POLICY BRIEF
November 2025

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES

SMARTER SPENDING TODAY, SAFER SOCIETIES TOMORROW

DIGITALLY-ENABLED CAPABILITIES FOR EUROPEAN DEFENCE

ABSTRACT

This policy brief provides an overview of European digital defence technologies and policy instruments that enable their development and procurement. It analyses cyber warfare, electronic warfare, unmanned systems, and space and communications, as well as cross-cutting enablers, such as artificial intelligence and big-data analytics, quantum cybersecurity and computing.

The policy brief provides a description of four potential areas for improvement in European defence industrial policy: strengthening the technology base; reforming the public procurement process; enabling joint purchasing; and protecting the digital defence capabilities.

The policy brief concludes with a series of topics for further research.

AUTHORS

KIRILL SHAMIEV
Policy Fellow, European Council
on Foreign Relations (ECFR)

GIORGOS VERDI
Policy Fellow, European Council
on Foreign Relations (ECFR)

THE FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)
European Political Foundation - Nº 4 BE 896.230.213
Avenue des Arts 46 1000 Brussels (Belgium)
www.feps-europe.eu
@FEPS_Europe

This policy brief was produced with the financial support of the European Parliament. It does not represent the view of the European Parliament.

FEPS Project Coordination and Review: Monty Aal, Beatriz Abellán, Uwe Optenhögel, Vanessa Zwisele
Copy editing: Rosalyne Cowie
Layout: Downtown
Cover photo: Shutterstock / DC Studio
Suggested citation: Shamiev, K. & Verdi, G. (2025). “Smarter spending today, safer societies tomorrow – Digitally enabled capabilities for European defence”. FEPS policy brief. https://feps-europe.eu/publication/smarter-spending-today-safer-societies-tomorrow

Belgian legal deposit number: D/2025/15396./43
ISBN number: 978-2-39076-048-1

Acknowledgements

The author wishes to thank the team of the Foundation for European Progressive Studies (FEPS) and a colleague at the European Council on Foreign Relations (ECFR) who reviewed an earlier draft of this paper and whose comments led to improvements to the text. Following review, we submitted the final draft to FEPS and revised the policy brief in response to comments provided by FEPS team.

TABLE OF CONTENTS

LIST OF ACRONYMS

AI: Artificial intelligence

APT: Advance persistent threat

AWACS: Airborne warning and control system

AWS: Amazon Web Services

C2: Command-and-control

C4: Command, control, communications and computers

CER: Critical Entities Resilience

CISA: Cybersecurity and Infrastructure Security Agency

DEF: Defence Equity Facility

DIU: Defence Innovation Unit (US DoW)

EASA: European Union Aviation Safety Agency

EDF: European Defence Fund

EDIP: European Defence Industry Program

EDIRPA: European defence industry reinforcement through Common Procurement Act

EIB: European Investment Bank

EIF: European Investment Fund

EMS: Electromagnetic spectrum

ENISA: European Union Agency for Cybersecurity

ESG: Environmental, social and governance

EW: Electronic warfare

FPV: First-person view

GIS: Geographic information system

GLONASS: Russian global navigation satellite system

GNSS: Global navigation satellite system

HIMARS: High-mobility artillery rocket System

HPC: High-performance computing

ISR: Intelligence, surveillance, reconnaissance

ITU: International Telecommunications Union

JDAM: Joint Direct Attack Munition

MALE: Medium-altitude long-endurance

NIS/NIS2: EU Network and Information Security Directive

NSPA: NATO Support and Procurement Agency

OWA: One-way attack

PGM: Precision-guided munition

PNT: Positioning, navigation and timing

SAFE: Security Action for Europe

SATCOM: Satellite communications

SESI: Strategic European Security Initiative

STEP: Strategic Technologies for Europe Platform

UAV: Unmanned aerial vehicle

UGV: Unmanned ground vehicle

UMPK: Universal Gliding and Correction Module (Russian glide kit)

USV: Unmanned surface vehicle

INTRODUCTION

The Russian invasion of Ukraine has greatly deteriorated the European security. The scale and quality of European assistance to Ukraine has negatively affected European military stockpiles and underscored the grave need for enhanced defence production. However, rising defence expenditures face political and economic trade-offs, as they typically slow down economic growth, reduce civilian consumption and increase public debt.[1] This makes it vital to ensure that European financial resources are invested strategically, and that better coordinated EU-led spending is directed toward high-impact digital defence capabilities, which deliver greater returns in deterrence, autonomy and resilience.

This policy brief covers four areas where there is most potential for digital technologies to support transformation capability changes: (1) cyber warfare; (2) electronic warfare (EW); (3) unmanned systems; and (4) space and communications. It also examines cross-cutting enablers that strengthen these capabilities: artificial intelligence (AI) and big-data analytics; quantum cybersecurity; and computing, including cloud, quantum computing and processors.

In Ukraine, unmanned systems, space communications, and electronic and cyber warfare have proven effective. Their employment not only enhanced operational capabilities but also offset manpower shortages and reduced dependence on traditional, high-cost assets. However, to avoid the risk of over-relying on one case, this policy brief analyses the application of emerging defence technologies in the most likely potential geopolitical scenarios in the European Union (EU).

The policy brief looks at the Russian Federation as the key threat to European security. The study assumes that the most likely operational theatre for countering the threat coming from Moscow lies in Eastern Europe, especially in the Baltic States and Poland. In the short term, Europe needs to quickly deny the Russian asymmetric advantage in drone capabilities and long-range strikes. Russia spends more than 30% of its annual federal budget on the military, including the annual production of 500 X-101 missiles (up to 4,000 km) and 700 9M723 Iskander missiles (up to 500 km), with the potential for increased production,[2] as well as the monthly production of 250,000 barrel ammunitions.[3] In the long term, Europe needs to be ready for the rebuilding of Russian ground forces, the spearhead of Russian military power.[4] According to some estimates, Russia can produce annually up to 250-300 T-90M tanks, the most advanced combat vehicles in service with the Russian Armed Forces. Moreover, Russia plans to hire more than 1.5 million UAV pilots by 2031-2035.[5]

Therefore, the development and deployment of European high-impact capabilities should be based on contingency planning of the potential use scenario. While this policy brief cannot cover the full spectrum of military development, investments in digitally enabled technologies should signal to the Russian leadership that any unwarranted military actions would be futile in achieving their political goals.

At the same time, the policy brief acknowledges the declining reliability of the USA as the key European ally due to the rapid changes in US foreign and security policies under President Donald Trump. This significantly complicates European defence sector development, which has historically been reliant on the American military-industrial production. Therefore, the analysis assesses how far these emerging technologies depend on US military and industrial support.

To do this, this policy brief assesses the technologies' impact, scalability and alignment with EU strategic autonomy objectives. It also outlines policy pathways to develop these technologies within existing regulatory frameworks, ensuring compliance with European and international standards and their responsible, effective use. The policy brief relies on the analysis of existing regulations, policies and studies on European defence, as well as on 14 semi-structured interviews conducted with representatives of the industry, public sector and independent experts (see Annex for more details).

Our analysis shows that Europe can get the biggest payoffs in digitally enabled technologies from two areas: unmanned systems in the short term and space/communications in the long term. Drones already drive-up adversary's costs but are fragile under strong EW and attrition, and Europe still depends on cheap external supplies, especially from China. Space assets keep targeting and communications going, enabling European militaries, but European autonomy is limited and resilience is only moderate due to cyber risks. Moreover, scaling space capabilities is costly. Cyber capabilities act mostly as a vital defensive layer, adding little direct deterrence, but protecting European capabilities across domains. EW could only moderately raise the adversary's operational costs and is Europe's weakest pillar; it has low resilience and low scalability.

The policy brief is structured as follows. Firstly, we outline today's key gaps in Europe's defence technology and the main European funding tools for modernisation. Next, we assess each selected capability and the cross-cutting enablers that can act as force multipliers. We then offer a set of actionable areas for improving the development, production and fielding of European defence capabilities. The policy brief ends with a brief conclusion and topics for future research. The Annex contains the methodology and analytical approach used for this research.

THE CHANGING CHARACTER OF WARFARE AND EUROPEAN DEFENCE INVESTMENTS

The EU and its member states still struggle to close gaps in defence capabilities, including in the most transformational digitally enabled technologies. In the short term, Europe should harden its deterrence against Russia in Eastern Europe by fixing near-term technology shortfalls using any available friendly sources. In the long term, Europe should be prepared for Russian military modernisation and the realisation of the repeated Trump-era calls for European autonomy without US backing. The USA's pivot to the Indo-Pacific and shifting production toward American needs warrant against relying on its military-industrial production.

Effective European foreign and security policy requires a broad, flexible toolkit, rather than a fixation on symbolic spending targets or specific weapon systems. For example, the nominal 5% defence spending target is prone to abuse by misallocating practically non-security-related assets under defence investment programmes. Smarter European spending should be forward-looking, rooted in contingency planning, integrated in European industrial and research & development (R&D) efforts, and collaborative in its essence.[6] The European response to contemporary security needs should be based on a whole-of-society approach to fuse civilian and military efforts in creating a safer, more prosperous and cohesive Union.

Contemporary European capability gaps

***Digital defence capabilities show that smarter spending is achievable**, as new technologies are disrupting traditional markets by opening lower-cost, higher-tempo production options. The EU can do more in aligning national governments with producers, as well as in reinforcing cross-border cooperation, while coordinating European action to receive strategic enablers, especially in space.*

The White Paper for European Defence lists seven areas of capability gaps, four of which involve gaps in digital defence, namely, air defence, drones, EW and space.[7] In the short term, Europe is lacking capabilities in air and missile defence and drones. The expansion of Russia's missile arsenal and drones underscore the need for the rapid development of European near-term defence solutions against saturated skies, especially the mass employment of drones combined with missile capabilities.[8] European militaries lack an arsenal of disposable defensive and offensive drones to engage in high-intensity combat. Some member states possess capabilities in expensive medium-altitude long-endurance (MALE) drones, but their effectiveness has been contested, as similar systems were downed in the first few months of the war in Ukraine.[9] Currently, tactical drones account for 60-70% of damaged and destroyed Russian systems in the war with Ukraine.[10] Drones that cost from as little as $500-100,000 can jointly take out hardware, such as aircrafts or tanks, worth millions of dollars.

Technological advancements are making Ukrainian defence capabilities leaner, directing limited financial resources towards innovative capabilities and cross-cutting enablers. They opened a window for non-traditional defence start-ups. Most of the Ukrainian drones, their parts and software are developed by soldiers, start-ups and other innovative new entrants that challenge the dominance of the large "traditional" defence companies.[11] Similarly, Russia is currently experimenting with a unique integration of a drone start-up in an actual combat role and military structures, disrupting its conservative military architecture. Russia's secretive Rubicon Centre acts as a developer, training centre, warfighting unit and analytical department in drone warfare.[12] The technological advancements are disrupting the defence industry, providing another opportunity for smarter spending.

In the mid- to long-term, the EU's gaps in its civilian technological base also translate into defence gaps, especially in AI, quantum, cyber and EW.[13] Additionally, Europe's shortfalls in launch capacity and space-based intelligence, surveillance and reconnaissance (ISR) capabilities undermine European autonomy and the protection of critical infrastructure.[14] Coordinated European efforts will be needed for developing space enablers, which were able to significantly augment Ukrainian military effectiveness.[15] Without centralised efforts, the EU will struggle to deliver space-based enablers and ensure redundancy in communication and space technologies.

Overview of the EU instruments to finance capabilities

European instruments for defence technology have expanded in scope and funding, including stronger support for dual-use innovation. Delivery still suffers from fragmentation across programmes; long award cycles; weak pathways from testing to production; and the lack of coordinated, multi-year demand for priority capabilities such as air defence and counter-UAV (unmanned aerial vehicle). In 2023, EU member states' defence-innovation outlays were roughly one tenth of US levels,[16] and member states devoted 4.5% of defence budgets to R&D versus 16% in the USA.[17] The overview below focuses on European programmes facilitating the invent-industrialise-procure-finance cycle in the defence sector.

In 2025, the European Commission amended existing EU instruments to support the EU's defence efforts through dual-use research and technologies. This change includes the Digital Europe Programme (DIGITAL), which allocates €7.59 billion to accelerate Europe's digital transformation, including dual-use technologies. Similarly, an amendment to the Horizon Europe programme allowed the support of dual-use technologies from its €93.5 billion budget. Finally, the €25.8 billion Connecting Europe Facility also supports dual-use efforts, particularly to improve military mobility.[18] This a welcomed development because most drones in Ukraine are produced with civilian parts and software, including those procured from China. Investments in the military application of cyber and space capabilities cannot be separated from their civilian use, just like cybersecurity efforts and space technologies demonstrated in Ukraine.

The European Defence Fund (EDF) facilitates collaborative defence R&D and prototyping. The EDF was set up to allocate €7.3 billion to collaborative defence research and collaborative capability development projects until 2027.[19] For the period of 2024-2027, it received an additional €1.5 billion top up under the new Strategic Technologies for Europe Platform (STEP) to boosts investments in digital technologies and deep-tech innovation. Its 2025 Work Programme aims to support the development of critical defence technologies and capabilities by funding collaborative defence R&D via annual calls run by the Commission with strict control and security-of-supply rules. Representatives from the industry and expert community suggested that the conversion of EDF efforts to fielded capability was slow and paperwork-heavy.[20] It delivered value to cross-border R&D efforts but demonstrated weaker effectiveness in the fielding of prototypes and operational adoption. The interim evaluation of the EDF and independent assessment also confirmed these findings.[21]

In July 2025, the European Commission proposed a European Competitiveness Fund (ECF) worth of €409 billion for the 2028-2034 Multiannual Financial Framework. This new instrument aims to bring together and consolidate 14 individual funding instruments to boost European competitiveness in strategic sectors. Defence is named as one of the main priorities of the ECF, as it will bring together activities that are currently carried out by Horizon Europe, the EDF, European Defence Industry Program (EDIP) and others. In this way, ECF will operate as one rulebook and offer a single gateway to funding applicants, focusing on civil-defence synergies and dual-use technologies. Importantly, under the current proposal, the ECF Regulation will repeal the EDF and integrate its activities under the ECF umbrella work.

Recent political agreement on EDIP closes the gap between EDF R&D support and actual procurements.[22] It aims to raise defence-industrial readiness by ramping up manufacturing capacity, opening cross-border supply chains, and involving SMEs and mid-caps. It incentivises joint procurement to cut fragmentation, strengthen standardisation and improve interoperability.[23] With a budget of €1.5 billion (2025-2027), it funds common purchases, derisks production investment and helps productise EDF outputs to strengthen the EU defence industrial base and ensure a steady supply. EDIP also harmonises and simplifies cooperative armament programmes, including possible VAT waivers for jointly owned systems. Moreover, it seeks to provide an EU-wide security-of-supply regime.[24] The European policymakers interviewed unanimously claimed that with EDIP, the EU now has all the instruments for defence-industrial development. However, these generally could be better funded. Existing cross-border cooperation schemes target non-critical capabilities, requiring stronger steering. Moreover, certification barriers still block cross-border use of identical platforms, inflating costs and delaying delivery.[25]

EDIP will support European defence industry reinforcement through the Common Procurement Act (EDIRPA) that was established in 2023. With a budget of €310 million, the instrument provided incentives to EU member states to jointly procure defence products.[26] EDIRPA financed the procurement of Mistral very-short-range air defence systems, IRIS-T SLM medium-range air defence systems, the Patria Common Armoured Vehicle System as well as ammunition.[27] Despite its high relevance, EDIRPA's budget was too small and plagued by competing national priorities.[28]

The European Investment Bank (EIB) also invests in dual-use research through the €8 billion Strategic European Security Initiative (SESI).[29] Since 2024 the EIB loosened defence-lending rules, scrapped the old ">50% civilian revenue" test for dual use, and set up a Security & Defence Office, which allows for more flexible loans for plants, infrastructure and supply-chain finance, while weapons and ammunition remain excluded.[30] In addition, the EIB's European Investment Fund (EIF) launched the Defence Equity Facility (DEF) in 2024, managing €175 million, with the aim of supporting venture capital and private equity funds that invest in European companies developing dual-use technologies.[31] In 2025, the EIB raised its financing ceiling, signalled a doubling-to-tripling of defence lending, and approved targeted operations for SMEs and critical capacity, useful to crowd-in private capital but still contingent on long-horizon national orders.[32] The respondents approved these changes, stating that both initiatives reflect the EIB's broader opening to security and defence, with more flexible lending and a new internal setup.[33] However, one policymaker interviewed commented that commercial banks were yet to follow the EIB's example. They can deny loans to companies with defence projects on environmental, social and governance (ESG) grounds, sending a negative signal to the market.[34]

In May 2025, the EU also opened the way to urgent and major procurement with the Security Action for Europe (SAFE) instrument, which provides loans of up to €150 billion to member states that request them. SAFE is part of the larger ReArm Europe Plan, which aims to mobilise €800 billion in total from member states, by introducing greater flexibility within the EU's fiscal rules.[35] The respondents generally welcomed these but noted that it was too early to comment on their impact on the European defence sector.

European defence capabilities

The Russian invasion of Ukraine has served as a testbed for defence innovations, triggering a multidimensional arms race. Breakthroughs in EW, drones, and space and communication systems have been the most prominent. For Europe, the most urgent need is to bridge the gap in its development and fielding of drones and counter-drone capabilities to increase its deterrence against potential attack by both degrading the effectiveness of Russian drone strikes and promising high retaliatory damage in the short term. Strategically, Europe needs to invest in EW and space technologies, as well as enablers such as AI, advanced materials and computing, that could act as force multipliers for European militaries.

Drones

Drone systems are described by various terms, which highlight different components and purposes, such as unmanned ground vehicles (UGVs), UAVs and unmanned surface vehicles (USVs). These terms refer to remotely controlled devices – from micro- and nano-drones to aircraft, vessels and transporters weighting several metric tones. [36]

Drones can be armed or unarmed. Their most natural use is for ISR purposes, whereby the drones capture photos, videos and data that can help track enemy forces.[37] Ukraine initially relied on off-the-shelf civilian drones like the DJI Mavic for reconnaissance. This evolved into drones that were used to help direct and conduct strikes, such as modular first-person view (FPV) drones that could be reconfigured for bomb-dropping or one-way attack (OWA) roles or by programming drones to seek pre-designated targets as loitering munition. Expensive pieces of equipment were destroyed by $500-1,000 bomb-dropping or OWA FPVs, made by 3D printing and rapid "garage" manufacturing.[38]

The deterrence potential of UAV, UGV and USV systems for Europe's defence is decisive in short term. *All interviewees agreed that a strong commercial drone industry, capable of generating and replacing a massive number of drones, offers a significant deterrent potential today. Drones do not replace existing capabilities, but they add more operational layers and significantly shift costs through mass and expendability. Cheap long-range UAVs make deep strikes affordable and compress the sensor-to-shooter loop, boosting deterrence by punishment.*[39]

This is why new applications for drones are constantly emerging, such as drones dropping mines and fire-spraying drones.[40] For example, operation Spider Web was the most vivid demonstration of drones' strategic potential to increase deterrence by punishment without using potentially escalatory legacy long-range strikes that the adversary can detect, counter and respond to. The small drones damaged or destroyed around 20 Russian strategic military aircraft in multiple locations.[41] However, this was likely a one-off operation, as Russia adapted and relocated its strategic assets away from the border.

Similarly, Moscow localised the production of Iranian Shahed OWA drones, which were rebranded as Geran. From late 2022, it launched hundreds of such drones in large quantities against cities, military command centres and infrastructure, overloading Ukrainian air defence systems, which made it easier for Russian ballistic missiles to hit high-value targets. Later, the Gerans were modified for reconnaissance roles by installing cameras and communication devices on board. Due to the Shahed OWAs and other UAVs, the idea of a safe rear was effectively removed, with both Russian and Ukrainian troops constantly under surveillance, even while resting.

Drones can also act as force multipliers for existing European military capabilities, increasing the adversary's costs and enhancing the denial value of traditional strike barrel and missile artillery. Ukraine integrated drone surveillance with battlefield apps (geographic information system (GIS) Arta, Delta, Kropyva, Vezha, Ochi) and data fusion tools, allowing rapid strikes on UAV-identified targets.[42] ISR drones greatly increase the value of missiles, supporting precision strikes at depth with cheaper costs compared to ISR satellites and radiofrequency surveillance.[43] This has led into a "Somme in the sky" over Ukraine, where opposing drone systems make the battlefield transparent and lead to stalemate.[44] Under such circumstances, drones also assumed logistical functions in UAV and UGV forms, from delivering supplies to evacuating wounded using remote-controlled all-terrain vehicles and heavy-lift octocopters.

Moreover, Ukrainian UMVs effectively denied Russia naval access to the Ukrainian Black Sea coast, making it redeploy its navy to the Russian internationally recognised territory.[45] These small uninhabited boats, usually filled with explosives, OWA drones, cameras or missiles attacked Russian warships and naval bases, rendering major "traditional" ships helpless.[46] Once, such a drone took down a Russian fighter jet that was trying to intercept it at close distance.[47] Russia was slow to catch up with Ukraine, but then struck a Ukrainian reconnaissance vessel in August 2025 with the same technology.[48] Therefore, the European navy should be prepared for similar threats in the Baltic Sea region, illuminating the value of the swift deployment of new drones and counter-drone systems.

This is why the resilience of drone systems can be evaluated as limited, which directly affects their operational potential. *Failure rates for UAVs are generally high and get only higher, to 70-80%,[49] under dense EW, layered air defence or bad weather, meaning that only two or three out of ten launched UAVs hit the target, which may not even be destroyed by the strike. That is why both sides rely on a massive number of these devices attacking the same target in large quantities or one after another.*

Both sides were able to develop effective counter-drone capabilities. From EW means to short-range air defence, Russian forces have refined these capabilities throughout the three years of fighting against Ukraine's drone threats.[50] By 2025, Ukraine and Russia started deploying "drone interceptors" to intercept attack drones that were too cheap and numerous to counter with traditional air defence missiles.[51] This led to drone-on-drone clashes and aerial ramming encounters.[52] Further developments in anti-drone capabilities, such as the development of effective energy-directed weapons, might make drone systems even more vulnerable.

Europe's autonomy in drone systems is also evaluated as limited. *Most systems use Chinese components (e.g., DJI drones, radiofrequency and microwave filters) and American Starlink-type antennas (with Chinese alternatives available).[53] China not only produces the majority of drones, but also most of the components needed to assemble them,[54] capturing approximately a 74% share.[55] This dependency on China is alarming due to the dual nature of drones and Sino-Russian cooperation, which may lead to sabotaged exports or outright export controls in the near future.*

The production of drone equipment in China has a significant benefit – it substantially lowers the costs. Moreover, all drones require modified software that is currently largely being supplied by volunteers or even soldiers themselves. Türkiye's drone supplies would not provide the answer either, as their drone capabilities differ from those of China. Moreover, the country's 30-year-old war threat against Greece violates the security interests of EU member states.[56] All in all, EU member states don't possess a sufficient arsenal of armed and expendable drones, except for a few large and costly MALE drones.

However, the scalability of drone systems is evaluated as substantial. *According to industry reports, Europe is home to 40% of the world's drone companies.[57]* Munich-based companies Helsing and Quantum Systems, which specialise in drones and AI systems, have secured investments of €450 million and €100 million, respectively.[58] The lack of regulatory barriers in the development of dual-use drones in the EU also points to a high potential in scalability.[59] However, the rapid innovation cycle in drone measures and anti-measures means that effective scalability will not take place through stockpiling but by constantly producing modified systems on the go, accounting for losses and the destruction of production facilities.[60]

However, the challenge lies in the costs and quantity of production. For example, Ukraine currently produces FPV drones that cost about €400 per unit; fixed-wing interceptors are about €4,500, UGVs are about €10,000 and USVs are up to €270,000.[61] All of these drones rely largely on Chinese parts. The cost of mass production of such equipment in Europe will be two or three times higher at the lowest estimates. Although the EU is also funding the development of drones, by allocating 4-8% of the EDF budget to Emerging and Disruptive Technologies, as well as with other funding sources, such as DEF, Horizon Europe and Digital Europe, there is evidently a need for more agile funding instruments.

Finally, drones can also be evaluated as having moderate coherence, as their cross-border deployment faces some challenges. *The EU Defence Commissioner lacks a clear mandate on drone strategy, while coherence between member states on drone development and deployment is also lacking.*[62]

The recent experience with adopting the "Drone Wall" initiative exemplifies the challenges associated with drone production and deployment. To win backing from southern and western governments, the European Commission reportedly expanded its scope from eastern borders to a continent-wide counter-UAV network. Moreover, smaller states preferred Commission coordination, while larger states had not endorsed the plan. Specifically, French President Emmanuel Macron showcased scepticism and argued that the threat of drones was more complex than the idea of the Drone Wall suggested.[63] This was also the case for Germany's Defence Minister Boris Pistorius, who characterised the initiative as unrealistic.[64] Additionally, the EU struggled to choose suppliers, deployment location and to link capabilities with NATO's air and missile defence.[65]

The EU built a comprehensive civilian drone regime while leaving military use to member states. Since 2014, European Union Aviation Safety Agency (EASA) has led common rules, but defence drone operations remain a national competence outside this EU framework. As one expert put it, European peacetime audit and certification regimes slow down drone production, but war would inevitably streamline processes; this is why Europe should introduce controlled shortcuts now, before it is forced to do so in wartime.[66] For example, Lithuania created a fast-track for "projects of state importance", letting defence plants start construction without ordinary building permits and compressing other permits into a single accelerated track.[67] Similarly, Denmark passed a temporary regulation that lets the government fast-track construction tied to essential national defence and civil preparedness. It enables ministers to assume permitting powers by executive order; derogate from planning, building, environmental and nature-protection rules; and limit or compress complaint procedures where necessary for a specific project.[68] Similar measures across the Union would help the industry overcome national bureaucratic challenges and expedite the delivery of investment projects.

The development and deployment of drone systems also pose serious challenges in their coherence with international humanitarian law. Drone strikes could also result in civilian casualties when they miss their intended target or misidentify combatants from non-combatants. For example, in the Russo-Ukrainian war, combatants advised civilians to always remain in basements, especially at night, when drones with thermal scopes could not realistically distinguish heat patterns of civilians from enemy soldiers. However, civilians also had to hide during the day due to intensive shelling and fighting, ending up being trapped underground. The development of fully autonomous drones that enables strikes without human intervention is also effectively prohibited under current humanitarian norms, while there is a strong impetus from the military to shorten the kill cycle as much as possible. These and other issues with drones pose serious international humanitarian law concerns that must addressed.

Cyber domain

Defence capabilities must be as effective in the cyber domain as in the conventional domains of air, land and sea. Cyber warfare capabilities can be used both before and during hostilities to obtain state secrets, including military intelligence and defence technology advantages.[69] Moreover, cyber warfare can be deployed to attack and disrupt critical infrastructure, including power grids,[70] communications, financial institutions and government bodies. On the battlefield, cyber warfare capabilities are not considered to elicit effects independent of kinetic warfare but serve as enablers of conventional capabilities. Offensive cyber capabilities can be used to monitor an adversary's operations and track the movements of specific units.[71] Finally, they can also be used to disrupt command-and-control (C2) communications[72] and to directly disable or disrupt adversarial weapons systems.

The ability of cyber warfare capabilities to deter adversaries is evaluated as being marginal. The Russian-Ukrainian war has proven that the offensive nature of cyber capabilities get eliminated due to good cyber defences and the difficulty in synchronising cyberattack with kinetic operations. None of the Russia-linked advance persistent threat (APT) groups have delivered strategic outcomes since 2014. In some instances, offensive cyber capabilities can disrupt an enemy's capabilities on a scale that legacy systems are unlikely to achieve. The strongest attack on Viasat's KA-SAT satellite network happened on 24 February 2022, disabling thousands of modems across Europe and disrupting one of the Ukrainian military communications channels.[73] Cyberattacks on Iran's nuclear programme damaged up to 1,000 high-speed centrifuges enriching uranium.[74] However, such high-impact cases remain rare. In Ukraine, most Russian attacks failed to coordinate with kinetic military operations, and the networks, including Viasat's KA-SAT, were quickly restored.[75] Similarly, Ukraine organised multiple hacktivist groups to infiltrate and disturb Russian digital infrastructure.[76] Hacktivists stole sensitive Russian datasets, encrypted companies' data for ransom and denied service to Russian websites.[77]

As a result, cyber operations require co-ordination with other lines of operations and tools to be effective.[78] As the Russian-Ukrainian war demonstrates, the defensive uses of cyber capabilities are more prevalent to deny strategic outcomes to an adversary.

The EU's autonomy in the field is evaluated as limited*, primarily due to the lack of European commercial providers. According to the European Cyber Security Organisation, 60-70% of the civilian cybersecurity market in Europe is captured by non-European companies.* As the Russian-Ukrainian war has shown, access to commercial cybersecurity capabilities is essential in a conflict scenario.[79] Europe's dependency also extends to other parts of the cybersecurity infrastructure. The rapid shrinking of the US Cybersecurity and Infrastructure Agency (CISA) under Trump's presidency has had direct effects on the EU's capability, which partially relied on CISA for reporting and patching cyber vulnerabilities.[80]

Ukrainian cyber defence benefited greatly from cross-border and public-private partnerships, including via cooperation with Amazon Web Services (government data on AWS clouds[81]), Cloudflare (Project Galileo), ESET, and Google (Project Shield for civil society), and were in large part responsible for countering Russian threats. Similarly, Russia also relied on such private sector companies as Kaspersky, Security Code and Positive Technologies.[82] However, Kyiv had competitively advantageous support from EU programs that put in place coordination mechanisms, reform programs and information-sharing networks before the war escalated in 2022.[83]

Scalability is evaluated as moderate when it comes to cyber warfare capabilities. On one hand, Europe is scaling the resources dedicated to strengthening cybersecurity capacity. For example, the EU increased Horizon Europe's funding for cybersecurity, from €60.4 million in 2024 to €90.5 million in 2025. The Digital Europe programme also dedicates €55 million, with €30 million allocated for the protection of Europe's healthcare systems from cyberattacks.[84] For example, funding through the Digital Europe programme will support the European Cybersecurity Alert System, which can scale cyber intelligence capabilities, and the Cybersecurity Emergency Mechanism, which can scale preparedness and incident response capabilities.

On the other hand, structural weaknesses in the EU's commercial cybersecurity market, its limited scale, fragmentation and talent constraints create vulnerabilities and limit how quickly European-autonomous, sovereign solutions can be developed and deployed at scale.[85] As respondents representing a cybersecurity firm and a public body commented, Europe lacks the baseline cyber hygiene and cyber defences of critical nodes, including physical infrastructure, such as undersea cables.[86] The latest example of a cyberattack (likely non-state; suspect arrested in West Sussex, UK) on the Collins Aerospace's automatic check-in system disrupted European airports, underscoring how a vulnerability at a single node can trigger knock-on effects across European mobility.[87]

The resilience of the EU's cyber warfare capabilities is substantial. *The EU's extensive legislative activity in the field has led to common minimum standards across connected devices and critical infrastructure*. The most relevant pieces of legislation include the NIS 2 Directive and the Cyber Resilience Act. The Cyber Solidarity Act has also established the EU Cybersecurity Reserve, which intends to assist member states and institutions with responding to cybersecurity incidents.

This also contributes to a substantial level of coherence between EU member states and facilitates the cross-border development of cyber capabilities. Coherence is also high between the EU and NATO, with the first Structured Dialogue on Cyber taking place on October 2024 and building on the previous EU-NATO High-Level Staff Talks on Cyber Security and Defence.[88]

Electronic warfare

The electrification of the battlefield has led to a pervasive presence of the electromagnetic spectrum (EMS) within defence capabilities.[89] The functions of EW include electronic surveillance, in which the EMS is surveyed to identify emissions, their location and their content. In turn, electronic surveillance allows forces to monitor and track adversaries. Offensive EW capabilities can be used to attack enemy systems and jam them or spoof them – whereby the receiver believes the signal is coming from a friendly system.[90] The latter can be used for navigational interference, causing ships, aircraft, drones and targeted munition to lose their way.[91] EW also has significant overlaps with cyber warfare, with the potential for both methods to be combined in a single attack or a technique from one used to inhibit the other.[92] The same capabilities can be used for purely defensive purposes to protect friendly forces and systems from adversarial jamming or from other techniques.[93]

The ability of EW to increase deterrence is moderate. *The war became a cat-and-mouse game between competing powerful Russian EW developments and Ukrainian intelligence eavesdropping on Russian communications.*[94] Russian forces jammed positioning, navigation and timing (PNT) signals of US-supplied precision-guided munitions (PGMs), such as high-mobility artillery rocket systems (HIMARSs), joint direct attack munitions (JDAMs) and Excalibur shells, delivering major declines in precision. Both sides also disrupted radio communication networks. Ukraine's indigenous EW systems, such as Anklav, Bukovel-AD and Pokrova, have also proved to be effective against Russian drones and PGMs, especially Universal Gliding and Correction Module (UMPK) equipped bombs.[95] However, this effectiveness was often temporary, as both sides tried to adapt their weapons to the limitations imposed by the other side.[96]

The resilience of EW capabilities is limited. *Constant technological modernisation of the EMS and countermeasures require constant adaptation.* In Ukraine, the EW proliferated and was miniaturised, becoming pervasive down to the squad/vehicle level. It shifted from high-power, vehicle-mounted systems to more survivable, directional systems, including with the use of commercially available parts and software. Moreover, coordinating EW use is a significant problem, as multiple squad/vehicle level devices can interfere with communications and drones' radio frequencies, leading to electronic "friendly fire".[97]

Europe's autonomy in EW capabilities is evaluated as marginal. *NATO forces rely heavily on the USA for EW capabilities, according to a former commanding general of US Army Europe.*[98] In the aerial and space domains, NATO allies are heavily dependent on the USA for electronic intelligence collection and the resulting threat library. Another area of heavy NATO dependency on the USA is supporting jamming where the allies' capabilities reside in US Navy squadrons.[99] This is why many frontline EW systems became "garage innovations" in Ukraine, using Chinese and other commercial equipment, due to the slow adaptability of traditional, big, industrial EW technologies.[100]

The scalability and coherence of European EW capabilities is limited. *The lack of a European doctrine on EW capabilities is one reason behind this*. Perpetual EW development requires massive investments (millions of euros) in R&D.[101] This means there is a lack of available funding allocated for the EU to catch up in EW. While EW capabilities are funded through scattered calls in the EDF, it is unlikely that they will allow Europe to significantly increase its fielded capabilities. However, weaknesses in EW technologies can have negative knock-on effects on the command, control, communications and computers (C4) and ISR systems, degrading or fully disrupting their functions in the EW emission areas.

Space

Space has become the fifth domain of modern warfare. **Space capabilities are now essential in gathering operational ISR.**[102] Space services can provide location-based data on enemy positions and logistics, as well as early warning for the monitoring of proliferation and ballistic missile activity.[103] Space is also essential for enabling navigation via the Global Navigation Satellite System (GNSS) used both for troops and to enable precision firepower through guided munitions.[104] Finally, satellite communications (SATCOM) enable secure exchange of information in multi-domain settings and across theatres, regardless of distance.[105] The strategic role of space has prompted the pursuit of counter-space capabilities.[106] These include kinetic means that target terrestrial space infrastructure, such as ground stations and satellite factories, and even direct anti-satellite weapons.[107] Anti-space capabilities also include non-kinetic means, such as EW or cyber warfare capabilities, such as Russia's cyberattack on Viasat, aimed at denying access to space capabilities or disabling a targeted system.

For Europe, the deterrent potential of space capabilities is evaluated as decisive. *While space capabilities can't directly degrade or disrupt adversarial logistical chains, they can provide invaluable support to European forces and increase their operational range, especially compared to legacy means.* Boths sides in Ukraine used space for SATCOM, ISR and PNT. Commercial satellite imagery and declassified ISR provided an early warning of Russia's invasion and improved battlefield transparency.

Russia's military SATCOM remain weak and outdated. Most are past their service life, while civilian systems like Gonets, Express and Yamal also suffer from low bandwidth and high latency. In 2026, the Russian aerospace company Bureau 1440 plans to launch a pilot project to provide communications via low-Earth-orbit satellites. By the end of 2030, the Bureau 1440 constellation is planned to reach 292 operational satellites, with a total of 383 launches, including 91 replacements for failed units.[108]

After the 2014 invasion, Ukraine prioritised space-focused ISR and SATCOM by contracting both commercial and government providers for satellite data. It started with volunteer-procured Viasat terminals after 2014 that enabled Ukrainian Kropyva and Delta software, which integrated drone and satellite data into fire control and situational awareness. In 2019, Ukraine gained access to the EU's Copernicus Sentinel data, and in 2021, it secured a contract with South Africa's Dragonfly Aerospace for additional remote sensing. Maxar, Planet Labs, Capella and BlackSky supplied critical imagery, with BlackSky even adjusting satellite orbits to maximise Ukraine coverage and deliver data within 24 hours of launch. HawkEye 360 provided a unique capability by detecting and geolocating radio-frequency emissions, helping Ukraine track Russian jamming and target associated forces. ICEYE's data allowed Ukraine to locate over 7,000 Russian military sites and confirm the destruction of hundreds of assets, including fighters and missile launchers. In 2024, ICEYE and Ukraine's Ministry of Defence formalised cooperation to expand data use and restrict Russian access.[109]

The rapid adoption of SpaceX's Starlink by spring 2022 significantly augmented Ukrainian SATCOM. Starlink illustrated both its unique value and risks of depending on private firms, especially where governance is based on ad hoc arrangements rather than contracts.[110] This is why Ukraine is planning to develop national SATCOM with European partners, including Luxembourg's SES, Spain's Hisdesat, the UK's Viasat and the French-British Eutelsat/OneWeb, by end of 2030.[111]

Unlike Russia's difficulties with upgrading its SATCOM and ISR, Moscow made improved use of PNT-enabled weapons in an attempt to overcome GNSS jamming, coupled with incremental upgrades to GLONASS. Moscow demonstrated its resilience in developing precision strike capabilities and reliance on diversified guidance systems, such as inertial navigation and terrain matching. Russia has strengthened its GLONASS system by launching its final GLONASS-M satellite in 2022 and its first GLONASS-K2 in 2023, expanding the reliance on its domestic capability. Similarly to Russian EW systems disrupting Western GPS-guided munitions, Ukrainian forces tried to jam Russian drones and munities by exploiting their GNSS reliance. Yet, this reinforced the technological race for developing new disruption-resistant PNT technologies, such as in Russia's new jet-powered Geran-3 OWA drones.[112]

Europe's autonomy in space is evaluated as limited. *When it comes to cheaper satellites in low orbit, the market is dominated by SpaceX, which was able to cut down costs due to its reusable rockets.*[113] *Europe's potential response to SpaceX's Starlink is the IRIS² Satellite Constellation, which envisages having more than 290 satellites entering into service only after 2031.*[114] However, the EU possesses some competitive capabilities when it comes to large satellites in geostationary orbit. The EU also owns and operates the space assets Galileo and Copernicus for PNT and ISR, respectively.[115] Thirdly, the EU also possesses some technical assets in space capabilities, including an independent launch site.[116] However, the EU lacks autonomous capabilities that can aggregate various space, EW and cyber data and make it swiftly useable in warfare, similar to sensing by the airborne warning and control system (AWACS) to complement it.[117]

The resilience of space capabilities is evaluated as moderate. *As space capabilities rely on information systems, they are susceptible to cyberattacks.* However, the adoption of cybersecurity requirements can help mitigate such attacks and recover from cyber incidents. The proposed European Space Act establishes such a sector-specific mitigation framework for cyberattacks that can enhance resilience if implemented across military space capabilities.[118] EW attacks could also disrupt space capabilities. According to the International Telecommunications Union (ITU), Russia has been using EW to disrupt European satellites.[119] Finally anti-satellite weapons also threaten the resilience of space capabilities. This raises the importance of redundance in space capabilities, including through the use of civilian/dual-use devices, similar to Starlink, that can create additional value layers if one or several other options are offline.[120]

The ability of the EU to scale its space capabilities is limited. The delay in the IRIS² Satellite Constellation, which was initially intended to be operational by 2027, indicates the existence of constraints in the scalability of space assets given the current state of EU affairs. Regulatory constraints have also partly contributed to slowing down private sector efforts, such as the Space Alliance, which the European companies Leonardo, Thales and Airbus are exploring.[121]

Coherence in space capabilities is substantial. *The third Joint EU-NATO Declaration in 2023 identified space as a field where two institutions were aiming to expand and deepen their collaboration*. Tensions between member states and efforts to promote national interests have not yet had any concrete impact on EU-wide efforts but point to potential issues in coherence in the short to medium term.[122]

Cross-cutting enablers

Europe's defence technologies also depend on three cross-cutting enablers – AI, quantum and computing – that amplify both conventional and digital capabilities. AI can harden cyber/C4ISR, speeds up target discovery and decision loops, counters jamming, and increasingly powers drones. In space, AI-driven autonomy and big-data analytics pull faster insights from ISR and improve tasking, targeting and logistics. Quantum is both a risk and an opportunity: it threatens classical cryptography and enables superior PNT and sensing under GNSS jamming. All of this rests on computers that power ISR fusion, R&D and AI training/fielding. Secure access to processors, sensors and cloud capacity is becoming a strong determinant of deterrence and resilience.

Artificial intelligence (AI)

AI can be viewed as a force multiplier in digital defence applications, increasing European deterrence and technological resilience. Importantly, there is no single answer to whether AI will single-handedly provide strategic advantages to the offensive or defensive side.[123]

When it comes to cyber warfare capabilities, AI can act as a double-edged enabler. Binding cyber and cloud with AI (including synthetic data) can harden C4ISR and real-time operations.[124] Moreover, using AI can accelerate network mapping/target identification from intercepts and make decision-making faster for commanders.[125] AI is empowering both offensive actors with accelerated speed of cyberattacks and defensive cyber capabilities by reducing the time to detect, respond and recover from an attack.[126]

Emerging applications of AI are also found in EW, where its use has emerged to help prepare and equip radio-frequency systems against sophisticated adversaries.[127] AI can counter jamming, by giving missiles AI-enabled visual terminal guidance to bypass EW and boost PGM lethality.[128]

For space, AI-enabled autonomy may offer a leap in capabilities in the near future.[129] Related to AI, big data analytics enabled conventional and digital defence capabilities through the extraction of useful insights from large amounts of data, including space-enabled ISR, making more timely decisions.[130] For example, the integration of the US Department of War's Project Maven with Palantir technologies enhances battlefield awareness, targeting and logistics though using AI and computer vision to process vast amounts of military data.[131] Similarly, the integration of AI into French Caesar artillery pieces could provide a 30% saving in ammunition.[132]

In drone systems, AI enables semi- or fully autonomous uses,[133] as well as the possibility of swarm technologies, especially under drone-saturated, EW-heavy skies.[134] While such systems are not officially deployed at scale, there's evidence to suggest they have been used in limited scenarios. As one interviewee mentioned, Ukraine has 20-25 firms adding narrow AI (EW-resistance, fallback guidance) to drones but is highly sceptical of swarm scenarios.[135] In the Russian-Ukrainian war, both sides use AI to process massive volumes of drone videos, with algorithms detecting artillery or hidden units more efficiently than humans. These capabilities rely on big-data systems, such as Ukraine's cloud-based platforms that fuse drone, satellite and radar inputs to prioritise threats.[136] Currently, both countries are rushing to develop "smart drone brains" that add functions like obstacle avoidance, target tracking and precision strikes even under jamming.[137]

AI also poses risks to the broader defence sector. The outputs of AI systems are shaped by data that can often embed human and societal biases.[138] In the context of defence, this issue can exacerbate unfair and discriminatory targeting during military operations. AI tools can also be used to spread disinformation through the generation of deep fake content that involves military and political leaders and the distortion of narratives regarding the situation on the battlefield.[139]

Quantum

Quantum technology is an emerging field that exploits the principles of quantum physics.[140] Advancements in quantum computing pose a threat to classical cryptography, which underpins the current methods of cybersecurity.[141] Experts predict that the first breaches of encryption methods by quantum computers might materialise by 2030.[142] However, the EU's Cybersecurity Agency (ENISA) argues that the development of the first fully functional large quantum computer will not be publicly announced, meaning that vulnerabilities in current defence capabilities must be addressed as soon as possible. The most promising solutions to this challenge are either quantum cryptography, which leverages quantum mechanics to transmit data in a secure way, or post-quantum cryptography, which focuses on developing new quantum-resistant algorithms.[143]

In the mid to long term, quantum computing can enable much higher data-processing power to aid sensing/targeting.[144] Quantum technologies can make better PNT and higher-sensitivity sensors, improving navigation/targeting resilience from cold-atom inertial sensors and next-generation atomic clocks that maintain precise position/weapon guidance when GNSS is jammed or spoofed.[145] However, direct quantum-enhanced weapon seekers or radars are very far from the current level of technological development.

Computing

Computing refers to information processing technologies, such as traditional microprocessors and specialist chips, such as graphical processing units. It also refers to cloud computing, which can scale the availability of computing power and deliver on-demand services.

Computing underpins many other conventional and digital capabilities. Both experts and industry representatives agree that strong computing is the backbone of "digital" pillars: intelligence gathering from drones or space capabilities; data transmission; data processing; real-time storage; and in-cloud analysis.[146] High-performance computing (HPC) is also central to R&D efforts, including in aerodynamics propulsion and thermal management for hypersonic weapons.[147] Finally, computing is a prerequisite for the development and fine-tuning of AI models that, in turn, enable a series of conventional and digital capabilities.

Both Russia and Ukraine depend on advanced microprocessors and electronics for drones and precision weapons, making global supply chains a hidden battlefield factor. Export controls since 2022 have forced Russia to rely on smuggling and repurposing commercial chips, while Ukraine's programs also depend on Western and Asian electronics. For example, Ukraine uses British/Taiwanese Raspberry Pi-class processors in their equipment. Similarly, sensor fusion/database management solutions like Palantir or Ukrainian applications like Delta, Kropyva, Vezha and Ochi also rely on computing power and benefit from faster processing. Therefore, the technological edge lies with the side able to secure better processors and sensors. By 2023, Ukraine's access to Western computing power and AI chips likely gave it an advantage.[148] However, most of these chips are produced in non-European countries, limiting European autonomy and underscoring the value of having reliable partnerships with the chip-producing countries.

Table 1. Net assessment of defence capabilities.

Capability	Deterrence	Autonomy	Scalability	Resilience	Coherence	Weighted Score
Drones	Decisive	Limited	Substantial	Limited	Moderate	3.30
Cyber warfare	Marginal	Limited	Moderate	Substantial	Substantial	2.45
EW	Moderate	Marginal	Limited	Limited	Limited	2.05
Space capabilities	Decisive	Limited	Limited	Moderate	Substantial	3.30
Average score	3.75	1.75	2.75	2.75	3.25	
Weight	0.3	0.25	0.15	0.2	0.1	

AREAS FOR IMPROVEMENT

Our analysis (Table 1) shows that in a potential Eastern-flank fight against Russia – marked by dense air defence coverage, heavy GNSS spoofing/jamming from Kaliningrad/Belarus, mass OWA drones/glide bombs and persistent cyber pressure on C2/logistics –

> *Investing in unmanned systems and space/communications provide the strongest current deterrent effects for the European military posture in the region.*

Drones already raise Russian operational costs in Ukraine but remain fragile under EW and munitions attrition, with limited autonomy in production and moderate coherence between member states and within the armed forces. Space assets enable targeting and communications continuity across battlespace and score decisively on deterrence, but European autonomy is also limited, while their resilience is only moderate given cyber exposure. The scalability of space is also limited due to significant technological investments and production costs, while coherence is substantial due to mature NATO/EU norms.

Cybersecurity is primarily an enabler rather than a stand-alone cost-imposer: its direct deterrence is marginal, but EU resilience and cross-border coherence are substantial with limited autonomy and moderate scalability. **EW sits at moderate deterrence** but suffers from limited resilience, limited scalability and marginal autonomy, while doctrinal gaps maintain limited coherence. Therefore, Europe's near-term strength lies in drone- and space-enabled denial/punishment under the contested spectrum, while cyber defences will keep availability high. EW remains the weakest pillar relative to massive, pervasive-spectrum Russian operations.

We suggest several areas for improvement that can improve European defence. Firstly, we propose improving the European technology base. Then we suggest potential pathways for changing public procurement processes. Finally, we propose options for joint purchasing and protecting the digital backbone of European defence.

Strengthen Europe's technology base

European autonomy is assessed as being low across the families of digital defence capabilities. Europe's limited capabilities in the applications of digital technologies in defence are closely linked to its limited capabilities in the civilian domain. The EU is overall dependent on others for 80% of its digital products, services and infrastructure.[149] This has prompted European leaders to call for a "sovereign digital transition" in October 2025. In both the civilian and defence domains, the EU is faced with risks of dependencies, as well as limitations in scale and further innovation capacity.[150]

> *European autonomy is assessed as being low across the families of digital defence capabilities.*

As a result, the EU should seek to strengthen its broader techno-industrial base and, at the same time, enhance civil-defence cross-fertilisation. This would promote smarter spending in two ways. Firstly, it holds the potential to increase the EU's GDP by stimulating cross-sectoral cooperation, investments and industrial growth.[151] Secondly, it would enable smarter spending, through access to new innovative products and services. For example, in the USA, commercial companies like SpaceX have demonstrated the ability to deliver cost-cutting capabilities to the Department of Defence.

In this regard, the establishment of a "28th regime" of corporate law that would allow European technology companies to scale faster and more effectively is critical.[152] President von der Leyen referenced the 28th regime in her 2025 State of the Union address. However, swift and effective implementation is needed for the EU to reap the benefits in defence innovation. Unlocking investments for European technology companies is also critical, including later-stage funding for start-ups.[153] Mobilising institutional investors will be key, as well as unlocking domestic savings.[154] Finally, the EU will need to attract high-tech talent to fill in the anticipated gaps. The restrictive policies of US administrations with respect to skilled workers presents an opportunity for European action.[155]

Reform public procurement processes

Europe has strong civilian tech funded by Horizon and Digital Europe, but too little reaches units in the field. Traditional processes that award defence contracts within member states can be slow-moving at best, and cumbersome at worst. This is an approach at odds with the rapid development cycles of commercial start-ups and negatively affects the scalability, resilience and autonomy of Europe within digital defence capabilities.

> *Europe has strong civilian tech funded by Horizon and Digital Europe, but too little reaches units in the field.*

Instead, member states should examine establishing alternative contracting processes that can cut down acquisition timelines while avoiding lengthy reform procedures.[156] A simple "handover rule" could require any project with defence potential, funded by Horizon Europe or Digital Europe, to file an EDF/EDIP plan for prototyping, trials and certification, with access to shared test ranges and computing.

The EU can consider discussing a NATO-EU pact that would share NATO industrial standards with the EU and empower Brussels to enforce them. This can reduce incompatibilities, even across identical platforms, and simplify cross-border procurement. A disclosure-and-enforcement deal would cut prices and raise interoperability across Europe.

Additionally, the US Defence Innovation Unit (DIU) was able to accelerate procurement of critical technologies developed by non-traditional vendors and award prototype agreements in as little as 60-90 days. The UK's RAF Rapid Capabilities Office fields digital/ISR capabilities quickly,[157] and Ukraine's BRAVE1 platform fast-tracks battlefield-driven robotics and EW solutions into service.[158] Europe's defence procurement authorities should consider setting up similar structures that would attract more founders to build defence-relevant products. Following the DIU's example, Europeans could also commit to completing a prototype project with innovators within 12-24 months.

Scale through joint purchasing and guaranteed supply

T Today, each member state often buys alone, which raises prices and slows delivery. The EU should learn from its developments in non-digital defence technologies. European politicians can consider coordinating multi-year joint purchases as the default for items like drone parts, counter-drone kits, sensors and secure communications, using EDIP/EDF, and apply the same technical specifications across participants. NATO allies already do this at scale: through the NATO Support and Procurement Agency (NSPA), allies have co-ordered large lots of 155 mm ammunition and air-defence items, pooling demand to cut costs and speed up delivery. EU funds can cover administrative overheads to scale joint orders, while member states place final orders.

> “Today, each member state often buys alone, which raises prices and slows delivery.”

To avoid production disruptions in a crisis, European politicians can consider supporting security-of-supply arrangements among producing states, so parts and finished systems move quickly across borders under the Defence Transfers Directive.[159] Nordic countries are also moving to joint purchases of artillery shells, giving more proof that “buying together” lowers risk and price. The USA likewise uses multi-year munitions contracts to give industry predictable demands for surge capacity.

Protect the digital backbone

Deterrence now depends on resilient data links and software. The EU should fully implement NIS2 and the Critical Entities Resilience (CER) Directive across defence supply chains and cloud providers, while prioritising a sovereign-compliant cloud for C2 and intelligence. For resilient connectivity, onboarding IRIS²/GOVSATCOM provides secure SATCOM for multinational operations; for processing power, the EU Chips Act and EuroHPC help guarantee access to modern processors and HPC. These steps reduce outage risks; keep systems interoperable; and ensure AI, drones, EW and space services keep working under stress.

> “Deterrence now depends on resilient data links and software.”

CONCLUSION

Europe's security environment is becoming worse and more dynamic than before. Recent studies show that Russia is rapidly rebuilding its land forces, supported by unmanned-systems troops. Our assessment shows that investments in unmanned systems and space/communications offer the strongest near-term deterrent on the Eastern flank, but Europe's autonomy in these technologies is low and resilience uneven, especially against Russia's scale and pervasive EW. Cyber technologies are an enabler that keeps forces connected and services available under cyberattacks and disruptions. EW remains the weakest pillar relative to Russian capabilities. Therefore, Europe can raise adversary costs now, but only if it closes critical gaps in drone production, EW and secure data links.

> *The path forward is practical and affordable: spend smarter by making defence an integral part of civilian technological and research development.*

The path forward is practical and affordable: spend smarter by making defence an integral part of civilian technological and research development. Europe can afford to improve its technology base and navigate its competitively advantageous human capital, so that fewer military capabilities will depend on non-EU suppliers. By reforming procurement, civilian innovation will reach units quickly, while procuring common items and spare parts together would cut cost and expedite delivery. Lastly, constantly hardening the digital backbone will help drones, EW and C2 keep working in a crisis. Therefore, European defence efforts should realise their enormous potential by integrating modernisation with civilian developments. These steps would increase deterrence, strengthen autonomy and improve resilience without locking Europe into single platforms or symbolic targets.

Topics for further research

This policy brief cannot comprehensively answer all the questions related to the modernisation of European digital defence technologies. Moreover, solutions to some of the issues rely on solving the bottlenecks in other, non-digital or non-technical areas. Over the course of this research, we identified several questions that both impacted the development of digital defence capabilities and their application.

Firstly, manpower. The EU has a larger population than Russia but generating mass, especially under continuous attrition, is difficult under current political and socio-economic circumstances. Still, there must be humans who will be able to use the technology, which is naturally damaged during warfighting. Therefore, the question of introducing bigger and better educated reserves – capable of deploying in a swift manner – supported by resilient production, logistics and emergency healthcare infrastructure is key. This question should be high on the political agenda.

Secondly, integrating diverse military and administrative cultures. All the experts interviewed for this policy brief doubted that there would be a common European army akin to the army of a single nation state. The most likely scenario is the development of "European armies", supplied and commanded by national administrations. Member states have different military cultures and public administration traditions. Therefore, ensuring that this diversity in civil-military relations transforms into an asset and not a bottleneck during a potential crisis should be high on the political agenda. Overall, improvements in this area would have positive knock-on effects for European cohesion and integration during peacetime as well.

Thirdly, integrating differences in threat perception between member states came up as a potential issue for developing common European defence technologies. Therefore, our proposal to anchor the development of military technologies in the civilian economy and improve pan-European procurement processes can potentially overcome political challenges that stem from the differences in the perception of Russia and European security. Exploring further how to minimise the trade-off between civilian economic development and defence technological production would be helpful to enable a political environment conducive to coordinated and joint European defence.

Lastly, future research should examine how EU regulations can keep defence technologies compliant with the EU's human-rights law and international humanitarian law.[160] The risks include discrimination by AI systems, failures of attribution and accountability in the use of autonomous weapons, and weak audit trails for battlefield decision support.[161] Policymakers should mandate clear human-in-the-loop controls and require incident logging for post-hoc review. Studies should investigate how procurement rules can embed safeguards by design and tie funding to transparency and verifiable risk mitigation. This agenda would align capability development with legal obligations while reducing strategic, ethical and reputational blowback.

ANNEX

1. CRITERIA

The study team integrates the analysis of capabilities based on the weighted attribution of scores to each criteria mentioned below. We use the following weighting scheme:

1. deterrence: 30/100;
2. autonomy 25/100;
3. resilience: 20/100;
4. scalability: 15/100; and
5. coherence 10/100.

The criteria were derived from FEPS's study questions and then operationalised. The deterrent value carries the highest weight given its near-term relevance in today's security environment. Strategic autonomy ranks second, reflecting shifts in Europe's ties with the USA and China's role in defence technologies. Resilience sits in the middle and captures the production ability and the capability to withstand combat stress and disruption. Scalability follows and measures the capacity to generate mass at speed and cost. Coherence rounds out the set and evaluates interoperability, standards alignment and regulatory fit.

Each study question was scored on a five-point scale against the relevant criterion: 1 = marginal; 2 = limited; 3 = moderate; 4 = substantial; and 5 = decisive. Scores reflect documented or well-supported effects of the capability. For example, if a drone system decisively disrupts Russian ISR, it received 5 for the pertinent criterion.

Due to the scope of this policy brief, it cannot comprehensively overview the full spectrum of defence capabilities or provide a detailed assessment of each selected capability. However, the analysis can be useful for policymakers, struggling to understand how to assess the ever-evolving families of defence technologies, as well as in the debate about the prioritisation of specific defence technologies.

I. Deterrence

Which of the selected capabilities most raises adversary costs today in the European theatre, and by what demonstrated mechanism?			
No	Study question	Operationalisation	Weight
1.1.	To what extent does the technology increase Russia's expected operational costs from aggression (deterrence by denial)?	Documented ability to degrade/disrupt Russian ISR/C2 and logistical chains	30
1.2.	Does it extend the EU's reach into domains where Russia holds a disadvantage (deterrence by punishment)?	Increase in operational range/reach compared to legacy means	

II. Autonomy

What are the top three EU dependency risks that can block rapid adoption? Can they be mitigated in-house?			
No	Study question	Operationalisation	Weight
2.1.	Does adoption strengthen European Defence Technological Industrial Base (EDTIB) autonomy or deepen reliance on non-EU partners?	Proportion of life-cycle costs spent within EU; Qualitative assessment of dependency on non-EU suppliers; Supplier concentration	25

III. Resilience

Under-estimated Russian pressure, what availability/uptime should European forces expect from each capability based on public evidence?			
No	Study question	Operationalisation	Weight
3.1.	How does the technology maintain European operational effectiveness under sustained attack or disruption?	Service availability/uptime under duress (cyber/EW); Time-to-restore after disruption reported in expert sources; Existence of redundant paths	20

IV. Scalability

With current EU frameworks, how quickly could member states multiply the capacity for each capability without new factories or laws?			
No	**Study question**	**Operationalisation**	**Weight**
4.1.	Can the production of the capability expand rapidly under existing regulatory, budgetary, or interoperability constraints while preserving its impact and contribution to European autonomy?	Expected challenges with boosting fielded capacity given current state of EU affairs; Unit-cost trend at higher volumes; Autonomy risks	15

V. Coherence

What is the strongest interoperability/legal challenge to cross-border deployment?			
No	**Study question**	**Operationalisation**	**Weight**
5.1.	To what extent can the technologies generate synergies and/or compensate possible trade-offs among them?	Doctrinal interoperability judged by policy documents and experts	10
5.2.	To what extent is the development of these technologies coherent with European and international standards, including defence doctrines and political priorities?	Regulatory compliance with EU/ NATO standards; Qualitative assessment of the alignment with EU norms	

2. ANALYTICAL APPROACH AND METHODOLOGY

A two-step analytical approach was deployed:

1) We analysed the use of current and emerging defence capabilities in the Russo-Ukrainian war and the existing gaps in European defence capabilities.

2) We studied what targeted investments in European defence could deliver a force multiplier effect to existing European defence technology and deliver an asymmetric advantage over Russian developing military capabilities.

Methodology

Desk research

- Analysis of reports and studies on the technological innovations in cyber warfare, SATCOM, EW and drones, and their application in the full-scale invasion of Ukraine and other contexts.

- Analysis of reports on the current state of European and Russian defence production with a particular focus on emerging and digital technologies.

Interviews

The study team conducted 14 interviews with representatives of FEPS, the European Parliament, industry and independent experts. The interviews were semi-structured with a list of questions derived from the study questions and adapted to each particular group.

Number	Group	Organisation
1	Industry	Helsing
2	Industry	Airbus
3	Industry	Delian Alliance Industries
4	Industry	European Parliament
5	Industry	NVISO/DIGITAL EUROPE
6	Experts	Carnegie Europe
7	Experts	EUISS
8	Experts	CNA
9	Experts	Carnegie Endowment
10	Experts	Globsec
11	FEPS	FEPS
12	FEPS	FEPS
13	FEPS	FEPS
14	Policy	European Parliament

Endnotes

[1] Report of the Secretary-General on the impact of the global increase in military expenditure on the achievement of the Sustainable Development Goals as requested by Action 13 (c) of the Pact for the Future (A/RES/79/1).

[2] Landay, J. (2024) “Satellite photos show Russia plans to expand missile production, researcher says”. *Reuters*, 18 November.

[3] Beznosiuk, M. (2025) “Why Russia’s military moves in 2025 show it is not ready to stop”. *New Eastern Europe*, 14 May.

[4] Shurnov, D. (2025) “Putin instructed to prepare infrastructure, not to place weapons ‘in the open field’”. *Gazeta.ru*, 12 June.

[5] “On the approval of the Strategy for the Development of Unmanned Aviation in the Russian Federation for the period up to 2030 and with a view to 2035”. Government of Russia, 21 June 2023.

[6] Interviews with the FEPS representative, September 2025.

[7] “White paper for European Defence – Readiness 2030”. EEAS, 21 March 2025.

[8] Wolff, G. B., A. Burilkov, K. Buschnell et al. (2024) “Fit for war in decades: Europe’s and Germany’s slow rearmament vis-à-vis Russia”. Kiel report, September.

[9] Rhodes, C. (2024) “Small aircraft, sizeable threats: Preparing army to counter small uncrewed aerial systems”. Australian Army Occasional Paper no. 24. Australian Army Research Centre.

[10] Watling, J. and N. Reynolds (2025) “Tactical developments during the third year of the Russo–Ukrainian War”. Royal United Services Institute.

[11] Corbyn, Z. (2025) “Move fast, kill things: The tech startups trying to reinvent defence with Silicon Valley values”. *The Guardian*, 29 March.

[12] Krutov, M., S. Dobrynin and Y. Lehalau (2025) “Inside Rubicon, the elite Russian drone unit wreaking havoc on Ukraine’s troops”. *Radio Free Europe/Radio Liberty*, 17 September.

[13] “The EU’s critical tech gap: Rethinking economic security to put Europe”. Digital Europe, 2024.

[14] Bollfrass, A. K., E. Sabatino and C. Wiley (2025) “Space capabilities to support military operations in the European theatre”. IISS, 30 January.

[15] “How to get more bang for the buck in Western defence budgets”. *The Economist*, 25 May 2023.

[16] Soler, P. (2025) “EU remains ‘highly vulnerable’ and dependent on US Defence production - report”. *Euronews*, 20 June.

[17] Draghi, M. (2024) “The future of European competitiveness”. European Commission.

[18] “EU budget set for defence-related boost under new regulation”. Press release. European Commission, 22 April 2025.

[19] “European Defence Fund Regulation”. European Commission, 2025.

[20] Interviews with industry representatives (nos. 3 and 4) and experts (no. 6), September-October 2025.

[21] “EDF interim evaluation report”. DG DEFIS, 17 June 2025; N.-J. Brehon (2025) “Unsettling shifts in the European Defence Fund”. Schuman Papers no. 801. Fondation Robert Schuman, 9 September.

[22] “EDIP | a dedicated programme for defence”. European Commission.

23 “EDIP proposal for a regulation”. European Commission, 5 March 2024.

24 “Commission welcomes political agreement on the European Defence Industry Programme”. European Commission, 16 October 2025.

25 Interviews with policy representatives (nos. 4 and 14), September-October 2025.

26 “EDIRPA Work Programme”. Directorate-General for Defence Industry and Space of the European Commission, 2024.

27 “EU boosts defence readiness with first ever financial support for common defence procurement”. European Commission, 14 November 2024.

28 Mejino-Lopez, J. and G. B. Wolff (2025) “Boosting the European defence industry in a hostile world”. *Intereconomics*, 1(60):34-39.

29 “EIB steps up financing for European security and defence and critical raw materials”. European Investment Bank, 2025.

30 “EIB Board of Directors steps up support for Europe’s security and defence industry and approves €4.5 billion in other financing”. European Investment Bank, 8 May 2024.

31 “Defence Equity Facility: European Commission and EIF announce a €40 million investment in European defence and security Tech fund Keen Venture Partners”. Directorate-General for Defence Industry and Space of the European Commission, 2025.

32 Badohal, K. (2025) “European Investment Bank expects to double or triple defence spending in 2025”. *Reuters*, 13 March.

33 Interviews with a FEPS representative (no. 12) and an expert (no. 7), September-October 2025.

34 Interviews with a policy representative (no. 14), September-October 2025.

35 Clapp, S., M. Höflmayer, E. Lazarou et al. (2025) “ReArm Europe Plan/Readiness 2030”. European Parliamentary Research Service, April.

36 Clapp, S. (2025) “Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks”. European Parliamentary Research Service, May.

37 Franke, U. (2023) “Drones in Ukraine and beyond: Everything you need to know”. ECFR, 11 August.

38 Hambling, D. (2024) “Volunteers worldwide with 3D printers are aiding Ukraine’s war effort”. *Forbes*, 7 June.

39 Interviews with industry representatives (nos. 1 and 3) and experts (nos. 6, 8 and 9), September-October 2025.

40 “How will mines dropped by Drones Change Warfare?” *The Economist*, 31 January 2025.

41 Andrijanič, M. B. (2025) “A Western-funded drone surge could end Russia’s invasion of Ukraine”. Atlantic Council, 14 July.

42 Interview with an expert (no. 6), September-October 2025.

43 Interview with an expert (no. 9) and an industry representative (no. 3), September-October 2025.

44 Franke, U. (2025) “Drones in Ukraine: Four lessons for the West”. ECFR, 10 January.

45 Sutton, H.I. (2025) “Overview of maritime drones (USVs) of the Russo-Ukrainian war, 2022-24”. *Covert Shores*, 20 June.

[46] Sutton, H.I. (2025) “Seen for first time: Ukraine’s original naval drone”. *Naval News*, 30 July.

[47] Sutton, H.I. (2025) “First image of Ukraine’s sidewinder-armed Magura V7 surface drone”. *Naval News*, 4 May.

[48] Hodunova, K. (2025) “Russia-Ukraine naval drone arms race could ‘usher in a new era of warfare’”. *The Kyiv Independent*, 1 September.

[49] Jajcay, J. (2025) “I fought in Ukraine and here’s why FPV drones kind of suck”. *War on the Rocks*, 26 June.

[50] Bronk, J. (2025) “NATO should not replace traditional firepower with ‘drones’”. Royal United Services Institute, 4 August.

[51] “The Russia-Ukraine drone war: Innovation on the frontlines and beyond”. CSIS, 28 May 2025.

[52] Thrasher, B. (2024) “The war in Ukraine: How multi-domain formations are combatting Russia”. Pulse of Army Medicine.

[53] Interview with an expert (no. 8), September-October 2025.

[54] Ibid.

[55] Clapp, S. (2025) “Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks”.

[56] “Greece says Turkey must lift war threat to get access to EU defence funds”. *Reuters*, 22 May 2025.

[57] Clapp, S. (2025) “Military drone systems in the EU and global context: Types, capabilities and regulatory frameworks”.

[58] Ibid.

[59] Ibid.

[60] Franke, U. (2025) “Drones in Ukraine: Four lessons for the West”.

[61] Malyasov, D. (2025) “What Ukraine’s drones really cost”. Defence Blog, 2 July; Jajcay, J. (2025) “I fought in Ukraine and here’s why FPV drones kind of suck”.

[62] Andersson, J. S. J. and S. Simon (2025) “Minding the drone gap: Drone warfare and the EU”. European Union Institute for Security Studies, 11 October.

[63] Gray, A., S. Mukherjee and M. Hunder (2025) “EU scramble for anti-Russia ‘drone wall’ hits political, technical hurdles”. *Reuters*, 15 October.

[64] Kayali, L. (2025) “Germany’s Pistorius pours cold water on drone wall concept”. *POLITICO*, 29 September.

[65] Gray, A., S. Mukherjee and M. Hunder (2025) “EU scramble for anti-Russia ‘drone wall’ hits political, technical hurdles”.

[66] Interview with an expert (no. 9), September-October 2025.

[67] “The government approved draft law on defence and security industry”. *LR Krašto Apsaugos Ministerija*, 10 April 2024.

[68] Taksøe, C. and L. H. Lauersen (2025) “New Danish legislation provides fast-track framework for defence and emergency preparedness projects”. Bruun & Hjejle, 1 October.

[69] Gorman, S., A. Cole and Y. Dreazen (2009) “Computer spies breach fighter-jet project”. *The Wall Street Journal*, 21 April

[70] Greenberg, A. (2017) “‘Crash override’: The malware that took down a power grid”. WIRED, 12 June.

[71] “Danger close: Fancy bear tracking of Ukrainian field artillery units”. *CrowdStrike*, 22 December 2016.

[72] Fischer, B. B. (2014) “CANOPY WING: The U.S. war plan that gave the East Germans goose bumps”. *International Journal of Intelligence and Counter Intelligence*, 3(27): 431-464. DOI: 10.1080/08850607.2014.900290

[73] “Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine”. Canadian Centre for Cyber Security. Government of Canada, 14 July 2022.

[74] Healey, J. (2025) “Is cyber revolutionary or barely relevant in modern warfare?” War on the Rocks, 28 February.

[75] Kerttunen, M. and M. Schulze (2023) “Cyber operations in Russia’s war against Ukraine”. Comment C 23. Stiftung Wissenschaft und Politik, 17 April.

[76] Kirichenko, D. (2025) “Ukraine’s IT army is waging a crowdsourced cyber war against Russia”. *Small Wars Journal*, 24 March.

[77] “F6 has named the main cyber threats of 2025 — a detailed analysis of hacker groups attacking Russia and the CIS has been released”. *F6*, 19 February 2025.

[78] Interview with an industry representative (no. 5), October 2024.

[79] “Cybersecurity market analysis recommendations”. European Cyber Security Organisation, 2024.

[80] Dubois, L. (2025) “EU to ‘step up’ on cyber security as dependence on US laid bare”. *Financial Times*, 9 June.

[81] White, R. (2022) “How the cloud saved Ukraine’s data from Russian attacks”. *C4ISRNet*, 22 June.

[82] Sherman, J. (2025) “Hacking and firewalls under siege: Russia’s cyber industry during the war on Ukraine”. Center for Naval Analysis, August.

[83] Mueller, G. B., B. Valeriano, R. C. Maness et al. (2023) “Cyber operations during the Russo-Ukrainian war”. CSIS, 13 July.

[84] “EU allocates €145.5 million to boost European cybersecurity, including for hospitals and healthcare providers”. European Commission, 12 June 2025.

[85] Interview with an expert (no. 6), September 2025.

[86] Interview with policy and industry representatives (nos. 4 and 5), October 2024.

[87] Nicholls, C. (2025) “Man arrested in connection with cyberattack that disrupted European airports”. *CNN*, 24 September.

[88] “European Union and NATO hold the first structured dialogue on cyber”. European External Action Service, 4 October 2024.

[89] Watling, S. and N. Sylvia (2025) “Competitive electronic warfare in modern land operations”. Royal United Services Institute, 30 January.

90 Anderson, M. (2024) “GPS spoofing attacks are dangerously misleading airliners”. IEEE Spectrum, 29 December.

91 “Above us only stars: Exposing GPS spoofing in Russia and Syria”. C4ADS, 2019.

92 Halwa, S. and L. Harriss (2025) “Electromagnetic (electronic) warfare”. UK Parliament POST, 10 July.

93 Watling, S. and N. Sylvia (2025) “Competitive electronic warfare in modern land operations”.

94 Magnuson, S. (2024) “Daily fight for Ukraine spectrum superiority puts electronic warfare front, center”. National Defense, 8 March.

95 Radin, A., K. Holynska, C. Tretter et al. (2025) “Lessons from the war in Ukraine for space: Challenges and opportunities for future conflicts”. Research report. RAND, 21 May.

96 Slusher, M. (2025) “Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience”. CSIS, 2 May.

97 Interview with an expert (no. 9), September 2025.

98 Kochis, D. (2025) “Reducing the US force presence in Europe would weaken American interests”. *Hudson*, 23 September.

99 Bronk, J. (2025) “Airborne electromagnetic warfare in NATO: A critical European capability gap”. Royal United Services Institute, 19 March.

100 Interview with an expert (no. 8), September 2025.

101 Interview with an expert (no. 6), September 2025.

102 Melkozerova, V. and J. Posaner (2024) “Ukraine’s ‘people’s satellite’ wreaks havoc on Russian targets”. POLITICO, 1 July.

103 “Space defence strategy”. French Armed Forces Ministry, 2019.

104 Suess, J. (2024) “Between ambition and reality: How space fits into the UK defence framework”. Royal United Services Institute, 16 July.

105 Suess, J. (2024) “Space: The vital frontier”. Royal United Services Institute, 8 August.

106 Swope, C., K. A. Bingen, M. Young et al. (2025) “Space threat assessment 2025”. CSIS, 25 April.

107 Sankaran, J. (2022) “Russia’s anti-satellite weapons: A hedging and offsetting strategy to deter Western aerospace forces”. *Contemporary Security Policy*, 3(43): 436-463.

108 Ustinova, A. (2025) “Russian equivalent of Starlink to test communications in the Arctic”. Vedomosti, 14 March.

109 Ibid.

110 Radin, A., K. Holynska, C. Tretter et al. (2025) “Lessons from the war in Ukraine for space: Challenges and opportunities for future conflicts”.

111 Lapaiev, Y. (2025) “Ukraine prioritizes developing national satellite communications system”. The Jamestown Foundation, 10 April.

112 Epstein, J. (2025) “Ukraine says Russia’s new jet-powered attack drone is full of foreign parts and immune to electronic warfare”. *Business Insider*, 16 September.

113 Kayali, L. (2025) “Europe needs to up its space game to fend off Musk, Russia and China”. POLITICO, 4 May.

114 “Commission takes next step to deploy the IRIS² secure satellite system”. European Commission, 16 December 2024.

115 “EU space strategy for security and defence”. European Commission.

116 Geslin, L. (2025) “Europe back in space with new satellite launcher”. Euractiv, 3 March.

117 Interview with an expert (no. 7), September 2025.

118 “EU Space Act”. European Commission, 25 June 2025.

119 Miller, H. (2024) “Russia used exclave of Kaliningrad to disrupt EU satellites”. *Bloomberg*, 2 July.

120 Interview with an expert (no. 9), September 2025.

121 Segreti, G (2025) “Leonardo, Airbus, Thales to assess feasibility of space alliance by end-July”. *Reuters*, 17 June.

122 Posaner, J. (2024) “Brussels slams Berlin’s ‘ill-founded’ effort to delay EU satellite project”. POLITICO, 1 May.

123 John, A. (2025) “Anticipating AI’s impact on the cyber offense-defense balance”. Center for Security and Emerging Technology, May.

124 Interview with an industry representative (no. 2), September 2025.

125 Interview with an expert (no. 9), September 2025.

126 Lewis, C., I. Kristensen, J. Caso et al. (2025) “AI is the greatest threat—and defense—in cybersecurity today. Here’s why”. McKinsey & Company, 15 May.

127 “Off to the races: DRBE develops world’s largest real-time EW test range”. DARPA, 12 August 2025.

128 Interview with an expert (no. 10), September 2025.

129 Huyhn, C. (2025) “AI on the edge of space securing space superiority and avoiding surprise in orbit”. Center for Security and Emerging Technology, June.

130 Interview with an expert (no. 6), September 2025.

131 Interview with an expert (no. 9), September 2025.

132 Hay, G. (2025) “Breakingviews - tech can give Europe more bang for defence buck”. *Reuters*, 8 May.

133 Rees, R. (2025) “Ukraine’s ‘drone war’ hastens development of autonomous weapons”. *Financial Times*, 27 May.

134 MacDonald, A. (2025) “AI-powered drone swarms have now entered the battlefield”. *The Wall Street Journal*, 2 September; S. Pfeifer and P. Nilsson (2025) “Fully autonomous strike drones within technological reach, says German start-up”. *Financial Times*, 28 April.

135 Interview with a policy representative (no. 4), September 2025.

136 Tregub, C. (2024) “The AI Frontier: Ukraine’s role in the future of warfare”. *Friends of Europe*, 13 October.

137 Bondar, K. (2025) “Ukraine’s future vision and current capabilities for waging AI-enabled autonomous warfare”. CSIS, 6 March.

138 “Artificial intelligence and the defence sector”. DCAF – Geneva Centre for Security Sector Governance, 26 March 2025.

139 Ibid.

140 “Post-quantum cryptography”. European Union Agency for Cybersecurity (ENISA), 2021.

141 De Luca, S. and T. Marcelin (2024) “Cryptographic security: Critical to Europe’s digital sovereignty”. European Parliamentary Research Service, November.

142 Ibid.

143 Ibid.

144 Interview with an expert (no. 7), October 2025.

145 Saywell, J. C., M. S. Carey, P. S. Light et al. (2023) “Enhancing the sensitivity of atom-interferometric inertial sensors using robust control”. *Nature Communications*, 1(14): 7626. DOI: 10.1038/s41467-023-43374-0; Helsel, S. (2022) “REPORT: Bringing quantum sensors to fruition”. Inside Quantum Technology, 25 March.

146 “Cloud strategic roadmap for defence”. (2023) UK Ministry of Defence, 2 February 2023. Interviews with an expert and industry representatives (nos. 1, 2, 7 and 9), September-October 2025.

147 Goodrich, J. (2025) “Don’t be fooled, advanced chips are important for national security”. RAND, 10 February.

148 Schonfeld, Z. (2022) “Hundreds of Western components found in Russian weapons in Ukraine: Think tank”. *The Hill*, 8 August.

149 “2023 Report on the state of the Digital Decade”. European Commission, 27 September.

150 Interview with an industry representative and an expert (nos. 2 and 6), September 2025.

151 “Making the most of EU research and innovation investments: Rethinking dual use”. European Commission, 2025.

152 Sandbu M. (2025) “The EU’s secret weapon for economic success”. *Financial Times*, 18 September.

153 “European defense tech start-ups: In it for the long run?” McKinsey & Company, 12 February 2025.

154 “A Savings and Investments Union to finance Europe’s future”. DIGITAL EUROPE, 24 April 2025.

155 Debusmann, Jr., B. and D. Kaye (2025) “Trump adds $100,000 fee for skilled worker visa applicants”. *BBC*, 20 September.

156 Interviews with an industry representatives (no. 1), September 2025

157 “Supporting success: Over £4 million awarded for the adoption of PYRAMID on avionics and mission systems”. GOV.UK, 4 September 2025.

158 Jacobsen, S. D. (2025) “Ukraine’s Brave1 is racing to redefine warfare”. *International Policy Digest*, 23 April.

159 Interviews with FEPS representatives, September 2025.

160 “Questions and answers: Israeli military’s use of digital tools in Gaza”. Human Rights Watch, 10 September 2024.

161 Zelalem, Z. (2025) “Deadly skies: Drone warfare in Ethiopia and the future of conflict in Africa”. ECFR, 28 February.

About the authors

Kirill SHAMIEV

Kirill Shamiev is a Policy Fellow at the European Council on Foreign Relations. He focuses on Russia's civil-military relations and domestic politics and policymaking.

Prior to joining ECFR, Shamiev worked as a Senior Researcher at PPMI, a European consultancy company. He has extensive experience in designing, coordinating, and conducting studies and evaluations for the European Commission, including most recently a study to support the evaluation of the European Union Agency for Cybersecurity and the European cybersecurity certification framework, interim evaluation for the European Solidarity Corps, and analysis of organisational models in EU cohesion policy programme authorities (2000-2020) for DG CNECT, DG EAC and DG REGIO.

Shamiev holds a PhD in political science from Central European University. He is a founding member of the MethodsNET global network of methods experts in the social sciences and a member of the Inter-University Seminar on Armed Forces and Society. His work has been published in the Armed Forces and Society journal, Foreign Affairs, Foreign Policy and the Routledge Handbook of Russian Politics and Society.

Giorgos VERDI

Giorgos Verdi is a Policy Fellow with the European Power programme at the European Council on Foreign Relations. His research focuses on the implications of critical and emerging technologies for the EU's competitiveness, economic security, and foreign policy.

Before joining ECFR, Verdi was a policy advisor to the European DIGITAL SME Alliance, where he worked with high-tech small and medium enterprises and start-ups. He has also worked with the European Parliament and the Hellenic Foundation for European and Foreign Policy.

Verdi holds an MA in EU international relations and diplomacy from the College of Europe and a BA in international relations from the University of Piraeus.

ABOUT THE FOUNDATION OF EUROPEAN PROGRESSIVE STUDIES

The Foundation for European Progressive Studies (FEPS) is the think tank of the progressive political family at EU level. Its mission is to develop innovative research, policy advice, training and debates to inspire and inform progressive politics and policies across Europe.

FEPS works in close partnership with its 76 members and other partners -including renowned universities, scholars, policymakers and activists-, forging connections among stakeholders from the world of politics, academia and civil society at local, regional, national, European and global levels.

www.feps-europe.eu | X/Instagram: @FEPS_Europe | Facebook: @FEPSEurope

ON SIMILAR TOPICS

POLICY BRIEF
March 2025

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

EUROPEAN DEFENCE FOR SECURITY AND PEACE

ABSTRACT

The new geopolitical scenario requires the EU to create a European defence system, also as a European pillar of NATO. The EU urgently needs to develop an autonomous hard power, while also strengthening its traditional soft power. For security and economic reasons, the EU should prefer an integrated defence system to the mere coordination of national defences. Recent polls show that this is also the citizens' preference. A dual model, including an autonomous military capacity and the ability to draw and coordinate national forces, could be set up rapidly, exploiting the Permanent Structured Cooperation on security and defence. A European Defence Union requires adequate financing and democratic governance. EU defence shall be at the service of peace and could be partly put at the disposal of the UN. The EU needs to think out of the box and act with ambition and speed.

EDITED BY

ROBERTO CASTALDI
Associate Professor of Political Theory and Director of the Jean Monnet Centre of Excellence fEUture at eCampus University; Director of CesUE and of Euractiv Italia

IN PARTNERSHIP WITH

CesUE

POLICY BRIEF
November 2025

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

REARM EUROPE

THE IMPACT AND ROLE OF EU ARMS EXPORT CONTROLS

ABSTRACT

In response to the security challenges generated by Russia's full-scale invasion of Ukraine, the European Commission has launched several initiatives to boost rearmament in the EU. These include measures to strengthen the European Defence Technological and Industrial Base by means of facilitating joint arms production among EU member states. These measures call for both the simplification of existing regulations to facilitate the intra-EU transfers of defence products as well as an increased convergence of EU member states' arms export control policies.

The outcome and discussions taking place in the framework of the latest review of the EU common position on arms exports highlight the obstacles that any attempt to apply single market standards to intra-EU transfers of defence items will confront. There are increasing concerns about the negative impact that regulatory simplifications in this field could have, including the risk that exported weapons may be used to violate international law.

The EU and its member states should ensure that mechanisms to facilitate the intra-EU transfers of defence products and general efforts to boost rearmament plans are equipped with proper safeguards and transparency requirements in line with export control-related obligations. At the same time, this context also offers an opportunity to bridge EU internal discussions on intra-EU transfers and EU exports of military materiel.

AUTHOR

GIOVANNA MALETTA
Senior Researcher, Stockholm International Peace Research Institute (SIPRI)

IN PARTNERSHIP WITH

sipri

POLICY BRIEF
November 2025

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

MORE MONEY, MORE DEPENDENCE?

FINANCING EUROPEAN UNION DEFENCE FOR AUTONOMY AND COOPERATION

ABSTRACT

Europe is entering an era of unprecedented defence investment, with EU institutions and member states projected to spend nearly €6.8 trillion on defence by 2035. This surge comes amid a deteriorating security environment shaped by Russia's war on Ukraine, growing transatlantic uncertainty and intensifying dependencies on non-EU defence suppliers – particularly the United States. Against this backdrop, the EU has developed an expanding suite of financial instruments, including the European Defence Fund (EDF), the European Defence Industrial Programme (EDIP) and the Security Action for Europe (SAFE) loan facility, to strengthen the European Defence Technological and Industrial Base (EDTIB) and incentivise cross-border defence cooperation.

The objective of this policy brief is to assess whether these mechanisms effectively support the EU's strategic autonomy ambitions and to evaluate how Europe's financial architecture can better channel rising defence expenditure into cooperative, long-term capability development. The analysis finds that the EU has made significant progress, yet challenges remain. Despite the scale of new investments, the risk of renewed renationalisation persists as member states increasingly procure off-the-shelf non-EU systems and utilise fiscal exemptions to support national industries. Moreover, governance fragmentation at the EU level threatens to limit the effectiveness of emerging joint procurement tools. The success of the new EDIP, particularly with flagship European Defence Projects of Common Interest, will depend on substantial post-2027 funding and much tighter links between EU financing and binding commitments to joint capability development.

The brief concludes that to avoid financial integration becoming a vehicle for managed national competition, the EU must strengthen conditionality on cooperative procurement, prioritise EDPCIs within a significantly enlarged EDIP, improve oversight of SGP defence exemptions and develop a more coherent governance model that aligns the Union's diverse financing instruments with its long-term strategic autonomy goals.

AUTHOR

DANIEL FIOTT
Professor, Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussel (VUB)

POLICY BRIEF
March 2023

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

PROGRESSIVE PATHWAYS TO EUROPEAN STRATEGIC AUTONOMY

HOW CAN THE EU BECOME MORE INDEPENDENT IN AN INCREASINGLY CHALLENGING WORLD?

ABSTRACT

The debate on European strategic autonomy (ESA) has gained new momentum with Russia's invasion of Ukraine, even though the idea of European autonomy has been present throughout the history of EU integration. The main idea behind the concept of ESA is the EU's ability and means to enhance its freedom from a set of external dependencies – and also to enhance its freedom to conduct its policy autonomously and in line with its fundamental values and interests. Yet does the EU have the capacity and agency to set priorities and make decisions autonomously in its external action? What political, institutional, and material steps are needed to achieve strategic autonomy? Guided by these questions and in search of a progressive answer to them, FEPS, the Fondation Jean-Jaurès and the Friedrich-Ebert-Stiftung conducted a research project looking into three policy domains in which it is vital for Europe to attain the necessary freedom and wherewithal to pursue this objective of ESA: security and defence, economy and trade, and digital and technology. This policy brief summarises the main findings of our ESA research project. Overall, Europe must adapt to the new and challenging global realities. To do this, the EU needs to act with more unity and coordination in different domains, as well as to build resilience and reduce its external dependence on certain fundamental resources.

AUTHORS

DR ALINE BURNI
Policy Analyst on International Relations
FEPS

EDWARD KNUDSEN
Doctoral Researcher in International Relations University of Oxford & Affiliate Policy Fellow Jacques Delors Centre (Berlin)

JUSTIN NOGAREDE
Senior Policy Officer Friedrich-Ebert-Stiftung's Competence Centre on the Future of Work

DR NICOLETTA PIROZZI
Head of Programme on European Union and Institutional Relations Manager Instituto Affari Internazionali (IAI)

DR DAVID RINALDI
Director of Studies and Policy
FEPS

STRATEGIC AUTONOMY SERIES

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

POLICY BRIEF
December 2024

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

A FEMINIST FOREIGN POLICY APPROACH TO EU SECURITY AND DEFENCE

A CONTRADICTION IN TERMS

ABSTRACT

The global order is pronouncedly turbulent with multiple crises unfolding around us, including armed conflict and war. Russia's full-scale invasion of Ukraine and the war in Gaza have amplified the feeling of the EU and the rest of the world being insecure and vulnerable to military threat. Meanwhile, the EU has sought to prevent gendered inequalities and injustices through the adoption of Gender Action Plans and taking an active stance on the UN Women Peace and Security (WPS) Agenda. Several EU member states have adopted feminist foreign policies (FFPs), seeking to combine that move with increased military expenditure in times of instability in Europe. Seemingly, they see no contradiction in spending more money on defence and committing themselves to feminist global transformations. Similarly, the EU has adopted a range of initiatives aimed at enhancing its Common Security and Defence Policy (CSDP), with some of those initiatives containing a commitment to gender equality and justice globally.

While the EU is nowhere near adopting a full-scale feminist stance on defence and war, it could engage in a more thoroughgoing set of reflections on what an explicit feminist approach could bring to the EU as a global security actor and involve several stakeholders in such deliberations. Moreover, the Union's CSDP initiatives should be informed by intersectionality, taking cues from some of the member states' FFPs in this regard. This policy brief reflects on the specific question of whether it would be possible for the EU to adopt a feminist approach to security and defence policy, assessing the Union's feminist credentials to date, and providing a set of policy recommendations on the compatibility between FFP and enhanced military expenditure.

AUTHOR

DR ANNIKA BERGMAN ROSAMOND
Associate Professor of International Relations and Gender
The University of Edinburgh

FEMINIST FOREIGN POLICY PROGRESSIVE VOICES

IN PARTNERSHIP WITH

FRIEDRICH EBERT STIFTUNG
EU Office Brussels

POLICY BRIEF
April 2024

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

REDEFINING EUROPEAN ENGAGEMENT IN THE ISRAELI–PALESTINIAN CONFLICT

FROM FINANCIAL AID TO INSTITUTION BUILDING

ABSTRACT

The European Union (EU), once a peripheral observer of the Israeli–Palestinian conflict, has ascended to a role of considerable influence. The EU's engagement, once confined to delivering humanitarian and economic aid, has matured, particularly after the Oslo Accords, into a more proactive diplomatic force. Yet, despite these strides, it has regressed to being perceived as merely a financier, a "payer" rather than a "player". Today, the EU stands as the Palestinian Authority's premier financial ally, injecting upwards of €250 million per year, and it also represents over half of the funding for the United Nations Relief and Works Agency despite the recent suspension of pay. Additionally, it is Israel's predominant trade partner, encompassing 28.8% of Israel's trade in goods in 2022. With substantial economic clout and a reputation as a defender of human rights, the EU possesses both the resources and the moral imperative to actively champion peace and prosperity for both Palestinian and Israeli societies. However, the devastating terror attacks on 7 October 2023 and the consequent Israeli military response have prompted a moment of introspection for the EU, challenging it to reconcile humanitarian imperatives with the denunciation of violence, all while navigating the complex political landscape to rekindle the stalled peace process.

AUTHORS

ROBY NATHANSON
CEO of the Macro Center for Political Economics, Tel Aviv

ARIEL INDENBAUM
Senior researcher at the Macro Center, Tel Aviv