Recommendations for the revision of the Defence and Security Directive (2009/81/EC)

I. Introduction

The defence and security procurement terrain in the European Union faces unprecedented challenges. Russia's full-scale invasion of Ukraine, intensifying hybrid threats, supply chain vulnerabilities and the accelerating pace of technological change - particularly in artificial intelligence, cybersecurity and advanced digital systems - have fundamentally altered the strategic environment for European defence and civil security. These developments underscore an urgent need to modernise Directive 2009/81/EC to strengthen the European Defence Technological and Industrial Base (EDTIB), ensure strategic autonomy and technological sovereignty, and enhance the operational readiness of Member States.

The 2016 Commission evaluation of the Directive found that while the legal framework is fundamentally sound, significant gaps remain in implementation, guidance, and alignment with evolving capability needs. Key findings include: (a) uneven uptake across Member States; (b) limited use for high-value, strategically complex defence systems; (c) insufficient clarity on exclusions and exemptions, particularly regarding government-to-government contracts and Article 346 TFEU; (d) underperformance in opening supply chains to SMEs and new entrants; and (e) lack of clear interface with the 2014 public procurement directives.

Insights from Corvers' recent Innovation Uptake Report on defence and security procurement, together with findings from the CERIS civil security and resilience community on strategic autonomy, critical technologies and innovation gaps, further underline the need for targeted reforms to make the Directive more innovation-conducive across the full capability lifecycle.

Corvers' 2026 recommendations on innovation procurement across all public procurement directives, informed by best practices in the United Kingdom, United States, Canada, South Korea, Japan and China, identified additional reform imperatives: the need for uniform innovation - procurement definitions, clearer R&D services exemptions, innovation-friendly intellectual property regimes, support for SMEs and start-ups, and strategic security-related exemptions grounded in European autonomy and technological sovereignty. This consultation response applies the following proposed changes specifically to 2009/81/EC, whilst addressing the Commission's statutory review requirement under Article 73(2).

In this context, the following recommendations are proposed for the revision of Directive 2009/81/EC.

II. Recommendations

Corvers strongly recommends that the revision of the Defence and Security Directive (2009/81/EC) Directives addresses twelve concrete topics regarding: (1) Clarification of scope and relationship with 2014 directives; (2) Uniform definition of innovation procurement; (3) Innovation principle and value engineering; (4) Artificial Intelligence, digital infrastructure and critical technologies; (5) Defence-specific Intellectual Property Rights (IPR) regime; (6) Certifications for research and innovation excellence; (7) Market analysis, open market consultation and transparency; (8) Cooperative and joint procurement; (9) R&D services exemption - simplification and clarity; (10) Security-related exemptions, strategic autonomy and critical technologies; (11) Digitalisation - secure identity, data sharing and digital marketplace; and (12) Subcontracting and SME/start-up participation.

1. Clarify scope and relationship with 2014 directives

The current Directive does not explicitly address mixed defence/civil contracts or clearly demarcate when 2009/81/EC applies versus Directives 2014/24/EU and 2014/25/EU. This ambiguity creates administrative burden and reduces transparency and competition in the defence market.

It is recommended to:

- ***Insert a new recital:*** Explicitly stating that for contracts where defence or sensitive security is the primary subject-matter and specific security-of-supply or security-of-information risks are present, Directive 2009/81/EC should be regarded as the *lex specialis*, even where procedures are aligned with the 2014 directives, and this principle should be reflected in the conflict-of-laws rule in Article 3.
- ***Adopt a clear conflict-of-laws rule***: Where a contract relates to mixed defence and civil procurement, 2009/81/EC shall apply if the principal subject-matter falls within defence or sensitive security and the security-related requirements of the Directive are relevant; otherwise, 2014 directives apply. Cases related to critical infrastructure and cybersecurity shall fall under the scope of security, and, for the avoidance of doubt, services and systems falling within the scope of the NIS-II Directive (including essential and important entities in defence-relevant sectors) should be treated as potentially defence-relevant critical infrastructure when determining whether 2009/81/EC ought to apply.
- **Explicitly recognise defence-relevant critical infrastructure**, including dual-use assets with clear defence or sensitive-security implications, **as a legitimate basis** for applying the defence and security procurement regime, in order to avoid fragmentation and legal uncertainty across borders.
- ***Provide guidance (i.e. Commission notice) with worked examples illustrating***: (a) purely defence contracts; (b) mixed contracts (e.g. logistics with defence and civil elements); (c) civil contracts with incidental defence aspects; and (d) contracts for civil security where sensitive security criteria apply.
- ***Amend Article 3***: In order to make mixed-contract determination criteria explicit and include reference to the security-risk assessment that justifies use of 2009/81/EC rules rather than 2014 alternatives.

2. Uniform definition of innovation procurement

The Directive lacks a clear, cross-cutting definition of innovation procurement, hindering the consistent use of flexible procedures for R&D, Pre-commercial Procurement (PCP) and Public Procurement of Innovative solutions (PPI) across Member States.

It is essential that the basic taxonomy for R&D, PCP and deployment/scale-up phases is coherent across all EU procurement directives, so that innovation procurement concepts are applied consistently in both the defence-specific regime and the 2014 public procurement directives.

The recommended actions are:

- ***Mirror the innovation-procurement definitions:*** From the EU Innovation Act and Corvers' 2026 recommendations for the revision of the 2014 public procurement directives into the recitals and a new definitions section (amend Article 1) of 2009/81/EC:
    - ***Innovation procurement*** encompasses all procurements purchasing research and development (R&D), innovative supplies, services, works or combinations thereof.
    - ***R&D procurement*** includes fundamental research, applied research and experimental development as defined in Recital 13.
    - ***Public Procurement of Innovative solutions*** means procurement of goods, works or services that incorporate technologies or operational approaches not yet widely available in the defence and security market.
- ***Explicitly confirm***: That innovation procurement in defence covers the full capability lifecycle, from early-stage research through first-of-a-kind deployment and limited production.
- ***Ensure alignment:*** With definitions used in Directive 2014/24/EU (and 2014/25/EU) so that suppliers understand consistent terminology across all procurement directives.

3. Innovation principle and value engineering

The Directive does not articulate an explicit "innovation principle" - a commitment that procurement procedures should neither obstruct innovative solutions nor impose unnecessary barriers to innovative suppliers. Value engineering (post-award modifications to incorporate new innovations during contract performance) is not clearly permitted.

The Defence Readiness Simplification Omnibus signals an intention to introduce the open procedure into the defence procurement regime. While simplification and greater transparency are important, the open procedure, by design, presupposes a high level of ex-ante disclosure of requirements, technical specifications and selection/award conditions that may be difficult to reconcile with the handling of sensitive and classified information in defence and sensitive security procurement. Before embedding the open procedure into the revised Directive, the Commission should assess whether this tool is genuinely compatible with security requirements or whether more tailored procedures (such as the restricted procedure, negotiated procedure with prior publication or competitive dialogue) are better suited to balancing transparency, competition and national-security concerns.

The recommended actions are:

- ***Insert a new recital:*** Affirming that public procurement in defence and security

should actively encourage innovation wherever feasible and should not obstruct innovators or innovative solutions, reflecting the language of the EU Innovation Act and Corvers' recommendations for the 2014 public procurement directives. The innovation principle should in particular support faster demand-side adaptation for AI-enabled and other digital capabilities, enabling contracting authorities to test, scale and deploy battle-proven solutions at the speed required by next-generation warfare, including lessons learned from Ukraine.

- ***Insert a provision on modification of contracts as in Article 72 of Directive 2014/24/EU* and explicitly allow value engineering clauses**: contracting authorities may accept modifications to contract performance based on clear, precise and unambiguous value engineering provisions, provided that such modifications:
  - Do not fundamentally alter the contract's scope or security objectives;
  - Remain cost-neutral or cost-saving;
  - Are applied transparently and non-discriminatorily;
  - Do not compromise security of information, security of supply or interoperability.
- ***Provide Commission guidance***: On drafting value engineering clauses in defence and security contexts, with worked examples addressing cost, schedule, performance and security trade-offs.

4. Artificial intelligence, digital infrastructure and critical technologies

The Directive predates the emergence of AI, cloud computing, quantum computing, data sovereignty and space-based services as critical defence and security enablers. As the CERIS report and Competitiveness Compass emphasise, technological sovereignty and reduced external dependencies in these domains, including resilience against post-quantum cryptographic threats, are now strategic imperatives. Operational experience from Ukraine and other theatres shows that AI-enabled systems evolve in months rather than years, and that procurement rules must allow rapid iteration and scaling of combat-proven solutions. The Directive must explicitly address procurement of AI systems, secure data infrastructures, cybersecurity services and cloud services whilst supporting EU autonomy.

The recommended actions are:

- ***Insert recitals:*** Recognising that artificial intelligence, advanced cybersecurity, quantum computing cryptography, secure cloud and data services, space-based services and autonomous systems are now critical to defence and security capability. Procurement of such technologies must be designed to:
  - Reduce dependencies on extra-EU providers in sensitive domains;
  - Support EU technological sovereignty and strategic autonomy;
  - Ensure data security, algorithmic transparency and human oversight;
  - Enable interoperability across Member States and NATO.
- ***Extend the definition of "security of supply" and "security of information" (Articles 23 and 22):*** To explicitly include requirements for:
  - Data residency (processing and storage within the EU or allied jurisdictions);
  - Algorithmic transparency and explainability for AI-enabled systems;

- Protection against high-risk supply chain dependencies in semiconductors, cloud infrastructure and critical software, including: mandatory disclosure by bidders of their supply chains and critical single-source dependencies; multi-sourcing obligations for critical components where feasible; and, for systems where chip dependency constitutes a direct security risk, the possibility for contracting authorities to use minimum EU or allied manufacturing or packaging shares as award criteria or contract conditions, in line with applicable international obligations;
- Cyber-hygiene and resilience standards aligned with EU cybersecurity law;
- Trustworthy AI requirements for defence applications, taking into account emerging EU frameworks such as the European Defence Agency's work on the trustworthiness of AI in defence (including reliability, robustness, human oversight and auditability) and ensuring consistency with horizontal EU AI regulation.

- ***Clarify that security-related exemptions in EU law, including but not limited to Article 346 TFEU and the specific exemption provisions in the Defence and Security Directive, explicitly extend to AI systems and critical digital infrastructure in clearly defined, high-risk cases. These should include, for example, situations where:*** The procurement concerns autonomous systems, AI-enabled decision support tools or command-and-control systems whose compromise would directly affect mission-critical decision-making or use of force;
  - Cloud or data services handle classified information, operational intelligence, or highly sensitive personal data, such that routing or storing the data through third-country infrastructure would create unacceptable security risks;
  - Supply chain integrity or third-country technological dependencies in semiconductors, cloud infrastructure or critical software could enable disruption, remote interference, or unwanted access by hostile actors, and proportionate use of exemptions is necessary to mitigate these risks (for example, limiting procurement to EU or closely allied providers, or imposing stringent localisation and security-of-supply conditions).

These exemptions should remain exceptional, applied only where genuinely necessary and with clear, documented justification, to avoid abuse or unnecessary over-use.

- ***Encourage cross-border innovation procurement:*** For AI and digital defence capabilities through cooperative procurement mechanisms (see Recommendation 8), including joint testbeds, regulatory sandboxes and pre-commercial procurement (PCP) to identify and de-risk promising technologies before full deployment.
- ***Support R&I excellence certification:*** (see Recommendation 6) for suppliers of AI systems and critical digital services, recognising certifications from EU-funded R&I programmes (i.e. Horizon Europe, European Chips Act, Digital Europe, and initiatives under the EU Quantum Strategy) as evidence of technical capacity.

5. Defence-specific IPR regime

Current Directive language on IPR is minimal. Clear rules on ownership, usage rights, trade-secret protection and data rights are essential to foster innovation in defence and security, especially for AI models, training data and derived intelligence datasets, whilst protecting classified information and security interests.

The recommended actions are:

- ***Amend Article 20:*** Insert new provisions requiring that tender documents and contract terms explicitly define:
  - ***Default IPR ownership:*** Intellectual Property, including patents, designs, copyrights and know-how, shall remain with the contractor by default, unless justified exceptions apply (see below).
  - ***Usage rights:*** The contracting authority and other authorised users within the Member State shall receive royalty-free, irrevocable usage rights sufficient to operate and maintain the procured solution for its intended defence or security purpose.
  - **Upgrade and modification rights:** Where appropriate on a case-by-case basis, the contracting authority and other authorised users within the Member State shall receive sufficient rights to upgrade and modify the procured solution for its intended defence or security purpose, without requiring a transfer of ownership of the underlying intellectual property.
  - ***Data rights:*** For AI systems, data-intensive services and software, clear allocation of ownership and access rights to training data, derived datasets, models and algorithms.
  - ***Trade-secret protection:*** Contractors' trade secrets and confidential business information shall be protected during procurement, implementation and post-contract phases.
- ***Exceptional transfers of IPR ownership:*** May be justified and required only in documented cases where:
  - Open licensing or public-domain requirements arise from EU-funded research obligations;
  - Counter-intelligence, security or privacy concerns preclude commercialisation of the contractor's IP;
  - Exclusive use by the contracting authority or Member States is operationally necessary (e.g. unique sovereign capability).

Such transfers must comply with a "comply or explain" standard: Contracting authorities must justify transfer requirements in advance and document the proportionality assessment.

- ***Subcontractor IPR:*** Contracting authorities must ensure that prime contractors apply the same IPR principles to subcontractors, allowing subcontractors to retain ownership and usage rights except where security classification or exclusive-use requirements apply and are justified.
- ***Provide Commission guidance:*** On drafting IPR clauses in innovation defence procurement, including AI and critical software, with examples that balance innovation incentives, classified information protection and security interests.

6. Certifications for research and innovation excellence

Evidence of prior success in EU-funded research and innovation can streamline qualification processes and reduce barriers for SMEs and start-ups to participate in defence innovation procurement.

The recommended actions are:

- ***Amend Article 42:*** (Technical and Professional Ability) to recognise that successful

completion of relevant EU-funded R&I programmes and certifications, such as the EU Seal of Excellence, Horizon Europe grant awards, certifications from EU-funded research consortia, and recognition in the European Repository of Research and Innovation Results, may qualify as evidence of professional R&I capacity in innovation procurement.

- ***Establish a defence and security innovation excellence registry:*** Encourage creation of a database (hosted by the Commission or European Defence Agency) recording completed EU-funded defence and security R&I projects, allowing contracting authorities to verify contractor experience and capabilities with ease. Building on and integrating existing defence-related databases and platforms (for example those operated by the European Defence Agency), the Commission and EDA should support the creation of a harmonised, EU-level registry that consolidates data on completed EU-funded defence and security research and innovation projects and their suppliers. The registry should:
    - Integrate and standardise relevant data from existing systems to improve consistency and data quality and create incentives for Member States and beneficiaries to supply accurate, up-to-date information.
    - Be hosted or coordinated by the EDA< but designed so that filtered, role-based access can be granted not only to Member State defence ministries but also to other authorised contracting authorities involved in defence and security procurement.
    - Allow authorised users to identify suppliers with proven defence and security R&I performance, while responding classification constraints and protecting commercially sensitive information.
    - Participation in, and regular updating of, the registry could be encouraged through soft-law measures and by recognising registry entries as standard evidence of professional and technical capacity in relevant procurement procedures.
- ***Clarify and encourage use of simplified selection criteria for SME innovators:*** The Directive should explicitly confirm, and encourage, the possibility for contracting authorities to apply proportionate, lower selection thresholds for companies that have successfully participated in relevant EU-funded defence and security research and innovation programmes (for example Horizon Europe, EDF or similar schemes). Successful completion of such projects should be recognised as strong evidence of technical and professional capacity, allowing contracting authorities, where appropriate, to reduce standard turnover and experience requirements so that innovative SMEs and start-ups can participate in "normal" procurement procedures. This would provide a clearer pathway form EU-funded R&I to subsequent procurement opportunities, giving smaller innovators a tangible incentive to invest in EU programmes by demonstrating that their project track record can directly support their qualification and capability claims in later tenders.

7. Market analysis, open market consultation and transparency

Strategic market engagement, understanding the defence technology landscape, identifying promising innovators and solutions, and signalling procurement opportunities, is essential to build competitive, innovative supply chains and reduce fragmentation.

The recommended actions are:

- ***Amend the procedures chapter:*** To require that before launching major innovation-

driven procurements (particularly for AI, digital and critical technologies), contracting authorities shall:

- Conduct market research/State-Of-The-Art (SOTA) analysis covering EU and international suppliers, existing capabilities and emerging solutions;
- Perform a preliminary market consultation with industry to identify technical feasibility, cost, schedule and supply chain constraints, and to gather input on procurement clauses (i.e. security, IPR, data, performance).

- ***Use Tenders Electronics Daily (TED) notices and standardised fields:*** Introduce a new TED notice type for announcing preliminary market consultations (as recommended by Corvers' proposal for reform of the 2014 directives) and require contracting authorities to indicate in contract notices whether the procurement is for innovation, using a standardised "innovation procurement" field in TED.
- ***Enhance cross-border visibility:*** Make market consultation notices available for a minimum of 30-45 days to allow cross-border supplier participation; encourage notifications in multiple EU languages where feasible.
- ***Share findings:*** Encourage contracting authorities to summarise market consultation results (without revealing confidential bidder information) in the procurement documentation, helping to demonstrate that the Directive's objectives (i.e. competition, innovation, EDTIB strengthening) are being pursued.

8. Cooperative and joint procurement

The Directive does not contain explicit provisions on joint procurement (multiple Member States conducting a single procedure and awarding contracts jointly). The 2016 evaluation found the Directive does not hinder cooperation, but guidance is sparse. Joint procurement is increasingly vital for innovation, cost-sharing and supply chain resilience in complex defence systems, and the Directive could also draw on lessons from the EU's joint procurement arrangements during the COVID-19 pandemic, which can apply *mutatis mutandis* in the defence and security field.[1] In practice, many cooperation needs concern non-defence or dual-use projects (for example in cyber, critical infrastructure, space or emerging technologies) that nonetheless raise sensitive security, innovation and industrial-base questions, and the revised framework should explicitly accommodate such projects within cooperative procurement tools.

The recommended actions are:

- ***Insert a new chapter (or section) clarifying cooperative procurement:***
  - ***Definition:*** Cooperative procurement encompasses joint procurement (a single procedure managed by one or more Member States, with contracts awarded jointly) and coordinated procurement (aligned specifications and procedures across Member States, but separate contract awards).
  - **Joint procurement is explicitly permitted** for defence and security contracts, subject to the Directive's principles, and without requiring each Member State to comply separately with its domestic procurement rules. The applicable procurement rules and allocation of responsibilities in joint procedures should be clarified at EU level, including through guidance on which national rules apply (for example under a lead-buyer model) and how participating authorities can rely on a single set of procedural rules.

[1] See A. Georgopoulos, "The EU's Joint Procurement Agreement in the Light of COVID-19: Learning the Correct Lessons from the Pandemic and Identifying Actions for Improvement", SSRN, 20 November 2021, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3981564.

- ***Eligible entities:*** Member States, their contracting authorities, the European Defence Agency, and organisations established under EU law or international defence arrangements (e.g. OCCAR, NATO bodies) may jointly procure.
- **Enable joint R&D follow-on deployment:** Align with Corvers' recommendation for the reform of the 2014 directives on Article 32(3)(a) and GPA Article XIII(f): allow groups of contracting authorities that jointly procured R&D services (e.g. Pre-Commercial Procurement) to jointly purchase innovative products or services, counting full R&D costs (including suppliers' own R&D investment) as a baseline, and purchasing up to 10 times the R&D contract value without triggering a new full competitive procedure, provided:
  - The initial R&D was awarded competitively;
  - The follow-on procurement remains limited to solutions demonstrating Technology Readiness Level 9 (mature for production);
  - Pricing does not incur full cost recovery of R&D investments.

- ***Support structures for cooperative procurement:*** Provide Commission guidance and template agreements covering: legal frameworks (lead-buyer model, consortium models), financing mechanisms, intellectual property allocation among participating states, subcontracting rules, dispute resolution and security information handling.
- **Promote harmonised operational rules for handling classified information in cooperative procurement:** Including mechanisms to ensure that, where information or technologies are classified in one Member State, equivalent classification and approval standards can be applied in other participating Member States for the purposes of joint or cooperative procedures. This should aim to reduce fragmentation arising from divergent national practices on who may access classified information, under what conditions, and how it can be shared with other authorities or companies.
- **Create an EU Cooperative Defence Procurement Portal:** Develop, as a dedicated module or functional extension of the existing Tenders Electronic Daily (TED) system, a central repository where Member States can post planned cooperative procurements, find willing partners, exchange lessons learned and access templates. This module should use standardised notice templates tailored to cooperative and joint defence and security procurement, so that it builds on and upgrades existing TED infrastructure rather than creating a completely separate platform.

9. R&D services exemption – simplification and clarity

Article 13(j) contains a double negation ("*contracts which are not for research and development services*" are subject to the Directive unless…) - a formulation that creates ambiguity. Pre-Commercial Procurement (PCP), whilst legally permissible, lacks explicit recognition. EU Treaty principles must clearly apply.

The recommended actions are:

- ***Rewrite Article 13(j):*** To eliminate the double negation. Proposed new text:

"This Directive does not apply to research and development service contracts where:

- The benefits accrue exclusively to the contracting authority for its own use in the conduct of its own affairs;
- The service is wholly remunerated by the contracting authority; and
- The contracting authority has not made the results public or made them

available to third parties in a manner that would constitute a commercial supply or service."

- **Explicitly state:** in the Directive (new recital or amended Article 13(j) that PCP; market-testing, technical validation and limited production of innovative solutions prior to full commercialisation, is encompassed within the R&D services exemption, provided the above conditions are met.
- ***Affirm EU Treaty principles:*** Clarify that invocation of the R&D exemption does not exempt contracting authorities from the Treaty principles of non-discrimination, equal treatment, proportionality and transparency. Use of the exemption must remain limited to genuine research and development; it cannot be used to avoid the Directive's competitive procedures for procurement of production-ready goods or services.
- **Provide Commission guidance:** On the boundary between research and development (exempted) and procurement of innovative products or services (subject to the Directives), including worked examples for defence technology domains, and ensuring that this guidance is consistent and aligned with the definitions and explanations used in the 2014 public procurement directives for R&D and innovation-related contracts.

10. Security-related exemptions, strategic autonomy and critical technologies

The Directive and Article 346 TFEU permit exemptions on grounds of "essential security interests," but lack clarity on what this means in practice, how to justify exemptions, and how to balance security with competition and transparency. New security challenges (supply chain resilience, technological dependencies, hybrid threats) require more structured coordination rather than a new EU-level definition.

The recommended actions are:

- ***Encourage a common understanding of "essential security interests" in a new recital:*** A recital should illustrate, in a clearly non-exhaustive way, typical situations where Member States may consider essential security interests to be at stake, for example:
    - Protection of military capabilities, classified information and intelligence sources;
    - Continuity of supply for critical defence equipment and services, especially where single-source dependencies exist;
    - Technological sovereignty and autonomy in critical domains (AI, semiconductors, cloud, space, cybersecurity);
    - Protection of critical infrastructure whose disruption would seriously affect defence, security or public order;
    - Protection against supply chain infiltration or compromise by hostile foreign actors;
    - Capacity to respond to armed conflict, terrorism or large-scale public emergencies.

This clarification should expressly state that the list is indicative and non-exhaustive, while confirming that Member States remain responsible for defining their essential security interests in accordance with EU law.

- **Encourage the use of security-justification requirements:** Before using security

exemptions to disapply the Directive, contracting authorities must:

- Document the specific security risk or essential interest at stake;
- Assess proportionality: confirm that the exemption is no broader than necessary to address the identified risk;
- Consider whether less restrictive alternatives (e.g. security-of-supply conditions, security clearances, contractual safeguards) could meet the need whilst preserving competition;
- Provide this justification to the Commission (via the Member State), either publicly or (if the justification itself is sensitive) through a confidential notice.

- ***Encourage European preference for critical technologies where legally possible:*** Where proportionate and compatible with WTO GPA Article XXIII, the Directive should encourage tools such as: Contracting authorities may require that critical defence and security products incorporate a minimum share of EU-originated components or be manufactured/assembled in the EU or allied jurisdictions;
  - Contracting authorities may apply weighted scoring criteria favouring EU supply chains where cost, delivery time and technical performance are comparable;
  - Contracting authorities may mandate multi-source strategies to reduce single-source dependencies, particularly for semiconductors, rare-earth materials, advanced software and cloud services.
- **Encourage coordination with EU strategic-autonomy objectives:** The Directive should reference key Union strategic-autonomy instruments (e.g. the EU Competitiveness Compass and related initiatives) and encourage Member States to align their use of security-related exemptions and procurement strategies with the Union's broader technological-leadership and resilience objectives, without prejudging national competences on essential security interests.
- ***Provide Commission guidance:*** Invite the Commission to develop non-binding guidance – including indicative flowcharts, decision trees and illustrative case studies – on proportionate, transparent use of security-related exemptions, helping contracting authorities to apply them consistently while respecting Member State prerogatives.

11. Digitalisation - secure identity, data sharing and digital marketplaces

Defence procurement remains heavily paper-based and fragmented across Member States. Secure digital infrastructure, including digital identity, encrypted data sharing, secure digital marketplaces, can reduce administrative burden, improve transparency and facilitate cross-border participation whilst protecting classified information.

The recommended actions are:

- ***Enable EU secure digital identity measures:*** Allow and encourage contracting authorities to use eIDAS-compliant digital identity for supplier registration, qualification, tendering and contract performance, with enhanced security requirements appropriate to defence classification levels.
- **Establish secure data-sharing infrastructure:** Create (or use) EU-level secure communication channels (e.g. EUCLID, Ensemble, or successor platforms) for transmission of contract documents, tender submissions, clarifications and award notifications, meeting:

- Encryption and confidentiality standards aligned with EU and NATO classified information regimes;
- Interoperability with Member State national security infrastructure;
- Audit trails and non-repudiation.

- **Harmonised handling of classified information:** In parallel with technical secure-data solutions, the Commission and Member States should work towards more harmonised operational rules for the classification and cross-border sharing of sensitive and classified information in defence procurement, so that solutions cleared for use and marketing in one Member State can, where appropriate, be made visible and accessible to authorised contracting authorities in others.
- ***Develop a secure EU defence digital marketplace:*** Build on existing national e-marketplace models and relevant EU-level databases to create an optional, secure, EU-level digital platform where:
  - Contracting authorities can browse vetted suppliers, their capabilities and past performance;
  - Suppliers can showcase products, services and certifications (with a level of detail appropriate to the sensitivity of information);
  - The marketplace should be interoperable with existing defence-related databases and innovation platforms;
  - Explicitly allow the onboarding of suitable European Innovation Council (EIC) beneficiaries and other dual-use innovators as potential suppliers, subject to security screening and classification constraints;
  - Catalogue information is accessible onto to authorised defence and security procurement officers;
  - Cybersecurity and data protection standards are certified and continuously monitored.
- **Address cybersecurity and digital skills risks:** Mandate that contracting authorities and suppliers implement baseline cybersecurity standards (aligned with NIS2 Directive); provide Commission training and support for digital procurement tools.
- **Flexible reporting requirements:** Allow Member States to report contract award data through secure digital channels and reduce redundancy in TED v. national reporting, provided data is reconciled and published with appropriate security review.

12. Subcontracting and SME/start-up participation

The 2016 evaluation found that Articles 50-53 on competitive subcontracting requirements are rarely used and largely ineffective, while SMEs and start-ups still report barriers to defence procurement participation: excessive financial guarantees, lengthy security clearance processes, complex qualification procedures.

The recommended actions are:

- ***Simplify and de-bureaucratise subcontracting obligations:***
  - Remove the requirement that subcontracting competitions must replicate the main tender process; instead, permit primes to conduct simpler, streamlined competitions for subcontractors above a threshold (e.g. €100,000).
  - Require contracting authorities to set transparent subcontracting targets (e.g. minimum 20-30% for SMEs and start-ups in high-value contracts) and measure performance.

- Require primes to publish subcontracting opportunities with adequate notice (minimum 30 days) on a centralised platform (i.e. TED or the defence digital marketplace).

- **SME and start-up friendly selection criteria:**
  - Amend Article 41-42: For innovation procurements, allow reduced turnover thresholds (e.g. 3 years v. 5 years of trading) and lower financial guarantee requirements for SMEs and start-ups with strong R&I credentials or EU Seal of Excellence.
  - Recognition group capacity: Allow SMEs and start-ups to bid in consortia, with verification of commitment (formal agreements, joint liability provisions) rather than demanding individual financial strength.
  - Accept letters of intent from financial institutions or EU equity instruments as proof of financing capacity, in lieu of historical bank statements.
- ***Accelerated and harmonised security clearance processes:*** Encourage Member States, with support from the Commission and the European Defence Agency, to develop harmonised accelerated security clearance procedures for SMEs and start-ups, so that clearances obtained in one Member State can be more easily recognised or fast-tracked in others. The aim should be to move towards an EU-wide, risk-based approach in which common minimum standards, streamlined processes and mutual recognition mechanisms reduce duplication and delays, while fully respecting national security responsibilities and classification rules.
- **Strengthen EU-supported guidance and matchmaking:** Commission and European Defence Agency should operate matchmaking platforms connecting contracting authorities with qualified SMEs and start-ups; provide training on defence procurement rules, security requirements, contract management and reporting.
- **Improve payment and financing conditions:**
  - Require contracting authorities to impose prompt-payment clauses (e.g. 30 days) in main contracts and ensure these are passed down to subcontractors;
  - Encourage and support alternative financing mechanisms (i.e. supply chain finance, pre-financing) to reduce working-capital burden on SMEs/start-ups in long-term defence contracts.