues **four objectives:**

- identify regulatory inconsistencies;
- compare national and international frameworks;
- analyse contradictions and operational impacts;
- provide an industry-led policy analysis.

1.2 Methodology

This study is an **industry-led policy analysis** developed by DIGITALEUROPE in close collaboration with members of its Defence Working Group[6], representing a broad cross-section of the defence, dual-use and digital industries. It draws on operational input from companies involved in multinational defence programmes, including projects funded under the European Defence Fund (EDF), EDA frameworks, NATO initiatives and national procurement mechanisms.

Contributors provided concrete examples of regulatory and security challenges encountered when deploying digital systems across borders, with particular emphasis on RESTRICTED-level requirements. Unless otherwise indicated, the examples included in the study are illustrative and anonymised, used to identify recurring operational patterns rather than to provide an exhaustive legal or statistical assessment of all national frameworks.

The **methodology** combines several complementary sources: operational insights from industry, cross-industry comparative analysis, review of relevant EU and international policy frameworks, insights from the ongoing Digital Europe Programme-funded pilot project AEROSEC, integration of DIGITALEUROPE's prior strategic work and contributions to EU defence policy, consideration of relevant European standardisation frameworks and industry engagement with standardisation bodies including CEN and CENELEC, and expert consultation and review.

Taken together, these elements provide the analytical foundation of the study. They support an evidence-based assessment of practical bottlenecks and proportionate recommendations, while recognising that national security procedures remain context-specific and are not always fully publicly documented. Further details on the methodology and contributors to this study are provided in Annex 2: Methodology and contributors.

6 DIGITALEUROPE. (2026). *Defence and digital resilience.* https://www.digitaleurope.org/policies/defence/


TECHMARKER

Chapter 2 A fragmented regulatory landscape: nature of the problem and real-world impacts

European defence programmes currently operate within a **highly differentiated regulatory landscape,** in which each EU Member State maintains its own framework for **data classification, security accreditation** and **facility clearance.** While Member States share strategic objectives and participate in joint initiatives, national responsibility for classified information and security standards results in differing practices and interpretations. As a result, **European industry faces three recurrent and interlinked challenges:**

- **differing national frameworks** for data classification;
- **location requirements** that often limit deployments to a single Member State;
- **unaligned certification requirements,** which oblige companies to repeat similar processes.

This combination of national requirements can result in **overlapping compliance obligations,** requiring industry actors, vendors and service providers to address multiple, sometimes non-aligned requirements within a single multinational programme. In many cases, national procurement frameworks explicitly incorporate these domestic preferences, making **cross-border or alternative proposals difficult to consider.** These requirements are closely related in practice, but they do not all operate at the same level: some concern the **legal handling** of sensitive information, others the **technical accreditation** or certification of systems and others the **procedural conditions** for access, hosting or participation in a programme.

The consequences are structural inefficiencies that create **operational, technical** and **organisational** challenges: **higher compliance costs, longer deployment timelines** and **barriers to scaling secure digital solutions across Member States.** These inefficiencies can have a disproportionate impact on digital-first companies and SMEs, which often have more limited capacity to manage multi-country certification processes.

Beyond the administrative burden, regulatory divergence also **slows innovation** and **limits operational readiness.** This is particularly problematic for high-TRL digital and dual-use technologies, where capability cycles are short and where delays in testing, validation, certification or cross-border deployment can quickly reduce operational relevance. Defence projects that depend on digital interoperability, ranging from secure cloud environments to cross-border data exchange, can be delayed by procedural misalignment, duplicative vetting processes and incompatible national frameworks.

Against this background, this chapter examines **how regulatory divergence manifests in practice, why it persists** despite growing political attention and **how it affects the efficiency** and **scalability of multinational defence cooperation. Illustrative examples** further clarify how these dynamics materialise in operational contexts.

2.1 Divergent national rules

While many EU Member States participate in joint defence programmes, each retains **national responsibility for classified data and security requirements.** This results in **distinct national frameworks** governing how sensitive defence information is stored, processed and exchanged. Consequently, rules for data classification, access control, cryptography and cybersecurity may differ between countries. Companies participating in multinational programmes are therefore often required to comply with several national systems that were developed independently and may not fully interoperate.

At the EU level, this regulatory divergence also reflects historical and structural factors. Much of today's framework was shaped by the 2009 Transfers Directive (Directive 2009/43/EC)[7], which aimed to simplify intra-EU transfers of defence-related products. However, the directive was conceived in a strategic era very different from today's context. When it was drafted, Europe was experiencing declining defence budgets, limited cross-border industrial integration and far fewer digital-dependent capabilities. Its provisions, while appropriate at the time, did not **anticipate the emergence of cloud-based workflows, AI-enabled systems, secure remote collaboration or the need to synchronise nationally controlled data environments.**

These structural differences remain visible in the practical organisation of multinational defence programmes. Each project may require tailored arrangements to reconcile differing national requirements. In many cases, national regulations are embedded directly into procurement criteria, limiting the practical flexibility to deploy shared or cross-border digital solutions. As a consequence, **companies may be required to deploy and certify the same systems multiple times** to meet nationally defined requirements and remain competitive in procurement procedures. This increases costs, delays deployment timelines and reduces scalability without necessarily strengthening security outcomes. In some cases, Member States may require in-country hosting even when equivalent levels of protection exist elsewhere. Such requirements can fragment the market, restrict vendor options and increase both costs and timelines.

Finally, the limited scope of **mutual recognition of certifications** can lead to **redundant procedures, delays** and **administrative complexity.** Interviews with security and accreditation authorities across Europe indicate that the challenge is not limited to regulatory divergence itself, but also to the institutional capacity of national authorities to evaluate and accredit modern digital systems. In many cases, accreditation bodies face rapidly evolving technologies such as AI-enabled platforms, secure cloud environments and quantum-resistant cryptography, while existing accreditation procedures were designed for slower-moving hardware-based systems. As a result, even when equivalent security controls exist in another NATO or EU country, additional national validation processes are often required, contributing to delays in deploying digital capabilities.

These challenges become particularly pronounced when requirements diverge significantly or when new technical adaptations are needed to satisfy multiple national rules simultaneously. These examples reflect broader patterns observed across many multinational defence programmes. To illustrate these dynamics, this chapter presents practical examples, including cloud deployment location requirements and operational bottlenecks. Further examples are provided in Annex 3: Illustrative examples of national divergences (Table 1).

7 European Parliament & Council. (2009). *Directive 2009/43/EC simplifying terms and conditions of transfers of defence-related products within the Community.* Official Journal of the European Union, L 146, 1–36. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0043

Cloud deployment location requirements

In multinational defence programmes, cloud deployment is often among the most complex areas of regulatory divergence. Each Member State may apply its own requirements governing the deployment, use and operation of cloud environments that handle sensitive information. A significant source of cost and complexity arises where national rules require a full cloud deployment or data centre to be hosted entirely within national borders. While such requirements reflect national security and risk assessments, they can limit the ability to leverage certain cloud capabilities, including multi-location redundancy, scalability and distributed resilience models.

Establishing a new in-country cloud instance is not a simple technical adjustment. It may require additional facilities, dedicated hardware, trained personnel and a full national accreditation and certification process. These additional steps lengthen project timelines and increase costs, making it more difficult to scale solutions across multiple Member States. They also make it harder for innovative suppliers to move from prototype or pilot phase to wider operational deployment, particularly where digital solutions depend on rapid iteration, modular upgrades or shared validation environments.

Across the EU, there is currently no unified certification framework for cloud-based products addressing RESTRICTED-level data and systems. Previous discussions on EU-wide cloud certification approaches have highlighted the complexity of aligning security expectations across Member States, particularly in sensitive defence-related contexts. This situation may create additional compliance burdens, especially for SMEs and digital-first firms with more limited administrative capacity. The absence of a common approach may also slow innovation, as companies allocate significant resources to compliance activities in parallel jurisdictions.

These persistent divergences can complicate efforts to build a coherent, interoperable and secure digital defence ecosystem. They also highlight the need for pragmatic regulatory convergence, an objective pursued under the EU Defence Readiness Omnibus initiative.

Regulatory and operational bottlenecks

The EU Defence Omnibus package and the broader EU Defence Readiness 2030 agenda aim to reduce regulatory friction, including compliance costs and deployment delays and accelerate cross-border industrial scaling to meet Europe's growing defence needs. These initiatives envisage closer cooperation across Member States, including greater mutual recognition of pre-qualification processes and faster procurement pathways. However, the **current combination of national classification rules and layered vetting procedures can make it challenging to align with an EU-wide "fast lane" for defence readiness.** This creates practical challenges for the effective implementation of the Omnibus objectives.

The challenge is even more acute for digital capabilities, which often evolve faster than traditional defence planning and acquisition cycles. Where procurement or capability acceleration efforts seek to move quickly, fragmented accreditation, certification and security procedures can still delay deployment. In practice, this means that faster policy ambition is not always matched by faster operational implementation.

The differing cryptography requirements (see Table 1 in Annex 3) illustrate how these challenges can emerge in multi-country programmes. If such a programme were later expanded to include additional Member States, their specific national security requirements may require further technical adjustments or investment before full participation becomes possible.

In practice, incorporating a new Member State into a multi-country programme may require the participating countries to agree on a common approach to encrypting classified communications. Only then could the vendor assess whether the existing system can support this shared set of requirements. Because each new project involves a different combination of Member States, this coordination effort often needs to be repeated, creating recurring barriers to cross-border collaboration.

2.2 Why fragmentation matters now: consequences for multinational defence cooperation

The urgency of regulatory fragmentation becomes clear in the operational realities of multinational defence programmes. For joint initiatives, including those funded under the European Defence Fund (EDF), the consequences of legal, procedural and accreditation-related divergence are increasingly evident. Delays may arise between contract signature and programme launch, particularly during phases such as integration testing, certification and export approvals. These delays can increase project costs and affect delivery timelines, including for initiatives supporting EU Defence Readiness 2030 or national capability acceleration plans.

National security and accreditation authorities across Europe increasingly recognise that the growing role of software-defined and digitally enabled defence capabilities is placing pressure on existing accreditation frameworks. Many current procedures were originally designed for hardware-centric systems and longer development cycles. As defence technologies evolve towards cloud-enabled architectures, artificial intelligence applications and complex software platforms, authorities are increasingly required to assess systems that change more rapidly than traditional certification processes were designed to handle. As a result, even when digital systems have already undergone extensive security evaluation in another trusted environment, additional national accreditation procedures are often still required before deployment. While these procedures reflect legitimate national security responsibilities, they can also delay the operational deployment of modern digital capabilities across multinational defence programmes.

Given the rapid pace of technological change in modern defence systems, multinational programmes must be able to adopt new solutions and collaborate across Member States without unnecessary barriers. In practice, however, regulatory obstacles and the limited use of existing interoperability mechanisms often lead to bespoke security arrangements for each project. These ad hoc frameworks typically apply only for the duration of a specific programme, meaning that each new initiative recreates similar governance structures instead of building on existing mechanisms and experience.

In several Member States, procurement authorities increasingly seek to adopt advanced digital technologies from commercial suppliers, yet security accreditation procedures often remain significantly slower than procurement timelines. This mismatch between acquisition speed and accreditation capacity can create additional delays in operational deployment, even where technologies have already been validated in other trusted environments. This problem is especially visible in areas such as AI-enabled systems, cyber tools, secure connectivity, cloud-based services, software platforms and other digitally enabled capabilities, where innovation cycles are often measured in months rather than years.

If Europe wants to benefit from challenge-driven innovation and rapidly field-deployable solutions, it must reduce the procedural friction that prevents such technologies from moving efficiently from development to operational use across borders. Without faster and more predictable approval pathways, regulatory fragmentation will continue to delay deployment. It will also deter innovative suppliers, including SMEs and digital-first companies, from participating, particularly when they lack the resources to navigate complex, evolving compliance requirements across multiple jurisdictions.

Cross-border collaboration

Collaboration between teams located in different countries relies on shared digital tools, such as engineering platforms, secure messaging, video conferencing systems and cloud environments. However, national regulations or internal company security rules may restrict the use of certain tools, particularly when they are hosted abroad or are not aligned with national security requirements. As a result, partners often operate through separate, non-interoperable systems. This can complicate workflows, reduce coordination efficiency and make technical alignment more resource-intensive. See Annex 4: Deep dive on unified metadata and Product Lifecycle Management (PLM).

Intra-company compliance

Large industrial groups operating across multiple countries must adapt their internal processes to comply with each country's regulatory requirements. Even when an entity is already certified in one country, it may be subject to additional procedures in another. This regulatory divergence can increase compliance costs and limit potential operational synergies between subsidiaries or divisions within the same group.

Cultural differences

Beyond technical issues, European defence programmes also reflect differing institutional approaches to data governance, cybersecurity and digital sovereignty. Some countries prioritise highly centralised, sovereignty-driven models, while others adopt more flexible or mutualised approaches. These differing perspectives can slow the development of common frameworks, complicate negotiations and often require extensive coordination to align strategic visions.

Persistent legal uncertainty

Companies participating in Europe's multinational defence programmes must navigate multiple national regulatory frameworks. Fully understanding and complying with these requirements often demands specialised legal and security expertise. In practice, companies may need to engage multiple legal specialists and security experts for each jurisdiction in order to interpret national regulations and translate them into operational compliance requirements.

2.3 How fragmentation marginalises SMEs and innovators

Digital regulatory fragmentation across the EU-27 does not affect all stakeholders equally. While large industrial groups often have the resources to navigate regulatory complexity, SMEs, digital-first companies and cross-border service providers face structural barriers that can limit their participation in major European defence programmes. This situation can constrain the full participation of the industrial ecosystem and may affect the pace of innovation.

High entry barriers for innovative SMEs and academia

SMEs and academia, often at the forefront of innovation in areas such as cloud computing, cybersecurity and artificial intelligence, face the same regulatory requirements as larger companies but with fewer internal resources to manage them. The diversity of national security certification rules, particularly for RESTRICTED-level classifications, can place a relatively heavier burden on smaller organisations as they typically have less capacity and fewer specialised legal or security teams to manage complex compliance obligations or interpret multiple national regulations.

For smaller firms, these requirements can represent a significant share of available staff time, administrative capacity and financial resources. Certification delays can also have a more immediate impact on SMEs, which may depend on predictable cash flow and may not be able to keep teams idle while awaiting approvals. In addition, SMEs typically operate from a single Member State, making them more exposed to domestic hosting requirements, national vetting procedures and duplicative audits.

This is particularly relevant for SMEs, startups, scale-ups and academic actors developing high-TRL digital and dual-use technologies. Many of these organisations are well-positioned to respond to emerging defence needs with agile, challenge-driven solutions, but they often lack the capacity to navigate multiple national approval pathways in parallel. As a result, fragmentation can limit not only market access but also the speed at which innovative capabilities reach operational users.

A disproportionate regulatory burden for cross-border providers

Digital service providers operating across multiple European countries must adapt their offerings to heterogeneous regulatory frameworks. This often means redeploying nearly identical services in each country, maintaining separate infrastructures or navigating parallel certification processes. These constraints can result in fragmented service delivery, limited interoperability between Member States, higher deployment and maintenance costs and reduced operational efficiency. Such burdens are ultimately passed on to customers and can be particularly difficult for SMEs to absorb. They can also discourage investment in scalable European solutions, as firms may be forced to repeatedly adapt nearly identical services to fragmented national requirements rather than invest in common architectures, product improvements, or accelerated market uptake.

A structural imbalance in the European industrial ecosystem

Taken together, these obstacles can create uneven conditions for participation within the European defence ecosystem. Larger industrial groups may be better positioned to manage regulatory complexity, while SMEs and start-ups may find participation in complex cross-border tenders more resource-intensive. In some cases, regulatory complexity may influence investment decisions and the allocation of innovation resources across markets. Over time, such dynamics may affect Europe's ability to fully leverage its technological base and strengthen its defence industrial capabilities.

These realities do not diminish the importance of larger actors, whose experience, infrastructure and long-term commitments remain essential to multinational defence cooperation. Nevertheless, addressing these barriers would help ensure that Europe benefits from the full technological diversity and agility of its defence and digital ecosystem, allowing established industry, SMEs, academia and start-ups to collaborate more effectively.

2.4 One continent, many rules

Understanding cross-border interoperability challenges in defence requires a clear view of the diverse regulatory frameworks governing sensitive digital data. This study provides a comparative overview of selected national approaches, illustrating how different frameworks are structured and how key partners such as NATO and the Organisation for Joint Armament Cooperation (OCCAR) regulate RESTRICTED-level defence data and systems.

The detailed comparison is presented in Annex 5: Understanding Europe's security divergences. Rather than offering an exhaustive legal analysis, the annex focuses on identifying key divergences and similarities between regulatory systems. By highlighting these differences, the analysis illustrates how variations in regulatory approaches can affect cooperation and where greater regulatory alignment may enhance operational effectiveness. The comparison draws on examples from Germany, France and Spain.

These differences have practical implications. In several multinational defence programmes, pending licences, national authorisations, or unresolved security equivalence issues have delayed project progress. As collaborative projects require all partners to be authorised to access and handle shared information, delays affecting one participant can cascade across the entire consortium timeline.

Taken together, the examples presented in this chapter illustrate how regulatory divergence across Member States creates practical challenges for multinational defence programmes, particularly when digital systems and cross-border data environments are involved. While these frameworks reflect legitimate national security responsibilities, their interaction in multinational projects can lead to operational inefficiencies, increased compliance burdens and delays in capability deployment. These effects are particularly visible in areas such as cloud deployment, certification processes and the integration of SMEs and digital innovators into collaborative programmes.

Addressing these challenges, therefore, requires pragmatic approaches that respect national security prerogatives while improving regulatory coherence across the European defence ecosystem. The following chapter outlines possible pathways to achieve this objective.

Chapter 3
Recommendations to reduce digital fragmentation

The analysis presented in the previous **chapter highlights how regulatory fragmentation creates practical barriers to deploying digital systems in multinational defence programmes.** While these differences reflect legitimate national security responsibilities, their interaction within collaborative projects can generate operational inefficiencies, increase compliance burdens and slow the integration of innovative digital capabilities. In the current security environment, such delays directly affect Europe's ability to deploy digital capabilities at the pace required by operational needs. Addressing these challenges requires pragmatic solutions that improve regulatory coherence while fully respecting national security competencies.

Against this backdrop, this **chapter sets out industry-driven recommendations to strengthen interoperability and facilitate the secure deployment of digital systems across borders.** These recommendations do not seek full legislative harmonisation of national security frameworks, which is neither feasible nor necessary. Instead, they focus on practical near-term measures, alongside structural measures over the medium and longer term, to reduce digital regulatory fragmentation and support more effective cross-border collaboration in European defence projects. They are designed to improve predictability, reduce duplication and accelerate the deployment of digital capabilities across multinational programmes. In doing so, they also support a broader shift towards more software-defined, data-driven and modular defence capabilities, which increasingly depend on secure interoperability, predictable validation pathways and the ability to scale digital solutions across borders.

Coherence with the EU Defence Simplification Process

The recommendations presented in this chapter complement the political and legislative direction set out in the June 2025[8] proposal for a Directive amending Directives 2009/43/EC and 2009/81/EC (COM(2025) 823 final). However, while this proposal focuses primarily on the movement of defence products and the simplification of procurement procedures, it only partially addresses the digital, operational and cross-border deployment challenges highlighted in this study.

Several measures could help **reinforce the objectives of the Defence Simplification Omnibus** while remaining fully consistent with national security competencies. These include enhanced mutual recognition mechanisms, federated and layered system architectures, streamlined accreditation timelines and clearer participation pathways for SMEs and digital-first suppliers. Addressing these dimensions is essential to ensure that simplification efforts translate into faster and more effective deployment of digital capabilities across multinational programmes. This is particularly important for digital and dual-use capabilities, where lengthy or duplicative approval processes can undermine the speed advantages these technologies are meant to deliver.

8 European Commission. (2025). *Proposal for a Directive of the European Parliament and of the Council amending Directives 2009/43/EC and 2009/81/EC as regards the simplification of intra-EU transfers of defence-related products,* COM(2025) 823 final, 2025/0177 (COD). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0823

The recently proposed **Programme for Agile and Rapid Defence Innovation (AGILE)**[9] further confirms this policy direction. Presented by the European Commission as a complementary instrument to the EDF and EUDIS, AGILE is designed to support faster innovation cycles, simplified access to funding and a more rapid transition from development to deployment, particularly for SMEs, start-ups and other non-traditional defence actors. AGILE is especially relevant to the issues identified in this study because it places strong emphasis on testing, validation, field demonstration and market uptake, with the stated objective of reducing time-to-award and helping innovative defence technologies reach operational use much more quickly than under traditional funding approaches. In this sense, AGILE reinforces the case for clearer accreditation pathways, more coordinated testing environments and faster cross-border deployment conditions for digital and dual-use capabilities in European defence.

Without faster and more predictable accreditation timelines, validation processes and cross-border recognition mechanisms, regulatory fragmentation will continue to delay the deployment of digital capabilities and weaken Europe's defence readiness.

9 European Commission. (2026). *Commission presents €115 million programme for agile defence innovation (AGILE).* https://ec.europa.eu/commission/presscorner/detail/en/ip_26_687

3.1 Strategic recommendations to enhance interoperability

Current practice: mutual recognition practices in defence

In the defence and security domain, mutual recognition is not a new concept; it already exists in limited form. Within the EU, Member States recognise each other's security clearances for handling EU-classified information. This allows the exchange and protection of information generated within EU frameworks. Likewise, NATO and OCCAR establish recognised equivalence between their own classification levels and corresponding national categories.

However, these existing mechanisms primarily address the equivalence of classification and personnel clearances. They do not extend to the underlying technical, operational and accreditation requirements governing digital systems. As a result, even where classification levels are recognised as equivalent, the systems handling such information remain subject to divergent national validation and certification processes.

Recommendation 1: Strengthen operational mutual recognition mechanisms

To reduce the operational impact of regulatory fragmentation, the **study recommends establishing** structured, project-based **mutual recognition mechanisms** that would allow participating Member States to recognise national security controls already validated in another participating Member State within multinational programmes.

Current arrangements in the EU, NATO and OCCAR provide baseline equivalence between security classification levels. However, they do not address the deeper differences in national security standards, technical controls, accreditation procedures or compliance expectations. As a result, even when countries agree that information is "RESTRICTED," the systems handling that data must still comply with divergent national requirements.

A practical approach would be to establish a structured mechanism through which Member States could, on a voluntary, project-specific basis, recognise each other's validated security controls for joint programmes. Such an approach could, under defined and mutually agreed conditions, extend beyond classification labels to elements of the underlying security frameworks.

The practical implications of this challenge can be illustrated through national certification frameworks. For example, Germany uses the classification level VS-NfD (Verschlusssache – Nur für den Dienstgebrauch), which in this study is treated as a national reference point for restricted-level sensitive information in multinational defence cooperation. IT systems handling this information must be certified by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), reflecting the role of national certification requirements in shaping cross-border deployment conditions.

In a multinational defence programme, a system may already be certified by BSI to handle VS-NfD information. However, when the same system is deployed in another participating Member State, it may still be required to undergo additional national certification procedures. As a result, companies may need to repeat validation processes in several countries, increasing costs and delaying the deployment of digital solutions across the programme.

A structured mutual recognition mechanism would:

- reduce duplication of certification procedures;
- accelerate deployment timelines;
- increase predictability for multinational programmes;
- maintain national security safeguards through clearly defined conditions.

In practice, this would enable participating Member States to recognise validated national certifications within specific multinational programmes, while retaining the ability to apply justified national safeguards where necessary.

European standards can support this effort by aligning technical requirements across Member States and connecting European stakeholders to international standards through established cooperation mechanisms, such as the Vienna Agreement (CEN–ISO) and the Frankfurt Agreement (CENELEC–IEC).

In the longer term, Member States may also explore the feasibility of shared accreditation support mechanisms at the European or NATO level. Such mechanisms would not replace national authority over security decisions but could provide centralised technical evaluation, security testing or pre-assessment of digital systems and vendors.

This would **reduce duplication of effort across national authorities** and **accelerate the deployment of trusted technologies in multinational programmes.** It would also help accreditation authorities avoid repeating security evaluations across trusted partners and focus resources on assessing genuinely new technologies.

Recommendation 2: A federated and layered architecture

In the medium term, a **federated and layered model for defence data and systems** offers a realistic and implementable alternative. Rather than requiring countries to adopt a single system, this approach allows each nation to retain authority over its own data and security infrastructures. At the same time, it enables cooperation within a shared and secure framework.

In this context, digital sovereignty should not be understood solely in terms of physical localisation or the exclusive use of national infrastructure. In secure digital environments, sovereignty can, in some contexts, also be exercised through effective control over data, access rights, encryption, auditability, security policies, and operational governance. A federated and layered architecture can therefore help reconcile national sovereignty requirements with the need for secure interoperability by allowing Member States to retain authority over sensitive assets while enabling trusted cross-border collaboration. This study takes no position on national choices regarding data localisation, which remain a sovereign prerogative of each Member State.

Such an architecture can be structured around **three complementary layers:** a **data layer,** a **service layer** and an **application layer.** See Annex 6: A federated and layered architecture. **This approach enables:**

- national authority over sensitive data and security infrastructures;
- secure cross-border data exchange through standardised interfaces;
- modular integration of services and applications across multinational environments.

This structure allows systems to interoperate while respecting national sovereignty over sensitive data and security infrastructures. EU projects such as AEROSEC are particularly well-suited to exploring and validating these architectural approaches in practice. This approach also provides a more suitable foundation for software-defined and modular capability development, enabling updates, services and applications to be integrated more flexibly across multinational environments without requiring each participating country to redesign its entire national architecture.

As defence systems become increasingly software-defined and data-driven, federated architectures provide a scalable pathway to enable interoperability, accelerate capability deployment and support continuous technological evolution across European defence programmes.

3.2 Operational enablers for implementation

The strategic recommendations outlined above require practical operational measures to support their effective implementation. The following enablers address key bottlenecks identified in the analysis, focusing on **improving predictability, reducing duplication** and **facilitating the deployment of digital capabilities across multinational programmes.** These **measures** are designed to complement existing frameworks and can be implemented progressively, while fully respecting national security competencies.

Supporting measure A: more predictable accreditation timelines

Introducing predictable, time-bound accreditation processes is essential to align regulatory frameworks with operational and innovation timelines.

A key enabling measure is to introduce maximum processing times for basic personnel and facility clearances. As an indicative benchmark, approvals should, where feasible and without prejudice to national security assessments, move towards more predictable timelines, for example, 60–90 days for routine cases. System accreditations, which can vary more significantly in complexity, should also benefit from clearer predictability, including indicative benchmarks where feasible and appropriate.

Many national procurement processes allow contractors to obtain domestic personnel or facility clearances only after a contract is awarded. In practice, this means that critical clearance procedures often begin only once the contractual process is complete, delaying project mobilisation from the outset.

Without fixed processing timelines and given the significant differences between Member States' procedures, projects can face several recurrent challenges:

- uncertain project start dates;
- staff or facilities that must be retained but cannot yet be deployed;
- cross-border partners forced to plan around unpredictable delays.

These challenges are not hypothetical. In several recent cases, even routine approvals have taken several months to process. For rapidly evolving digital technologies, such delays create a mismatch between innovation cycles and approval cycles. One practical response to this mismatch is to enable the faster adoption of proven commercial and dual-use technologies where they have already been tested, validated, or accredited in trusted environments, provided that equivalent assurance levels can be demonstrated. Over time, accreditation approaches could also make greater use of secure-by-design principles, automated compliance evidence, continuous monitoring and real-time risk visibility, particularly for rapidly evolving software-defined capabilities.

Greater predictability in accreditation timelines would reduce delays, improve planning across multinational consortia and help ensure that critical digital capabilities can be deployed at the pace required by today's security environment.

Supporting measure B: transparent guidance and language harmonisation

Improving transparency and clarity of national requirements is essential to reduce misinterpretation and facilitate cross-border deployment of digital systems in defence programmes.

A key enabling measure is to publish clear and accessible guidance documents, in English and/or national languages, that map national requirements to existing international standards where relevant. Such guidance would help companies better understand compliance expectations across different jurisdictions and reduce uncertainty in multinational projects. Improved transparency would also facilitate participation by SMEs and digital-first firms, which often have fewer internal resources to interpret complex regulatory frameworks.

This would lower entry barriers for startups, scale-ups and dual-use technology providers whose solutions may be technically mature but whose ability to participate is constrained by fragmented and difficult-to-interpret compliance environments.

Greater transparency would improve interoperability by enabling companies to design and deploy systems that can meet multiple national requirements more efficiently, reducing the need for repeated adjustments and duplicate certification procedures.

Supporting measure C: coordinated testing and validation environments

Establishing coordinated testing and validation environments is essential to reduce duplication and accelerate the deployment of digital and dual-use technologies across European defence programmes.

A key enabling measure is to establish and support trusted, coordinated European testing and validation environments where digital solutions can be assessed, demonstrated and refined within frameworks recognised by participating national authorities.

Such environments would reduce the need for repeated national validation procedures and enable companies to test interoperability, security compliance and performance requirements in a more integrated and predictable setting.

This is particularly important for SMEs, startups and innovative suppliers seeking to transition from prototype to deployment in multinational programmes. Better coordination between Member States, relevant EU instruments and, where appropriate, NATO-linked testing ecosystems would further strengthen the efficiency and credibility of these environments.

Coordinated testing and validation environments would enable solutions to be assessed once and, where appropriate, deployed across multiple national contexts, reducing duplication and accelerating the scaling of trusted digital capabilities in European defence.

3.3 Priority actions and indicative implementation timeline

The strategic recommendations and operational enablers presented above do not all lend themselves to implementation on the same timeline. Some can be pursued in the short term within existing frameworks, while others depend on pilot activities, structured cooperation or longer-term institutional development. The following **priority actions,** ranging from the short to the longer term, therefore propose a possible implementation sequence based on industry experience and aligned with ongoing EU and NATO initiatives.

Short-term (0–12 months)	Medium-term (1–3 years)	Longer-term
Initiate pilot mutual recognition mechanisms in selected multinational programmes.	Scale federated and layered architectures through EU-funded pilots and existing initiatives (e.g. AEROSEC).	Explore shared European or NATO-level accreditation support mechanisms.
Introduce indicative timelines for routine personnel and facility approvals (e.g. 60–90 days).	Develop coordinated testing and validation environments.	Strengthen alignment of national frameworks through structured cooperation and exchange of best practices.
Publish clear guidance on national requirements and their relation to relevant standards.	Promote alignment of technical requirements through European standardisation efforts (e.g. CEN–CENELEC cooperation)	Promote gradual convergence of accreditation practices through continued standardisation, cooperation and exchange of experience.

3.4 Supporting annexes

The following annexes provide additional analysis that complements and reinforces the recommendations set out in this chapter, including cross-sector perspectives, operational pilot initiatives and alignment with ongoing EU policy developments:

- Annex 7: Cross-sector insights
- Annex 8: Multinational digital capability pilot: AEROSEC
- Annex 9: Strengthening the EU Defence Readiness Omnibus

Conclusion

European defence cooperation increasingly depends on secure digital systems, trusted data exchange and effective cross-border industrial collaboration. As this DIGITALEUROPE study shows, differences in national frameworks governing RESTRICTED-level sensitive information continue to create practical barriers to that cooperation. These barriers are particularly significant for digital and dual-use capabilities, where Europe's ability to innovate, validate and scale new solutions depends on whether secure systems can operate coherently across national boundaries.

The comparative analysis shows that national systems are often similar in overall structure and intent, but can differ significantly in technical interpretation and operational implementation. In practice, these differences shape encryption choices, access-control models, cloud architectures and certification pathways. Within multinational programmes, they can affect supplier participation, infrastructure design and programme timelines, with cumulative effects that fall especially heavily on SMEs and digital-first companies.

The evidence gathered through this study points to a clear conclusion: these challenges do not arise from a lack of shared strategic objectives. They stem from divergent implementation practices and from the absence of practical mechanisms that allow trusted security controls to be recognised across national jurisdictions. As a result, companies participating in multinational defence programmes can still face repeated certification procedures, additional infrastructure requirements and delays in deploying secure digital solutions across borders.

The way forward is equally clear. Europe does not need full legislative harmonisation of national security systems. It needs pragmatic regulatory convergence that improves interoperability, predictability and mutual confidence while fully respecting national security competences. In that context, the most immediate priority is stronger mutual recognition of accredited systems, validated security controls and equivalent assurance mechanisms across trusted EU and NATO environments. This should be supported by more predictable accreditation timelines, federated and layered digital architectures, stronger testing and validation capacities and more accessible participation pathways for SMEs and innovative suppliers.

Improving the timely, transparent and interoperable handling of RESTRICTED-level sensitive information is a foundational enabler of modern defence cooperation. Reducing avoidable regulatory friction will not alter national security responsibilities. It will, however, enable Europe to mobilise its defence and digital ecosystems more effectively in support of defence readiness, operational cooperation and capability development.

Advancing interoperability through pragmatic regulatory convergence, rather than structural centralisation, offers a realistic and achievable path forward. By strengthening mutual trust between national systems and improving regulatory predictability, Europe can accelerate the deployment of secure digital capabilities and improve the effectiveness of multinational defence cooperation. DIGITALEUROPE and its members are ready to continue contributing industry expertise to support policymakers, Member States and European institutions in addressing these challenges.

Ultimately, enabling the secure and efficient deployment of digital capabilities across borders is no longer only a regulatory or technical challenge. It is a strategic requirement for Europe's security, technological resilience and collective defence preparedness. Meeting this challenge will require faster, more predictable and more coordinated action across Europe.

Annexes

This section contains a **short terminology clarification** and the following **nine Annexes** to support the analysis, findings and recommendations of the study:

- **Annex 1.** Terminology clarification
- **Annex 2.** Methodology and contributors
- **Annex 3.** Illustrative examples of national divergences
- **Annex 4.** Deep dive on unified metadata and PLM
- **Annex 5.** Understanding Europe's security divergences
- **Annex 6.** Federated and layered architecture
- **Annex 7.** Cross-sector insights
- **Annex 8.** Multinational digital capability pilot: AEROSEC
- **Annex 9.** Strengthening the EU Defence Readiness Omnibus

1. Terminology clarification

The term "RESTRICTED" is used as a functional reference point for restricted-level sensitive information across national, EU and NATO frameworks. In practice, this includes national or transnational classification levels such as Diffusion Restreinte (France), VS-NfD (Germany), EU RESTRICTED and NATO RESTRICTED.

While EU and NATO classification systems have their own legal and procedural foundations, many multinational defence programmes rely on national restricted-level frameworks or programme-specific security instructions. These frameworks are not harmonised and form part of the regulatory fragmentation examined in this study. The term is therefore used as an analytical reference to examine cross-border challenges in multinational defence cooperation, without implying legal equivalence between the underlying frameworks.

2. Methodology and contributors

This annex provides additional detail on the evidence base underpinning the study and complements the methodological overview presented in Section 1.2. The study is based on a combination of operational input, comparative analysis, policy review and expert consultation. Its findings reflect recurring patterns identified across multinational defence programmes involving digital systems handling RESTRICTED-level information. Unless otherwise indicated, examples are illustrative and anonymised, used to identify operational and regulatory bottlenecks rather than to provide an exhaustive legal or statistical assessment of all national frameworks.

The **analytical foundation** of the study draws on the following components:

- **Operational input from industry:** Members of DIGITALEUROPE's Defence Working Group shared concrete experiences from multinational defence programmes. The Working Group represents a broad cross-section of companies active in Europe's defence, digital and dual-use ecosystem. These inputs included recurring challenges linked to accreditation delays, national divergences in RESTRICTED-level requirements, cloud-hosting constraints, encryption rules, facility and personnel clearances and interoperability barriers.
- **Cross-industry comparative analysis:** The study incorporates perspectives from a range of operational domains, including secure communications, cloud services, artificial intelligence, software engineering and Product Lifecycle Management (PLM) platforms. This helped identify common bottlenecks affecting the cross-border deployment of digital systems in defence environments.

- **Review of relevant policy and governance frameworks:** The analysis considered relevant EU, NATO and EDA initiatives addressing interoperability, secure digital architectures and defence cooperation. It also took into account the evolving EU policy context, including the Defence Readiness Omnibus and related discussions on simplifying the regulatory conditions for cross-border defence cooperation.
- **European standardisation and technical cooperation:** The study also considered the role of European standardisation frameworks and industry engagement with relevant bodies, including CEN and CENELEC, in supporting interoperability and greater alignment of technical requirements across Member States.
- **Insights from the AEROSEC pilot project:** Additional operational insight was drawn from the ongoing Digital Europe Programme-funded pilot project AEROSEC. These inputs helped inform the study's reflections on secure multi-cloud collaboration, federated architectures and the testing of interoperable digital solutions in sensitive defence environments.
- **DIGITALEUROPE's prior policy work:** The study builds on DIGITALEUROPE's broader strategic work on defence digitalisation and industrial readiness, including contributions to relevant EU defence policy processes and related analytical work on digital defence innovation, simplification and interoperability. This includes DIGITALEUROPE's:
  - Contribution to the EU Defence Simplification Omnibus;
  - Executive Brief "Boosting European Digital Defence Innovation", including its Annex of Nine Policy Recommendations[10];
  - Input to the European Defence Industry Transformation Roadmap[11].
- **Expert consultation and review:** Draft findings and recommendations were reviewed by senior industrial experts and technical specialists with experience in secure cloud, cybersecurity, AI assurance, engineering and PLM, as well as members of the Defence Working Group.

Taken together, these components provide the basis for an industry-led policy analysis that identifies practical barriers and formulates proportionate, sovereignty-respecting recommendations to support more secure and effective cross-border digital cooperation in European defence.

10 DIGITALEUROPE. (2025). *Executive brief: boosting European digital defence innovation* https://cdn.digitaleurope.org/uploads/2025/02/DIGITALEUROPE-THE-EXECUTIVE-BRIEF-FINAL-WEB.pdf

11 DIGITALEUROPE. (2025). *Our input to the European defence industry transformation roadmap.* https://cdn.digitaleurope.org/uploads/2025/11/DIGITALEUROPE-paper-_European-Defence-Industry-Transformation-Roadmap-1.pdf

3. Illustrative examples of national divergences

Cross-border classification and accreditation

To illustrate how these divergences manifest in practice, the following examples (see Table 1) highlight typical barriers industry may face when operating across multiple Member States. These cases reflect broader patterns observed in many multinational defence programmes.

Table 1. Illustrative examples of national divergences in RESTRICTED-level requirements

Example 1. Divergent encryption requirements (France, Germany, Spain)	
ISSUE	**IMPACT**
Encryption requirements for classified communications vary between France, Germany and Spain[12] making it challenging to define a common standard for embedded systems. In practice, a provider wishing to serve all three markets must invest in solutions that can adapt to distinct national requirements. This can be achieved through **modular product design,** which is not always feasible for specialised offerings, or through **parallel products** tailored to each national regime. Both approaches can increase development costs, require scarce technical expertise and raise the risk of integration errors associated with non-standardised solutions.	This example illustrates how well-intentioned national security policies can inadvertently hinder multinational cooperation. To participate in joint programmes, companies must adapt their systems to satisfy a range of divergent national requirements, some of which may be technically incompatible. This can lead to parallel technical solutions, repeated certification procedures and additional layers of engineering complexity. The result may be higher costs, longer deployment timelines and increased operational burdens, particularly for specialised suppliers and SMEs.
Example 2. Illustrative national framework example (Hungary)	
ISSUE	**IMPACT**
In Hungary, the domestic legal regime on classification is based on the **Act CLV of 2009 on the Protection of Classified Information** (as subsequently amended). The Act defines classification levels, responsibilities for entities handling classified material and obligations for public authorities and contractors. However, national vetting and accreditation functions are carried out by distinct services, notably the **Constitution Protection Office** (for civilian national-security vetting) and the **Military National Security Service** (for defence-specific clearances). This institutional separation can result in parallel procedures and differing interpretations of the same national rules.	Hungary's example illustrates that even within a single Member State, multiple agencies, procedures and approval pathways may coexist, creating additional layers of complexity for industry. For multinational projects, this fragmentation can increase administrative effort, extend timelines and complicate efforts to achieve consistent compliance across participating countries. This type of institutional overlap is not limited to Hungary. Similar coordination challenges may arise in other Member States where multiple authorities are responsible for security accreditation and technical certification. For example, in Germany, responsibilities related to defence industry regulation and IT security certification involve different authorities, including the **Federal Ministry responsible for economic affairs** and **the Federal Office for Information Security (BSI).**

12 Murphy, R., & West, H. (2025, August 7). *The Encryption Debate*. Center for European Policy Analysis. https://cepa.org/comprehensive-reports/the-encryption-debate/

4. Deep dive on unified metadata and Product Lifecycle Management

Product Lifecycle Management (PLM) systems depend on structured technical metadata that can be shared reliably across industrial partners. In multinational defence programmes, however, the absence of aligned metadata practices creates significant barriers to collaboration from the earliest stages of development. Differences in formats, data structures, reference models and documentation rules between Member States and companies lead to incompatibilities, duplication of work and loss of traceability throughout the programme lifecycle. These issues are amplified when RESTRICTED-level information cannot be exchanged through a single secure PLM environment due to differing national accreditation rules and diverging hosting requirements.

This challenge is already visible in early Research and Technology (R&T) and Research and Development (R&D) phases of several international armament programmes, where partners seek to establish a common PLM backbone but are forced to maintain parallel national environments to comply with domestic security requirements. The **result is fragmented engineering workflows, inconsistent datasets** and **reduced efficiency** at stages where early alignment is critical for long-term cost control and programme scheduling.

These emerging patterns underline the **need for more predictable cross-border rules** for secure PLM usage rather than entirely new technical standards. Without greater convergence on accreditation and handling requirements for RESTRICTED-level defence data under national classification regimes, the benefits of shared PLM systems cannot be fully realised. Multinational programmes may therefore continue to carry unnecessary digital fragmentation from their earliest phases.

As defence systems become increasingly digital and software-defined, the ability to exchange engineering data securely and efficiently across national boundaries is becoming a critical enabler of programme delivery, industrial cooperation and Europe's overall defence readiness.

In addition to approaches based on cross-border rules, there is also a need to consider approaches grounded in shared digital models inspired by the principles of Model-Based Systems Engineering (MBSE). These approaches can help standardise metadata structures and collaborative processes across participating organisations.

Experience from complex multinational programmes such as the Future Combat Air System (FCAS) and the Main Ground Combat System (MGCS) suggests that using federated digital models aligned with MBSE principles can significantly reduce design-phase lead times. This approach is software-agnostic, for example, across PLM platforms and Computer-Aided Design (CAD) systems, applicable to multiple collaborative ecosystems, and compatible with existing national architectures. At the same time, it can help reduce duplication costs by limiting manual data re-entry and repeated data conversions between systems.

Such an approach could support the establishment of a common technical reference framework based on neutral formats, such as STEP AP242 (Standard for the Exchange of Product Model Data – Application Protocol 242) for 3D engineering data, combined with shared metadata ontologies and automated compliance mechanisms capable of integrating national security requirements.

5. Understanding Europe's security divergences

Understanding the challenges of cross-border interoperability in defence requires a clear view of the diverse regulatory landscapes governing sensitive digital data. This annex provides a comparative overview of how different national frameworks, including those of EU Member States and key partners such as NATO and the Organisation for Joint Armament Cooperation (OCCAR), regulate RESTRICTED-level defence data and systems.

Rather than offering an exhaustive legal analysis, the annex focuses on identifying key divergences and similarities. Highlighting these differences illustrates **recurring patterns of fragmentation** that **impede seamless cooperation** and **identifies opportunities for greater regulatory coherence that could enhance operational effectiveness.** The examples discussed here focus on the regulatory differences that have the greatest impact on cross-border interoperability, including data access, secure communication protocols and system certification.

This snapshot approach helps to map the current landscape and provides a basis for future efforts to improve regulatory coherence, supporting more agile and integrated multinational operations. To better illustrate these challenges, this analysis draws on examples from the regulatory frameworks of **Germany, France** and **Spain.**

Germany: Verschlusssache – Nur für den Dienstgebrauch (VS-NfD)

The German classification system uses **Verschlusssache – Nur für den Dienstgebrauch (VS-NfD),** meaning "Classified Information – For Official Use Only," as its lowest level of government classified information. In this study, it is used as a national reference point for restricted-level sensitive information in multinational defence cooperation and is governed by defined national security controls. Although it represents the baseline level of classified information, mishandling VS-NfD data, such as technical drawings or contract details, can still cause damage to national interests or government operations.

The **German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI)** approves specific IT security solutions for handling VS-NfD data, with a strong emphasis on encryption, role-based access and detailed audit logging. Responsibilities related to defence industrial participation and regulatory oversight involve several authorities, including the federal ministry responsible for economic affairs and the BSI. For cross-border collaboration, Germany typically requires formal arrangements between partners to establish security equivalence between national classification systems. Similar to France's Diffusion Restreinte framework, VS-NfD is not limited exclusively to defence-related information and may also apply to other sensitive governmental or industrial data.

France: Diffusion Restreinte (DR)

In France, **Diffusion Restreinte (Restricted Distribution – DR)** is a designation for sensitive but non-classified information. Introduced in 1991, it is a dissemination marking distinct from higher-level classified information such as Secret and Très Secret. DR is intended to protect non-public information whose unauthorised disclosure could harm France's political, military or economic interests.

The regulatory framework governing DR information systems is defined in the Interministerial General Instruction No. 1300 (Instruction générale interministérielle n°1300 – IGI 1300) and complementary guidance issued by the Secrétariat général de la défense et de la sécurité nationale (SGDSN) and the French cybersecurity authority ANSSI (Agence nationale de la sécurité des systèmes d'information). These frameworks require security measures such as strong authentication, data tagging and the certification or homologation of information systems and their interconnections. The DR framework applies not only to defence but also to sensitive public- and private-sector information, reflecting its broader use across government and critical sectors.

Spain: Difusión Limitada / Reservado

Spain applies national rules and security procedures for handling sensitive information in defence and governmental contexts. Publicly available information on the detailed operation of these arrangements appears to be more limited than in the cases of Germany and France. However, the Spanish approach is clearly based on national control of access, controlled dissemination and the protection of information whose unauthorised disclosure could harm national interests.

The designation **Difusión Limitada (Limited Distribution)** is used to categorise sensitive but non-public information requiring controlled dissemination, while **Reservado** represents a higher level within Spain's formal classification system. In the context of this study, these categories may serve as national reference points for restricted-level sensitive information in multinational cooperation, while remaining fully subject to Spain's own legal, procedural and security requirements.

In operational terms, the Spanish framework appears to rely on need-to-know principles, controlled access, formal authorisation procedures and appropriate organisational and technical safeguards. In multinational programmes, more detailed handling arrangements may also be set out through national instructions, bilateral security arrangements or programme-specific security documentation. As with other national frameworks, the practical implementation of these requirements can shape the conditions under which secure digital systems are deployed and operated across borders.

The gaps that create real problems

While all three EU Member States aim to protect sensitive defence data, their differing regulatory approaches can create operational friction in collaborative projects. The most notable differences appear in two broad areas: the **level** of **technical prescription** and the **conceptual classification of restricted data.**

- **Divergent technical implementation:** Germany's VS-NfD framework is relatively prescriptive, with the Federal Office for Information Security (BSI) approving specific hardware and software solutions for handling and encrypting sensitive information. In contrast, France and Spain generally follow a more principles-based approach, focusing on security requirements and the "need-to-know" principle without necessarily mandating specific technologies. As a result, a digital platform designed to comply with German requirements using BSI-approved components may not be directly interoperable with French or Spanish systems. Bridging these differences may require additional technical integration and adaptation efforts.
- **Different conceptions of restricted information:** Another important difference concerns how each country defines restricted or sensitive data. Germany's VS-NfD is part of a formal hierarchical classification system, while France's Diffusion Restreinte is treated as sensitive information subject to controlled dissemination rather than formal classification. Spain's framework, while often used in multinational contexts as a national reference point for restricted-level information, is less publicly documented and frequently relies on bilateral or programme-specific security arrangements to define detailed protocols. These differences do not prevent cooperation, but they can affect predictability, implementation timelines and the conditions for cross-border deployment.

- **Differences in access and clearance procedures:** Germany allows certain VS-NfD information to be processed without a formal Personal Security Clearance, provided that appropriate organisational, physical and IT security measures are in place. In France and Spain, information designated as Diffusion Restreinte (DR) or Difusión Limitada may also be handled under relatively low-threshold access procedures, although formal briefings, authorisation processes and organisational controls are still required.

Taken together, **these divergences can lead to operational delays in multinational programmes.** In several cases, **pending licences, national authorisations, or unresolved security equivalence questions** have **delayed programme progress for months or even longer.** Because collaborative projects require all partners to be authorised to access and handle shared information, delays affecting one participant can affect the wider programme timeline.

Delays affecting one participant can cascade across the entire consortium timeline. Procedural misalignment, rather than purely technical complexity, can therefore become a significant bottleneck in multinational digital defence programmes.

To **illustrate how these divergences translate into operational obstacles,** the following examples (Table 2) provide a practical view of the challenges encountered when multinational teams attempt to work within a shared digital environment.

Table 2. Practical examples of how divergent national rules create operational challenges

Challenge 1: Encryption		
CONTEXT	**REGULATORY DIVERGENCE**	**OPERATIONAL IMPACT**
Consider a joint defence project between Germany, France and Spain to develop a new multinational command-and-control software system. All three countries' industry participants need to share RESTRICTED-level data, documents and source code. To ensure this data remains secure, all three nations agree that the data must be encrypted both in transit and at rest.	The difficulty arises from differing national encryption requirements. ▶ **Germany** mandates the use of encryption algorithms and products certified by the Federal Office for Information Security (BSI). ▶ **France** requires encryption solutions that meet a defined level of robustness, often guided by standards issued by ANSSI (Agence nationale de la sécurité des systèmes d'information). However, these may not rely on the same list of approved products as Germany. ▶ **Spain** may apply national security guidance, formal authorisation procedures or programme-specific approval arrangements that differ from those used in Germany or France.	Because of these differences, the project cannot simply adopt a single off-the-shelf encryption solution. Instead, developers may need to design a multi-layered system or identify solutions that are technically and operationally acceptable to all participating nations. This can increase development complexity, introduce delays and raise programme costs.
Challenge 2: Data access		
CONTEXT	**REGULATORY DIVERGENCE**	**OPERATIONAL IMPACT**
In the same joint project, engineers from all three countries need access to a shared digital platform that contains RESTRICTED-level data.	The core issue is not the classification of the data itself, but the different national rules governing how access to that data is managed. ▶ **Germany** uses a highly controlled, role-based access management model in which access is formally documented and audited according to specific job functions. Access to VS-NfD information generally takes place through appropriately secured and accredited networks or information systems. ▶ **France** applies a more principles-based model, relying on personnel-based authorisation and the overall homologation of the information system, within which an engineer's clearance may grant broader access based on the "need-to-know" principle. ▶ **Spain** often relies on formal bilateral agreements or project-specific security plans to define access rules, with approvals granted through a project-specific authorisation procedure.	These differing approaches can make it difficult to establish a unified digital workspace. As a result, projects may need to deploy multi-layered systems or rely on slower, manually controlled processes, which can slow cross-border collaboration and make it less efficient.

Comparison with EU RESTRICTED, NATO and OCCAR

National restricted-level classifications are often used in multinational cooperation as functional reference points alongside EU RESTRICTED, NATO RESTRICTED and OCCAR RESTRICTED. This does not imply legal equivalence or fully harmonised national security requirements. Rather, it reflects the use of agreed classification mappings and practical arrangements that support the exchange and protection of sensitive information across different frameworks.

NATO and OCCAR provide a common baseline of security requirements accepted by participating nations, establishing a shared foundation for the handling, exchange and protection of sensitive information. However, individual countries may apply additional national rules on top of this baseline. As a result, **even where a system complies with NATO or OCCAR standards, further adjustments may still be required to meet the specific requirements of a particular nation.**

Because of these differences, countries often rely on formal bilateral agreements or programme-specific security arrangements to support the mutual recognition of security measures in operational contexts. These arrangements help bridge the gap between the shared international baseline and the additional national requirements that may apply to restricted-level information.

The impact on cloud technologies

Fragmented national regulations create significant obstacles for defence projects that use cloud technologies. When RESTRICTED-level data must be stored or processed in a shared cloud environment, it can be difficult to deploy a single standardised security solution across all participating countries. Instead, the cloud architecture often needs to be adapted to meet the strictest requirements of participating national authorities, resulting in highly customised architectures that can be cumbersome and costly.

In practice, a contractor may be required to host data in separate, isolated cloud instances, each configured to comply with the rules of different national authorities, for example, by using BSI-approved encryption products for Germany. This reduces the efficiency and scalability normally associated with a unified cloud environment.

As a result, **regulatory complexity can slow the adoption of modern cloud-native services.** Defence programmes may be forced to rely on less efficient on-premises systems or build expensive custom cloud infrastructure. Ultimately, **this fragmentation can limit Europe's ability to deploy integrated, interoperable and agile digital defence solutions.**

The impact of AI on defence

Regulatory fragmentation affects cloud technologies, but it can create even greater challenges for the development and deployment of AI in defence. While the EU's AI Act does not apply to AI systems developed or used exclusively for military, defence or national security purposes, each country, including Germany, France and Spain, applies its own national governance frameworks and security requirements for how AI systems can be trained, validated and used. This **creates divergent approaches to the governance and deployment of AI in defence environments.**

For example, an AI system trained on Diffusion Restreinte (DR) data in France may not be directly usable in Germany. The logging, auditing, and data-access rules required by French authorities may not fully align with the security controls applied under the frameworks of Germany's Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI). Even if the algorithms themselves are similar, the underlying data governance and security requirements can diverge significantly.

International standards for AI training and development, such as ISO/IEC 42001, can help reduce barriers to joint development by providing structured governance frameworks for AI systems. However, **fragmented national approaches can slow innovation, increase costs and encourage the development of nationally isolated AI solutions.** This can undermine interoperability and limit the ability of multinational forces to benefit from shared, high-performance AI capabilities.

In some cases, the absence of widely adopted technical standards further complicates the development and deployment of defence AI systems. Strengthening engagement between industry, technical experts and standardisation bodies can help ensure that emerging standards support interoperability while reflecting operational requirements in defence environments.

Summary of regulatory divergence

The examples discussed in this annex highlight how national security frameworks, while designed to protect sensitive information, can lead to differing technical requirements, access procedures and different understandings of restricted-level data. These differences do not necessarily reflect conflicting security objectives, but they can introduce operational complexity when multiple national systems interact within a single multinational programme. Table 3 provides a consolidated overview of the most relevant divergences identified across national and international frameworks.

Table 3. Comparative summary of regulatory divergences across national and international frameworks

Entity	Technical Requirements	Data Access Model	Conceptual Classification
Germany (VS-NfD)	Relatively prescriptive; includes approval or certification of specific hardware and software by the Federal Office for Information Security (BSI).	Structured role-based access management with strict controls and audit mechanisms.	Formally classified as the lowest tier of national classified information, requiring formal secrecy procedures.
France (Diffusion Restreinte)	Focuses on broader principles and certification standards (e.g., ANSSI) rather than mandating specific products.	Relies more on personnel-based authorisation linked to system homologation and the "need-to-know" principle.	Categorised as "sensitive, unclassified information," distinct from higher-level classified defence secrets.
Spain (Difusión Limitada / Reservado)	Less publicly detailed; often relies on bespoke, project-specific security protocols.	Emphasises manual, case-by-case approval by national security officers.	Used in multinational cooperation as a national reference point for restricted-level information, while remaining governed by national procedures.
NATO / OCCAR	Provide baseline security principles and interoperability requirements agreed by participating nations.	Nations may apply stricter national requirements beyond the shared baseline.	NATO/OCCAR RESTRICTED provide commonly recognised baseline classifications across members.
All Nations (Cloud Hosting)	Divergent national rules often prevent the deployment of a single shared cloud solution.	–	–
All Nations (AI Development)	Divergent governance and lifecycle requirements for AI (training, validation, deployment) can create isolated development environments.	–	–

6. A federated and layered architecture

In the medium term, a **federated and layered model for defence data and systems offers a realistic and implementable alternative.** Instead of requiring countries to adopt a single system, it enables each nation to retain authority over its own data and security infrastructures while operating within a shared, secure framework structured around a **data** layer, a **service** layer and an **application** layer. EU projects such as AEROSEC may help explore and validate such architectural approaches.

This **model has two key components:**

1. **A Federated Security Model:** Nations maintain their own secure data networks while adopting a common framework for controlled data exchange based on standardised Application Programming Interfaces (APIs) and data formats. This allows systems to interoperate more effectively while ensuring that each nation retains full ownership and sovereignty over its data. The model is not intended to prescribe national choices regarding localisation or infrastructure. Rather, it illustrates how interoperability can be supported while preserving national authority over sensitive data and security decisions.
2. **A Layered Architecture.** The model is structured around three functional layers:
    - **The National Data Layer,** where highly sensitive, nationally governed information remains under full national sovereignty and subject to national security rules.
    - **The Federated Service Layer,** providing standardised interfaces, shared services and trusted exchange mechanisms that allow systems to interoperate while preventing uncontrolled data transfers.
    - **The Application Layer,** where mission-specific tools, including command-and-control systems, simulation platforms and AI applications, can operate across Member States while supporting cross-border collaboration.

This approach supports interoperability without imposing structural changes on national systems and provides a flexible foundation for advanced digital capabilities. It is particularly relevant in two domains of strategic importance:

- **AI development,** where federated learning enables models to be trained across nationally controlled datasets without transferring raw data, preserving sovereignty while accelerating capability development.
- **Cloud deployment,** where the federated layer allows countries to use their preferred national or sovereign cloud providers while still enabling cross-border collaboration and shared mission environments.

However, this federated and layered model is proposed at the conceptual and policy levels, based on recurring operational patterns observed across multinational defence programmes, rather than as a fixed technical blueprint. Its concrete technical design, requirements and validation should be further assessed in close cooperation with Ministries of Defence and relevant national authorities. In this context, pilot initiatives such as AEROSEC provide an appropriate framework for testing, refining and operationalising such architectures based on real-world use cases and security constraints.

Illustrative example:
Imagine Germany, France and Spain collaborating on a multinational drone programme. Each country keeps its sensitive design, testing and operational data within its own secure national environment. Through a federated and layered architecture, however, engineers and programme teams can still exchange selected data, use shared digital tools and coordinate design and testing activities through common interfaces. This reduces duplication, supports secure cross-border collaboration and allows the programme to move forward without requiring all partners to adopt a single national system.

7. Cross-sector insights

As Europe strengthens its defence technological and industrial base, it is valuable to draw lessons from sectors that have already addressed comparable challenges of regulatory divergence, mutual recognition and cross-border digital cooperation. This **section highlights examples from other highly regulated sectors that help translate the study's recommendations into practical governance approaches.** A cross-sector example (see Table 4) demonstrates how mutual recognition and shared procedural standards have been implemented in other EU policy domains.

Cross-sector best practice: lessons from PSD2 for reducing fragmentation

The following **example from the EU financial sector** illustrates how another highly regulated domain has reduced fragmentation through shared standards and trusted cross-border mechanisms. Under the revised **Payment Services Directive** (PSD2), the **European Banking Authority** (EBA) introduced harmonised guidelines and a common licensing framework supporting cross-border financial services within the internal market. **While the defence sector is fundamentally different, the PSD2 experience demonstrates how coordinated guidance and mutual recognition mechanisms can contribute to a more predictable environment for cross-border cooperation.** The example is not proposed as a direct model for defence, but as an illustration of how common procedural guidance and structured cooperation between authorities can improve predictability in complex cross-border environments.

Table 4 summarises key features of this governance model and highlights elements that may offer useful insights when considering future approaches to RESTRICTED-level digital capabilities in defence.

Table 4. PSD2 passporting: a cross-sector illustration of procedural coordination

Illustrative example from the EU financial sector relevant to defence cooperation		
OVERVIEW	**KEY MECHANISM**	**IMPACT**
The EU financial sector illustrates how fragmented national procedures can be aligned through common rules and mutual recognition mechanisms. Under the PSD2 licensing scheme, the European Banking Authority introduced harmonised guidelines for national authorities assessing licence applications from financial technology (fintech) companies. These guidelines support: ▶ a shared interpretation of requirements across Member States; ▶ structured communication and cooperation between national authorities; ▶ a more predictable and consistent licensing procedure.	A central feature of PSD2 is "passporting". Once a licence is granted in one Member State, a company may provide services across the EU without repeating the full licensing process in every jurisdiction.	By standardising procedures and encouraging mutual recognition, PSD2 significantly reduced barriers to cross-border activity within the financial sector. Fintech firms are able to scale more easily across the EU and new entrants, particularly SMEs, can plan investments with greater regulatory predictability.

While PSD2 shows how coordinated rules and mutual recognition can reduce fragmentation in certain regulated sectors, applying similar mechanisms to defence requires careful consideration. **Defence and national security frameworks remain under national competence and security requirements may differ significantly between Member States.** Nevertheless, experience from other regulated domains suggests that **mutual recognition mechanisms are most effective when supported by clear governance structures, trust between authorities and practical benefits for participating actors.**

Standardisation has played a comparable role in other sectors by providing common technical specifications that **enable interoperability, facilitate conformity assessment and accelerate the deployment of new technologies.** Similar approaches could support the development of interoperable digital capabilities in European defence cooperation.

8. Multinational digital capability pilot AEROSEC project

Building on the White Paper of the Aeronautics and Security Working Group of the Alliance for Cloud, titled *"Framework of Functional Requirements for Supporting Cloud- and Edge-Based Co-Design and Collaboration for European Defence Programmes,"* a multinational digital capability pilot project has been launched to design a **Highly Secure Multi-Cloud Platform (HSMP).** The objective of this initiative is to enable the secure handling of **EU RESTRICTED, NATO RESTRICTED, OCCAR RESTRICTED and National Equivalent Official (NEO)** data, allowing European defence stakeholders to collaborate more efficiently in shared digital environments.

Strategic vision

AEROSEC is a European initiative designed to facilitate and standardise the way defence programmes collaborate in a secure, multi-cloud digital environment. Today, many multinational defence programmes must establish dedicated secure networks and obtain separate accreditation for digital tools and environments. This process often leads to delays, additional costs and operational inefficiencies. AEROSEC seeks to address this challenge by developing a Highly Secure Multi-Cloud Platform that enables agile, secure and sovereign collaboration in the development of next-generation defence systems, while reducing the need to recreate secure infrastructures for each programme.

Consortium and partnerships

The project is coordinated by Dassault Systèmes and brings together major European defence and technology actors, including Dassault Aviation, Airbus Defence and Space, Indra, Leonardo, Cefriel and OUTSCALE, alongside seven European universities. Supported by the European Commission (DG CONNECT and DG DEFIS), national Ministries of Defence, national cybersecurity authorities and the European Commission Security Authority, AEROSEC runs from 2025 to 2028 with a budget of approximately €27 million under the Digital Europe Programme. The initiative combines industrial expertise, academic research and public governance within a collaborative European framework.

Solution and innovation

AEROSEC aims to deliver a reusable, secure digital backbone built around:

- a trusted **EU RESTRICTED network;**
- **federated identity and access management;**
- **multi-cloud collaboration services** supporting standardised Common Work Environments for defence programmes.

The project will develop **three prototypes** designed to support the handling of EU RESTRICTED-level information and demonstrate:

- centralised identity and access management and secure data-sharing mechanisms;
- secure multi-cloud service capabilities;
- secure programme co-design environments based on **Model-Based Systems Engineering (MBSE).**

These capabilities aim to enable more efficient cooperation across industrial partners and supply chains involved in multinational defence programmes. More broadly, initiatives such as AEROSEC can help provide the type of coordinated testing and validation environment that Europe needs if digitally enabled capabilities are to move more rapidly from the pilot phase to scalable operational use across multinational programmes.

9. Strengthening the EU Defence Readiness Omnibus

To address the persistent challenges of regulatory fragmentation, the **EU Defence Readiness Omnibus should prioritise measures that improve interoperability rather than focusing solely on procedural simplification.** While fully respecting national frameworks, many of which reflect legitimate sovereignty and security considerations, the objective should be to **create an enabling environment that facilitates effective cross-border cooperation and operational efficiency.**

Experience from numerous cross-border projects shows that **formal rules alone are not sufficient.** If they are not accompanied by coordinated interpretation and active engagement from national authorities, even well-designed provisions can lead to inconsistent implementation. In many Member States, security, export-control and procurement authorities operate with limited internal coordination, creating delays, contradictory guidance and uncertainty for industry actors involved in multinational programmes.

The **Omnibus** therefore **offers an important opportunity to promote structured coordination both within Member States and between national authorities and industry,** ensuring that shared rules are applied coherently in practice. It also provides a policy basis for practical mechanisms such as **enhanced mutual recognition of security controls** and **federated digital security architectures,** which are core recommendations of this study. To achieve this in practice, however, simplification should be accompanied by **clearer pathways for the testing, validation and scaling of digital and dual-use technologies across borders.** Without such pathways, promising capabilities may continue to face delays between development and deployment.

Recent analysis[13] of European defence procurement suggests that **innovation support alone is not sufficient.** If start-ups, SMEs and other non-traditional suppliers are to scale and contribute meaningfully to defence capabilities, they must also have **access to credible procurement pathways and contracts.** This reinforces the argument that reducing regulatory fragmentation is important not only for participation, but also for the validation, uptake and scaling of innovative technologies in European defence.

13 Kapstein, E., Ospital, J., & Wolff, G. B. (2026, March). *Reforming European defence procurement to boost military innovation and startups* (Policy Brief 04/26). Bruegel. https://www.bruegel.org/policy-brief/reforming-european-defence-procurement-boost-military-innovation-and-startups

Simplification alone is not enough. Europe also needs clearer pathways for the testing, validation and scaling of digital and dual-use technologies across borders.

Fostering innovation: integrating non-traditional suppliers

To meet the urgent need for rapid technological advancement in defence, the **EU must also reduce regulatory barriers that limit the participation of start-ups, SMEs, digital-first companies and academic institutions in multinational defence programmes.** These actors frequently develop cutting-edge dual-use capabilities, including advanced Artificial Intelligence and Machine Learning (AI/ML) models, secure cloud technologies, advanced software platforms and innovative hardware solutions. However, many of these innovators face significant obstacles when attempting to participate in defence projects, as fragmented national security frameworks can be complex, costly and time-consuming to navigate.

Improving regulatory predictability and reducing unnecessary procedural barriers would allow these emerging actors to contribute more effectively to Europe's defence innovation ecosystem, strengthening both the technological competitiveness and the resilience of the European Defence Technological and Industrial Base (EDTIB). This is particularly important where innovative companies are developing mature digital solutions ready for testing, validation or rapid fielding, but struggle to scale because approval pathways and cross-border deployment conditions remain too fragmented. Better alignment among validation environments, interoperability efforts and capability demand would help more of these solutions achieve operational uptake.

DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies.

Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations which are global leaders in their field of activity, as well as national trade associations from across Europe.

www.digitaleurope.org

@DIGITALEUROPE

@digitaleurope_org

DIGITALEUROPE

@DIGITALEUROPEvideo

www.digitaleurope.org