Wilfried
Martens Centre
for European Studies

Europe's New Security Architecture:

Ukraine as a Strategic Pillar of the Continent's Defence Future

Aliona Hlivco

Summary

June 2026

Since Russia's invasion of Ukraine in 2014, and the full-scale assault launched in 2022, Ukraine has transformed from a state struggling to defend itself into one of Europe's most capable and innovative military powers. Faced with the absence of a credible security umbrella, a weakened military and initially limited Western assistance, Ukraine has been forced to rely on ingenuity, rapid adaptation and technological innovation to survive.

After more than a decade of war, Ukraine has developed extensive expertise across multiple domains of modern warfare, including conventional kinetic operations, cyber warfare, and information and cognitive warfare. It has also pioneered significant advancements in automated aerial, maritime, ground and subsea systems, reshaping the future battlefield in real time. As a result, Ukraine is no longer solely a recipient of European security support but is increasingly emerging as a contributor to Europe's defence and deterrence capabilities.

While Ukraine's formal accession to the EU remains ongoing, integrating Ukraine into Europe's evolving security and defence structures is both viable and strategically necessary given the scale of the threats facing the continent. Ukraine offers critical battlefield experience, expertise in rapid defence innovation, and insights that could help shape the future European pillar of NATO and broader European defence policy.

Drawing on Ukraine's military capabilities, defence–industrial innovation and progress towards EU integration, this policy brief outlines pathways for positioning Ukraine as a central pillar of Europe's emerging security architecture.

Keywords Ukraine – EU defence integration – Hybrid warfare – European security architecture – Defence–industrial cooperation – Strategic resilience

Introduction

Since Russia's first invasion of Ukraine in 2014 and its full-scale assault in 2022, the Kremlin has demonstrated that its aggressive ambitions extend far beyond Ukraine's borders. What Europe faces is not a regional conflict, but a systemic challenge to the continent's security order. Russia is not simply waging war against Ukraine, it is actively testing the resilience, unity and political will of Europe as a whole.

This confrontation has evolved well beyond the battlefield. Alongside its kinetic campaign,[1] Moscow has deployed a broad spectrum of hybrid tools against the European states supporting Ukraine. What has emerged is, in effect, the 'weaponisation of everything': energy supplies, migration flows, food security and critical infrastructure have all been leveraged as instruments of coercion.[2] This has been reinforced by acts of sabotage, cyber operations, espionage, disinformation campaigns, and persistent attempts to interfere in democratic processes and deepen societal divisions. Much of this activity operates in the grey zone—below the threshold of conventional war—leaving European governments navigating ambiguity, often without clear or coordinated response mechanisms.[3]

What makes this challenge particularly stark is that it originates from Russia, whose economic weight is modest compared to that of the EU. Yet, through alignment—formal and informal—with actors such as Iran, North Korea and China, Moscow amplifies its reach within a wider axis of disruption.[4] These partnerships together bring capabilities that are economically, technologically and militarily significant, underscoring that Europe's security challenge is no longer singular but systemic and global in nature.

Europe's existing security architecture was not designed for this reality. While the EU embedded a mutual defence clause in Article 42(7) of the Treaty on European Union, efforts to build a fully fledged European defence union have repeatedly stalled, with hard security ultimately deferred to NATO. The Alliance remains indispensable. Yet, as hybrid threats evolve—accelerated by emerging

1 Kinetic warfare refers to military operations that involve the use of physical force to inflict damage, destroy targets, or achieve strategic objectives through direct military action.

2 EEAS, 'EU Response to Hybrid Threats' (2024).

3 European Commission, *Joint Framework on Countering Hybrid Threats*, Joint Communication, JOIN (2016) 18 final, 6 April 2016.

4 A. Kendall-Taylor and R. Fontaine, 'The Axis of Upheaval', *Foreign Affairs*, 23 April 2024.

technologies such as artificial intelligence—it is increasingly clear that traditional structures alone are insufficient. Security today demands not only deterrence, but resilience: the ability to anticipate, attribute, absorb and respond swiftly to disruptions across multiple domains.

Concurrently, the transatlantic relationship is entering a period of adjustment. That the American security guarantee is unconditional can no longer be assumed.[5] This does not diminish the importance of the US, but it does reframe the relationship. A more balanced partnership—one grounded in shared responsibility—is both necessary and overdue.

In this context, the EU is uniquely positioned to act. It possesses the political legitimacy, regulatory frameworks and financial instruments required to address long-standing structural weaknesses in European defence. The question is no longer whether Europe can afford to take greater responsibility for its own security, but whether it can afford not to.

Ukraine's experiences present a unique opportunity for Europe to draw on advanced battlefield and tactical knowledge accumulated over more than a decade of war. The country has not only withstood sustained aggression but has also conducted effective counter-offensives across the kinetic, cyber, informational and electronic domains. Its rapid innovation in unmanned systems—in aerial, land, maritime and subsea environments—is among the defining features of modern warfare, alongside its accelerated development of defence artificial intelligence (AI). Crucially, these technological advances have been complemented by the evolution of battlefield tactics, making the Ukrainian armed forces the most combat-experienced military on the European continent.

This combination of capability and experience represents a significant strategic asset for the EU as Ukraine advances towards accession. As a close security partner and a future member, Ukraine has the potential to materially strengthen the EU's defence posture. Realising this potential, however, will require sustained and targeted EU support for Ukraine's defence sector, enabling it not only to integrate effectively but also to continue resisting ongoing aggression. At stake is not only Ukraine's future but the security of the European continent as a whole.

[5] Munich Security Conference, *Munich Security Report 2025: Multipolarisation* (2025).

Ukraine as a pillar of Europe's emerging defence architecture

As Russia's full-scale invasion unfolded, Ukraine moved decisively towards European integration. In 2022 the European Council granted Ukraine official EU candidate status—an unprecedentedly rapid political decision, reflecting both the geopolitical urgency and Ukraine's strategic importance to the Union.[6] Since then, Kyiv has progressed steadily through the accession framework, advancing legislative alignment and deepening institutional integration despite wartime constraints.

One of the most notable areas of progress lies in Cluster Six of the accession process—external relations. According to Ukrainian diplomats based at the Mission of Ukraine to the EU in Brussels, substantial elements of this cluster have, in practice, already been achieved. This includes alignment with the Common Foreign and Security Policy (CFSP), as well as convergence with EU positions on trade policy, sanctions regimes, humanitarian assistance and development cooperation. Ukraine demonstrated near-complete alignment with EU sanctions against Russia, alongside consistent coordination on external security policy.[7] This indicates that Ukraine is already acting as a de facto contributor to the Union's foreign and security posture rather than as a future recipient of it.

In parallel, the EU has undergone a significant transformation in its own security role. The activation of the European Peace Facility to finance military assistance to Ukraine marked a watershed moment in EU policy, effectively positioning the Union as a security actor in its own right.[8] This has been complemented by efforts to expand joint procurement among member states, as well as new initiatives such as the Security Action for Europe[9] instrument and the broader ReArm[10] agenda, aimed at strengthening Europe's defence–industrial base.

Ukraine has become deeply embedded in these emerging frameworks. Under the Defence Industry Programme, the European Commission has outlined funding mechanisms to mobilise up to €131 billion in industrial capacity and research

6 European Council, *European Council Conclusions, 23–24 June 2022, EUCO 24/22 (24 June 2022).*

7 European Commission, *Ukraine Report 2025*, Staff Working Document, SWD (2025), 759 final, 4 November 2025.

8 Council of the European Union, 'European Peace Facility'.

9 European Commission, DG DEFIS, 'Security Action for Europe'.

10 S. Clapp et al., *ReArm Europe Plan/Readiness 2030*, European Parliamentary Research Service, Briefing PE 769.566 (April 2025).

funding within the 2028–34 budget framework.[11] The creation of a dedicated Ukraine pillar within these initiatives has been made possible by Ukraine's candidate status, which provides the legal and political basis for this early integration into the EU's defence–industrial structures. This evolution underscores that Ukraine's accession is no longer a distant prospect but an expected outcome. The key challenge now lies in structuring the defence and security integration in a way that precedes full EU membership.

Officials within the cabinet of the commissioner for enlargement indicate that Ukraine could participate in EU joint procurement mechanisms well before accession is finalised. Such participation would have both practical and strategic implications. Materially, it would enable Ukraine to become integrated into European supply chains, enhance interoperability and scale production. Politically, it would foster a shift in mindset on both sides, with Ukraine viewed not as an external partner, but as an integral component of the European system. Integration, in this sense, is inherently reciprocal.

Ukraine will need to continue aligning with the EU's foreign and security policy, accompanied by sustained progress on the rule of law, governance reforms and adherence to internal market regulations. Ukraine currently has restrictions on defence exports, and while these are justified under conditions of martial law, they present a structural obstacle to integration into EU defence supply chains. As noted by a senior European Commission official in a conversation with the author, Ukraine will need to develop a phased approach to easing these restrictions, enabling the controlled transfer of technology, expertise and intellectual property. Establishing secure, mutually beneficial frameworks for such exchanges will be critical for Ukraine to transition from a front-line innovator to a fully integrated component of Europe's defence–industrial ecosystem.

At the same time, Ukraine offers capabilities that the EU currently lacks. Its experiences in high-intensity warfare, rapid innovation cycles and operational adaptation provide a unique form of added value—particularly as the EU seeks to strengthen its own military and industrial capacity.

In a recent conversation, President of Global Affairs at Goldman Sachs Jared Cohen noted that Europe has entered a structural defence investment cycle, but he also emphasised that its success will depend on translating increased spending into industrial capacity and operational capability rather than fragmented procurement. He highlighted Ukraine's role as a critical source of innovation and

[11] European Commission, 'The 2028–2034 EU Budget for a Stronger Europe'.

battlefield learning, observing that for Europe it will be an existential matter to systematically integrate these lessons into its defence transformation.[12]

The following non-exhaustive list highlights where Ukraine's experience and innovation can be directly leveraged to strengthen Europe's defence architecture even prior to full EU membership.

Ukraine's critical capabilities as a foundation for the European Defence Union

Innovative defence sector

As the Iran war has shown, Ukraine can offer innovative solutions in asymmetric warfare due to its development of the drone sector and advances in electronic warfare. Of particular interest to the Gulf states are Ukraine's interceptor drones which have proven highly effective in countering Iranian Shaheds.[13] Not only could Ukraine supply drones to the EU or set up joint production in Europe, but it could also contribute its invaluable know-how and operational experience to the drone deployment strategies and tactics which are shaping modern warfare globally.

Ukraine is currently developing automated vehicles for the aerial, maritime, subsea and land domains for defence and interception, long-range offensive operations, reconnaissance, evacuation and so on.[14]

Ukraine has already established numerous joint ventures with the EU, European governments and private companies for technology sharing and the co-production of weapons systems and technology. These include multiple initiatives with German companies, such as Quantum Frontline Industries[15] and the Auterion–Airlogix

[12] J. Cohen et al., 'The Future of European Defense', *Goldman Sachs Global Institute,* June 2025.

[13] T. Kelly and M. Shiraki, 'Gulf States Eye Cheap Ukrainian Interceptor Drone as Iranian Attacks Drain Missile Stocks', *Reuters*, 7 April 2026.

[14] M. Halstian, 'A First Point View: Examining Ukraine's Drone Industry', *Georgetown Security Studies Review* (2025).

[15] Quantum Systems, 'Deliveries on Schedule: Quantum Frontline Industries Sends First Batch of Drones to Ukraine', Press Release, 1 April 2026.

joint venture for strike drone production.[16] Sweden's Saab has taken steps to begin cooperation with a number of Ukrainian companies for collaboration and joint production.[17] Romania has signed a strategic partnership with Ukraine which includes joint drone production,[18] Portugal[19] and Greece[20] have agreed to the joint production of sea drones, and the UK has begun Project Octopus[21] and the LYRA programme[22] for drone manufacturing. The deal between Ukraine's Culver Aerospace and Denmark's Copenhagen Global A/S has been the first of the joint ventures to formally authorise arms production within EU/NATO countries.[23] Numerous other initiatives and joint ventures have been agreed upon.

In order to realise this potential, Ukraine will need access to the EU market and support in the capitalisation of its defence sector. Building a trusted, reciprocal industrial relationship will accelerate innovation, strengthen the European defence–technological base and deliver mutual strategic advantage.

Defence AI

Ukraine's battlefield integration of AI-enabled systems[24] offers a practical foundation for EU–Ukraine cooperation on interoperable defence technologies and operational innovation.

Ukraine has emerged as a leader in defence AI. Leading US tech firms are testing their platforms and technologies in Ukraine and leaning on real-world battlefield conditions to refine their systems.[25]

---

16 D. Shumlianskyi, 'Germany's Auterion and Ukraine's Airlogix to Jointly Produce Autonomous Strike Drones', *Militarnyi.com*, 13 February 2026.

17 Saab, 'Saab and Joint Stock Company "Ukrainian Defense Industry" Sign Memorandum of Understanding', Press Release, 13 February 2026.

18 *Reuters*, 'Romania Signs Deal With Ukraine on Joint Defence Production Including Drones', 12 March 2026.

19 T. Myronyshena, 'Ukraine, Portugal Sign Partnership to Produce Sea Drones', *Kyiv Independent*, 20 December 2025.

20 V. Khomenko, 'Ukraine and Greece to Jointly Manufacture Naval Drones', *Militarnyi.com*, 18 November 2025.

21 T. Rozouvan, 'UK to Provide Ukraine With Thousands of Octopus Interceptor UAV's Each Month', *Janes.com*, 13 January 2026.

22 UK Government, 'Hundreds of Missiles Delivered to Ukraine Months Ahead of Schedule as UK Leads Kyiv Trade Delegation', Press Release, 10 October 2025

23 V. Litnarovych, 'Denmark Makes History: First NATO State to Host Ukrainian Arms Production', *United24*, 3 December 2025.

24 K. Bondar, *Ukraine's Future Vision and Current Capabilities for Waging AI Enabled Autonomous Warfare*, CSIS (6 March 2025).

25 E. Bienvenue et al., 'Private Tech Companies, The State and the New Character of War', *Carnegie Endowment for International Peace*, 1 December 2025.

Ukraine has introduced operational battlefield platforms such as DELTA[26] which provides real-time situational awareness of enemy capabilities, and VEZHA[27] which integrates continuous feeds from across the battlefield, including data gathered from deployed drone systems. These are just two examples of systems deployed at scale, with many others in development—including systems designed to enhance decision-making in command and control, as well as in intelligence, surveillance and reconnaissance.

Harnessing Ukrainian defence AI capabilities would give the EU a competitive edge in this sector and therefore has the potential to make it a global military power. The EU is already supporting Ukrainian innovation through the European Innovation Council's recent award of €20 million to fund 41 Ukrainian startups and small and medium-sized enterprises.[28] Additional targeted funding and scaling mechanisms for defence AI startups, including access to EU innovation programmes and venture financing would be beneficial.

The EU has also taken significant steps to link Ukrainian and EU defence, academic and industrial ecosystems under the European Defence Industry Programme, with the recent announcement of a €1.5 billion work programme aimed at strengthening the defence industries, including the defence AI domain.[29]

European Defence Force

Ukraine fields approximately 800,000 personnel across its armed forces, the vast majority of whom have direct combat experience.[30] As hostilities subside, this will constitute one of the largest cohorts of combat-tested veterans in Europe. These individuals could serve as the foundation for the much-discussed European Defence Force (EDF)—providing it with combat experience in technologically advanced, asymmetric warfare.

---

26 Ukraine, Ministry of Defence, 'Order on Implementing DELTA Provides Defence Forces With Legal Framework for the System's Wide-Scale Use: Denys Shmyhal' (8 October 2025).

27 K. Chernoherenko, 'The Battlefield Video Analysis Platform Known as VEZHA Is Now Accessible Within the DELTA Combat System', Ministry of Defence of Ukraine, 14 October 2024.

28 European Innovation Council, 'Commission Boosts Support to Ukraine Deep Tech Innovators' (1 April 2026).

29 Ukraine, Ministry of Defence, 'EU Launches €1.5 Billion Programme for the Development of the Defence Industries, Including Funding for Ukrainian Drones, Ammunition, and Innovation' (2 April 2026).

30 W. Merrow and M. Bricknell, 'Comparing the Size and Capabilities of the Russian and Ukrainian Militaries', *Council on Foreign Relations*, 3 June 2025.

Ukraine is already at the forefront of modern battlefield practice, including drone operations,[31] electronic warfare[32] and ground-based air defence.[33] The nation is well placed to contribute to training, doctrine development and operational innovation in these domains. Furthermore, Ukrainian personnel could, over time and under the appropriate political framework, be integrated into European training missions and advisory roles along the EU's eastern flanks and into its central military formations, including the EU Military Committee.

Since joining the Joint Expeditionary Force as an associate partner, Ukraine has contributed to the planning of multinational military exercises, thereby enhancing operational effectiveness.[34] Its unique operational insights—including understanding adversary behaviour, battlefield psychology and decision-making processes—inform doctrine, tactical thinking and the use of asymmetrical approaches alongside advanced technological capabilities. Integrating Ukraine into high-level command, control, communications, computers, intelligence, surveillance and reconnaissance coordination centres would be a crucial step in strengthening Europe's readiness and resilience in the event of armed conflict.

Europe will need to complement this foundation with its own military personnel—approximately 1.3 million active troops across the EU member states—bringing the total towards a potential 2-million-strong European force. However, sustained funding for the Ukrainian armed forces would also be necessary, alongside the development of a structured long-term military career model for Ukrainians (i.e. the professionalisation of the Ukrainian forces and the introduction of a retention system).

Espionage, sabotage and strategic disruption

As I argued in my 2024 paper for the Baltic Defence College's Annual Russia Conference,[35] Ukraine has long been exposed and highly vulnerable to Russian espionage, sabotage and hybrid warfare campaigns, and it has developed robust resilience mechanisms in response. Since 2022 European states have experienced

[31] J. Hakmeh, 'What Ukraine Can Teach Europe and the World About Innovation in Modern Warfare', *Chatham House*, 5 March 2025.

[32] M. Slusher, 'Lessons From the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information and Resilience', *CSIS*, 2 May 2025.

[33] G. Di Mizio and M. Gjerstad, 'Ukraine's Ground-Based Air Defence: Evolution, Resilience and Pressure', *IISS*, 24 February 2025.

[34] J. Healey, 'Joint Expeditionary Force Launches Enhanced Partnership With Ukraine as Allies Step Up Further', UK Ministry of Defence, 5 November 2025.

[35] A. Hlivco, 'Russia's Wartime Influence Inside Ukraine', in S. Šrāders and G. T. Terry (eds.), *The Paradox of Power: Ukraine's Struggle, Russia's Dilemmas, and Global Consequences. The Conference of Russia Papers 2024* (Baltic Defence College, 2024).

an increase in covert activities attributed to Russian state actors, ranging from the physical sabotage of infrastructure (including undersea cables, rail links and industrial facilities) to espionage and information operations aimed at exploiting vulnerabilities in civil and military systems.[36]

Ukraine's experience in quickly identifying, countering and mitigating these threats—including institutionalising cross-domain intelligence, resilient logistics and civilian–military countermeasures[37]—represents vital expertise for its European partners which are now confronting similar risks. By sharing the lessons learned on threat detection, attribution, and rapid response to espionage and sabotage, Ukraine could help to strengthen European resilience against hybrid threats that seek to disrupt political cohesion and critical infrastructure.

Ukraine recognises the need to deepen intelligence cooperation within a small group of key partners, following a model similar to the Five Eyes alliance. This reflects growing uncertainty regarding the long-term reliability of US intelligence support and underscores the importance of building a more resilient, European-centred intelligence framework.

Ukraine's contribution would include its extensive experience in intelligence gathering, analysis and counter-intelligence operations against Russia, as well as real-time insights into adversary tactics, hybrid operations and battlefield developments. Ukraine could provide valuable expertise in threat detection, attribution and operational intelligence, particularly in relation to Russian activities across Europe.

An EU–Ukraine partnership could create a two-way learning environment, wherein Ukraine could share front-line experience in countering espionage and sabotage,[38] while Europe contributes methodological, technical and legal frameworks aligned with NATO and EU standards for responsible human-centric intelligence operations. The EU could perhaps call upon its lessons learned and experience of signals intelligence integration and intelligence-sharing structures, such as the Maximator Alliance,[39] to shape a future partnership.

---

36 C. Bailey, 'Are We at War With Russia? How Warden's Rings Map Russia's Hybrid Strategy', *RUSI*, 4 December 2025.

37 A. Romandash, *Hybrid Warfare: Ukraine, Russia and Western Lessons*, Centre for International Governance Innovation (29 September 2025).

38 N. Gurkov, *Behind the Lines: How Ukraine Has Outgunned Russia in Sabotage*, ACLED, 27 November 2025.

39 B. Jacobs, 'Maximator: European Signals Intelligence Cooperation From a Dutch Perspective', *Intelligence and National Security* 35/5 (2020).

Such a partnership would lay the foundation for a European intelligence alliance, strengthening strategic autonomy and ensuring the continuity of intelligence capabilities in an increasingly uncertain security environment.

Significant intelligence sharing is already taking place. In the wake of the US cutting off intelligence flows last year, France has stepped up to fill many of the gaps.[40] In January French President Emmanuel Macron claimed that France is currently providing Ukraine with two-thirds of its intelligence, largely that of 'technical origin', from sources such as satellite imagery and early warning systems detection.[41]

Disinformation

Ukraine has developed significant expertise in countering disinformation, with several AI-powered platforms and comprehensive strategic communication campaigns designed to detect Russian disinformation, bot networks and microtargeting operations.[42] These platforms and strategies are already collaborating with the UK's Ministry of Defence and Foreign, Commonwealth and Development Office,[43] as well as NATO,[44] providing real-time analysis and verification of online narratives that threaten national and European security.

The integration of Ukraine into EU resilience structures and the provision of assistance to scale Ukrainian-developed programmes, platforms and initiatives aimed at detecting and mitigating disinformation would strengthen the EU's ability to deal with disinformation. These solutions could be introduced and coordinated at a pan-European level, strengthening collective capabilities against hybrid threats.

Such cooperation is essential to counter the rise of radical political movements, which adversaries often exploit by amplifying social divisions and domestic vulnerabilities within European societies and allies.[45] Disinformation campaigns from Russia have been highly effective in swaying considerable portions of the

40 J. Irish, 'Macron Says France Now Providing Two Thirds of Intelligence to Ukraine', *Reuters*, 15 January 2026.

41 Ibid.

42 R. Van Leeuwen, 'What We Can Learn From Ukraine About Countering Disinformation', *Westminster Foundation for Democracy*, 24 July 2023.

43 UK Foreign, Commonwealth and Development Office, *Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy* (19 September 2025).

44 H. Padalko, 'AI for Freedom: Ukraine's Digital Strategy in the Information War', *Forum for Ukrainian Studies*, 28 November 2025.

45 E. Treyger, J. Cheravitch and R. S. Cohen, *Russian Disinformation Efforts on Social Media*, RAND (7 June 2022).

world's opinion against Europe and its allies.[46] Many key academics and industry experts are of the opinion that Russia is winning the global information war.[47]

With the rapid advancement of agentic AI and large language models—and the increasing availability of underlying datasets—disinformation campaigns are expected to grow in scale and sophistication, making coordinated European responses an urgent priority in the coming years.[48]

Societal resilience and civil preparedness

Ukraine has developed exceptional societal resilience[49] in response to the sustained Russian aggression, underpinned by strong civilian–military cooperation, decentralised digital governance, and the rapid mobilisation of volunteer networks supporting logistics, humanitarian response and national defence. Institutional mechanisms for crisis management, continuity of government and the protection of critical infrastructure have been tested under real wartime conditions,[50] offering valuable lessons for European partners facing growing hybrid threats. This experience aligns with the recommendations of Sauli Niinistö on strengthening whole-of-society resilience across Europe.[51]

Cybersecurity

Ukraine has developed extensive cyber-defence expertise through continuous exposure to sophisticated Russian cyber operations since 2014. The year 2024 saw Ukraine face a 70% surge in cyber-attacks targeting critical civilian and defence infrastructure, yet the number of these attacks that succeeded and inflicted serious damage fell sharply due to Ukraine's growing experience and expertise in combating Russian cyberwarfare.[52] This operational experience would make Ukraine a valuable partner for Europe as it could share its expertise with the operational cyber units and the Computer Emergency Response Team of Ukraine, which detect, analyse and mitigate threats in real time.

---

46 D. Presl, 'Russia Is Winning the Global Information War', *RUSI*, 7 May 2024.

47 Ibid.

48 A. M. Fitz-Gerald and H. Padalko, 'The Need for a Strategic Approach to Disinformation and AI Driven Threats', *RUSI*, 25 July 2024.

49 Swedish Civil Contingencies Agency, *Building Resilience for the Future: Lessons From Ukraine* (September 2023).

50 Ibid.

51 EU, 'Niinistö Report: Shifting From Crisis Response to Resilience' (31 October 2024).

52 L. Williams, T. Rajic and K. Badgi, 'Unpacking Ukraine's Future Cyber and Space Forces', *CSIS*, 20 October 2025.

Ukraine is already providing EU and NATO partners with insights into Russian cyber tactics, techniques and procedures.[53] Ukraine is an active participant in the implementation of the EU's Network and Information Systems Directive,[54] and the fourth EU–Ukraine Cyber Dialogue in October 2025 saw both sides pledge to deepen cooperation in countering cyber threats and strengthen the EU's collective response to cyber-attacks.[55] Additionally, Ukraine has engaged in numerous successful initiatives with private industry throughout Europe and other allied nations to develop and bolster its cybersecurity capabilities.[56] It also operates AI-driven platforms for monitoring vulnerabilities and detecting attacks and these have already been integrated into allied systems.[57]

Space

Ukraine enjoys a strong legacy in space, having been at the forefront of space engineering in the Soviet Union and responsible for roughly one-third of its rocket industry, producing key intercontinental ballistic missiles, satellites and other space technologies.[58] The Dnipro region was central to the USSR's space and rocket sector: Dnipro city, commonly known as 'Rocket City', was home to the Yuzhmash factory, the Yuzhnoye Design Bureau and the Pivdennyi (now Pivdenmash) Machine Building Plant, the latter often considered the birthplace of ballistic missiles.[59] Many of these companies and facilities still exist today.

Ukrainian defence enterprises such as the Luch Design Bureau and Motor Sich[60] still employ engineers widely recognised as among the most talented in the post-Soviet space.[61] These companies have contributed to the development of rocket, cruise and ballistic missile technologies, demonstrating the capacity to produce advanced systems, such as the R-360 Neptune anti-ship missile,[62] the

53 L. Ilves, 'Ukraine Teaches Europe Cyber Lessons', Centre for European Policy Analysis, 20 March 2025.

54 European Commission, 'NIS2 Directive: Securing Network and Information Systems'.

55 European Commission, 'EU and Ukraine Deepen Cooperation on Cyber Security at 4th Cyber Dialogue' (18 October 2025).

56 L. Axon et al., 'Private Initiatives for Public Cybersecurity in Ukraine', *Journal of Cyber Policy* (2025).

57 O. Tokariuk, 'Ukraine's Secret Weapon: Artificial Intelligence', *Centre for European Policy Analysis*, 20 November 2023.

58 S. Berezutsky, 'Why Ukraine Is a Space Nation', *Ukraine World*, 14 June 2022.

59 V. Toporkova, 'Ukraine, the Overlooked Powerhouse of Missile Production', *United 24 Media*, 27 August 2024.

60 *Ae.metu.edu*, 'Information About Ukrainian Space Industry. Composition of the Ukrainian Space Industry'.

61 Toporkova, 'Ukraine, the Overlooked Powerhouse of Missile Production'.

62 I. Kabachynskyi, 'What You Need to Know About Ukraine's Own Neptune Missile', *United 24 Media*, 5 June 2024.

FP-5 and the Flamingo cruise missile, efficiently and cost-effectively.[63] Sharing this experience in the design, manufacture and integration of space-capable systems, along with Ukraine's experience in countering Russian electronic warfare threats, could support European initiatives to establish resilient space operations.

The importance of public–private partnerships in the new security architecture

Contemporary strategic competition is increasingly defined by a technological race in which private actors are not merely suppliers, but central to the projection of state power. From the outset of Russia's full-scale invasion, leading technology firms moved rapidly to support Ukraine, securing critical government data, mitigating large-scale cyber-attacks, and enabling advanced intelligence and operational capabilities. Their involvement has demonstrated that the resilience and effectiveness of modern states in wartime are now deeply contingent on access to privately developed digital infrastructure, cloud services and data analytics.

The role of private companies has in some cases extended beyond support into direct strategic impact. A notable example is Starlink, whose satellite communications network has been critical to maintaining Ukrainian battlefield connectivity. Decisions regarding the availability of such systems have had immediate operational consequences on the battlefield, including the achievement of some of Ukraine's most significant territorial gains in the past year, as of early 2026.[64]

Microsoft stepped in to help Ukraine during the early stages of the invasion. In February 2022 Microsoft protected Ukraine from the destructive 'FoxBlade' cyber-weapon, while coordinating with US and European authorities and sharing intelligence at a classified level.[65] The company then provided real-time alerts, malware analysis and incident response to Ukrainian authorities, as well as helping to counter disinformation and influence operations. The critical element in helping the Ukrainian state to survive

63 F. Hoffman, 'Flight of the Flamingo Spells Trouble for Russia', *Centre for European Policy Analysis*, 8 September 2025.

64 *France 24*, 'Ukraine Makes Fastest Battlefield Gain in 2.5 Years', 16 February 2026.

65 B. Smith, 'Digital Technology and the War in Ukraine', *Microsoft*, 28 February 2022.

was moving the government's data to secure cloud servers abroad. By 2024 Microsoft had effectively provided $540 million in aid to Ukraine.[66]

The biological threat is another area where public–private partnership between a company, Perimeter (formerly Gingko Bioworks), and the Ukrainian government, in this case the Ministry of Health, has played an important role. War degrades infrastructure, strains healthcare systems, displaces populations and creates surveillance blind spots that adversaries can exploit, whether deliberately or inadvertently. According to Max Breet, the senior director for Europe, the Middle East and Africa at Perimeter, advances in synthetic biology and the wider democratisation of biotechnology are lowering the barriers to engineering and deploying biological agents. Capabilities that were once restricted to advanced state programmes are becoming increasingly accessible to a broader range of actors. Detection and response systems, by contrast, have not kept pace.

Operating continuously throughout the conflict, Perimeter has built what is arguably one of the most advanced bio-surveillance architectures currently deployed anywhere. This includes genomic surveillance across 15 oblasts, an advanced sequencing capability, a 200-pathogen viral surveillance system and increasingly automated laboratory workflows. A key component of the programme is its dedicated research on war-wound infections—work that directly informs treatment protocols and has clear implications for protecting the health of NATO forces.

In a hybrid warfare context—where attribution is deliberately obscured and thresholds are ambiguous—a biological event could unfold well before a consensus is reached on its origin. That ambiguity is itself a strategic tool. What Perimeter has demonstrated in Ukraine is that persistent, software-enabled environmental surveillance can significantly compress that uncertainty window, but that this capability must be in place before an event occurs; it cannot be built reactively. The insights gained in Ukraine—the most instructive operational setting available—will shape how Europe and NATO design biosecurity infrastructure for decades. Concurrently, Breet notes that private companies should not replace state capacity—rather they should act as force multipliers. Governments must retain strategic direction and oversight, but trusted private partners should be embedded from the outset in planning, exercises and operational response, rather than being introduced later on in the game through procurement processes.

66 L. Basset, 'Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare', *Cambridge Journal of Political Affairs* 5/1 (2024).

Palantir's engagement in Ukraine illustrates the emergence of private technology firms as core operational actors within modern warfare, rather than as peripheral enablers. As Louis Mosley, the executive vice-president for the UK, Europe and the Middle East at Palantir, explains, the company's involvement began indirectly through its integration into US military command structures, where its software underpinned the flow of Western intelligence and logistics support to Ukraine. This positioned Palantir at the centre of early intelligence-sharing, providing Ukrainian forces with actionable outputs—particularly targeting coordinates—well before direct bilateral cooperation was established. Subsequent engagement with Kyiv, driven at the highest political level, led to Palantir becoming embedded directly within Ukrainian systems, navigating institutional fragmentation to identify where its software could deliver decisive operational value.

Operationally, Palantir's contribution has centred on data integration and the targeting cycle at the strategic level. Mosley highlights that Ukrainian forces have developed a hybrid ecosystem in which Palantir's platforms support the fusion of satellite imagery, signals intelligence and other data streams into a common intelligence picture, while also enabling strategic targeting. Crucially, this capability is sustained by a dedicated Ukrainian unit composed largely of software engineers, who continuously adapt and build applications on top of the Palantir stack. This model—combining commercial cloud infrastructure, AI-enabled tools and front-line iteration—has enabled Ukraine to operationalise emerging technologies at speed, creating a level of battlefield integration and adaptability that most European militaries currently lack.

The implications for the European security architecture are stark. Ukraine, the US and Israel are currently the only actors able to deploy advanced AI-enabled military data systems at scale. European states lack the underlying cloud infrastructure and secure environments required to operationalise such capabilities. This is creating a growing interoperability gap within NATO and European states risk becoming strategically irrelevant if it remains unaddressed. Mosley's argument is that the private sector's involvement is therefore not optional but essential, given that the critical expertise—particularly in AI and data infrastructure—resides outside governments. At the same time, he cautions that this must be balanced with democratic accountability: decisions over the deployment of such technologies in conflict must remain with elected governments, not private companies, even as those companies become increasingly embedded in the conduct of war.

A decisive advantage in novel technologies now translates directly into strategic advantage in the theatre of hybrid war. The war in Ukraine has shown that private-sector innovation can anticipate unconventional threats, deliver battlefield-relevant capabilities at speed and materially shape the outcome of military campaigns—highlighting a structural shift in which critical technological advantages are increasingly generated outside of state structures. For Europe, this creates both urgency and opportunity: while the pursuit of technological sovereignty remains a valid long-term objective, it cannot come at the expense of immediate operational effectiveness. Europe must therefore adopt a pragmatic approach that embeds public–private cooperation within its security architecture, leverages existing innovation and ensures rapid access to cutting-edge capabilities.

Policy recommendations: defence cooperation

Strengthen and integrate Ukraine's defence innovation ecosystem

The EU should establish a dedicated framework to capitalise Ukraine's defence sector, including providing targeted funding for defence startups through the Security Action for Europe mechanism and facilitated access to the EU market. This should be paired with the expansion of trusted joint ventures and public–private partnerships, enabling structured sharing of intellectual property from Ukraine's battlefield-driven innovations and Europe's advanced capabilities in high-precision and long-range systems.

The EU should also support Ukraine in securing resilient supply chains for dual-use technologies, including semiconductors, fibre optics and critical raw materials, to reinforce defence production.

Under the same auspices, the Union should deepen education and knowledge-exchange frameworks linking Ukrainian and European defence, academic and industrial ecosystems, building on initiatives under the European Defence Industry Programme, to accelerate capability development and technology transfer.

Finally, the EU should advance a values-based AI regulatory framework that aligns with European standards while remaining sufficiently flexible to support rapid innovation and battlefield adaptation.

Develop an EDF based on Ukraine's armed forces

The EU, together with Ukraine, should move towards establishing a European defence capability by integrating Ukraine's over 800,000 battle-ready personnel and the approximately 1.3 million active troops across the EU member states into a coherent, interoperable force structure.

This would require sustained EU funding for the Ukrainian armed forces, alongside the modernisation of military bases and infrastructure, the development of a collective European air defence, and comprehensive veteran support and rehabilitation systems.

Integration should be underpinned by NATO-standard training, command-and-control structures and operational practices, ensuring full interoperability and significantly enhancing the effectiveness of the combined European forces.

Build a structured European intelligence partnership with Ukraine

The EU should establish a structured intelligence-sharing framework with Ukraine, enhancing coordination among intelligence, security and law-enforcement agencies, supported by the provision of advanced capabilities in signals intelligence, data processing and analysis. This partnership should operate as a two-way exchange, combining Ukraine's front-line experience in countering espionage and sabotage with European methodological, technical and legal standards which align with NATO and EU frameworks for responsible, human-centric intelligence operations.

Over time, this framework should evolve into a European intelligence alliance, incorporating other trusted partners to strengthen strategic autonomy and ensure resilience in an increasingly contested security environment.

Enhance cooperation on countering disinformation

The EU and Ukraine should establish structured knowledge exchanges and joint operational frameworks to counter disinformation, strengthen early warning systems and enable coordinated responses to hybrid threats. These should include shared practices, real-time information exchange and integrated analytical capabilities to improve detection, attribution and response across the European information space.

Integrate Ukraine into European civil protection and resilience frameworks

The EU should support Ukraine's integration into European civil protection and resilience mechanisms, and this should be complemented by a structured knowledge exchange on strategic communications, crisis governance and social cohesion. This partnership would strengthen Europe's capacity to withstand and recover from large-scale disruptions while embedding Ukraine's front-line experience into a broader, values-based resilience model.

Strengthen EU–Ukraine cyber resilience and cooperation between computer emergency response teams

The EU should integrate Ukrainian cyber teams into European cyber-resilience structures, including by enhancing cooperation between national computer emergency response teams, to improve collective monitoring, early warning and incident-response capabilities. Given Ukraine's position among the world's leading cyber-defence actors, its operational expertise should be systematically embedded into EU frameworks, including implementation of the Network and Information Systems Directive, where cooperation is already emerging. The EU should further provide technical assistance, platform development and structured knowledge exchange mechanisms to scale Ukrainian cyber innovation across Europe. Joint training programmes and exercises should be expanded to leverage Ukraine's front-line experience, significantly enhancing Europe's preparedness against hybrid and cyber threats.

Integrate Ukraine into EU space and satellite security initiatives

The EU should include Ukraine in key space programmes such as IRIS²[67] and Galileo[68] through structured knowledge-sharing, joint training and operational collaboration. Coordination through the Directorate-General for Defence Industry and Space (DG DEFIS) should ensure that Ukrainian expertise contributes to the resilience and security of Europe's space infrastructure, while enabling Ukraine to access EU standards, operational procedures and secure communications systems.

---

[67] IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) is the EU's planned multi-orbit satellite constellation, designed to provide secure communications, high-speed connectivity and strategic digital sovereignty for governments, businesses, and citizens across Europe and beyond.

[68] Galileo is the EU's global satellite navigation and positioning system, designed to provide highly accurate and secure timing, naivigation and location services for civilian and governmental use worldwide.

The EU should also leverage Ukraine's significant legacy and contemporary space and missile engineering capacity to strengthen Europe's technical expertise, production capability and systems resilience. In return, structured cooperation would provide Ukraine with targeted investment and technological support to modernise its space sector and develop the sovereign intelligence, surveillance and reconnaissance capabilities essential to national and European security.

Embed public–private partnerships within Europe's new security architecture

The EU should leverage Ukraine's proven experience in mobilising public–private partnerships in advanced technology and defence innovation, embedding similar mechanisms more systematically within Europe's security architecture. This requires a pragmatic approach that accelerates cooperation with private-sector innovators, ensures access to cutting-edge technologies, and integrates them into defence planning and procurement cycles.

To address the growing interoperability gap within NATO and enhance operational coherence, the EU should develop a shared secure cloud and digital infrastructure, enabling trusted data exchange, scalable innovation and the secure deployment of dual-use technologies across member states and partners. This would strengthen Europe's technological sovereignty while preventing fragmentation and strategic obsolescence in the rapidly evolving domains of modern warfare, while also ensuring that its democratically elected governments—not private companies—retain the key decision-making authority over emerging technologies.

Institutional pathways to Ukraine's integration into the European security architecture

Ukraine's integration into the European defence and security structures is no longer prospective—it is already underway. Since 2022 Kyiv has moved from a partner framework into operational, industrial and increasingly institutional integration with the EU's security architecture. This evolving baseline creates the conditions for a phased transition from participation to institutional embedding across the EU's defence governance ecosystem.

European External Action Service and political coordination

Ukraine's interaction with the European External Action Service (EEAS) has already evolved beyond standard third-country engagement. Regular coordination on sanctions, diplomacy and crisis response has created a de facto strategic dialogue framework. The next steps for this coordination could be the establishment of a dedicated Ukraine desk within the EEAS's Security and Defence Directorate, Ukraine's formal inclusion in crisis-response planning consultations, and its integration into EU hybrid threat and strategic communications coordination. Such mechanisms would formalise Ukraine's role as a co-shaper of European security policy, rather than a passive partner.[69]

Political and Security Committee

The Political and Security Committee (PSC) remains the core decision-making body for the EU's CFSP. While full participation is legally restricted, Ukraine is already involved through PSC+ formats on Ukraine-related dossiers.

The viable next step would be to grant Ukraine's ambassador permanent observer status. This would ensure Ukraine's consistent representation in important discussions, enable its early input into EU crisis-management decisions, and bridge the gap between operational integration and political participation. This model follows established EU practice with close partners and avoids the need for treaty change.[70]

EU Military Committee

The EU Military Committee,[71] composed of member states' chiefs of defence, represents the highest military authority within the EU. Ukraine's current engagement is indirect, primarily via the EU Military Assistance Mission and NATO-linked coordination channels. A logical next step would be to grant Ukraine's chief of defence observer status for relevant sessions, as well as enabling Ukraine's structured inclusion in lessons-learned and capability-development processes.

Given Ukraine's unparalleled battlefield experience, such integration would not only benefit Kyiv but also significantly enhance EU military planning and readiness.

---

69 EEAS, 'EU–Ukraine Relations'.

70 European Council, 'Political and Security Committee'.

71 European Council, 'European Union Military Committee (EUMC)'.

DG DEFIS

The most advanced integration is taking place within DG DEFIS. Ukraine is already participating in EDF-funded projects and is being incorporated into the European Defence Industry Programme and related procurement frameworks. The trajectory here is clear and should also include Ukraine's full participation in European Defence Fund consortia, integration into joint procurement mechanisms and evolution towards a 'quasi-accession' industrial model, in which Ukraine becomes an associated defence–industrial base state.

This reflects a broader shift through which Ukraine becomes an extension of the European defence–industrial ecosystem, particularly in terms of high-intensity warfare capabilities.

European Defence Agency

The European Defence Agency (EDA) remains formally restricted to EU member states, yet it already provides a tested framework for third-country participation through Administrative Arrangements. Ukraine should utilise this mechanism—already employed by Norway, Switzerland and the US—to participate in capability-development projects, research initiatives and limited coordination processes such as the Coordinated Annual Review on Defence.[72]

The most feasible trajectory is a gradual upgrade from operating under an Administrative Arrangement to acquiring 'structured associate partner' status, which would enable Ukraine's participation in selected capability steering groups. This would institutionalise Ukraine's role in areas where it already holds a comparative advantage, such as drones, electronic warfare and battlefield innovation, while preserving member states' control over decision-making.

EU Satellite Centre

The EU Satellite Centre[73] operates at the sensitive intersection of intelligence and geospatial analysis. Ukraine's current engagement remains limited but has expanded under wartime conditions. Realistic integration pathways include expanded operational cooperation agreements, the establishment of a Ukrainian liaison cell within the Satellite Centre, and gradual participation in Earth observation and space-based security programmes after the war.

---

72 EDA, 'EDA's Relations With Third Parties' (Factsheet, 2025).

73 EU Satellite Centre, 'About SatCen'.

While classification barriers will persist, selective integration is feasible and would be strategically valuable.

Military Planning and Conduct Capability

The Military Planning and Conduct Capability serves as the EU's operational headquarters for non-executive missions.[74] Ukraine's interaction currently flows through EU Military Assistance Mission structures. Future integration should focus on participation in mission planning consultations and the co-designing of post-war training and stabilisation missions.

This would position Ukraine not only as a beneficiary of EU missions, but also as a co-architect of future EU military engagements.

A European Security Council

A future European Security Council (ESC)[75] should position Ukraine as an associate permanent member, transitioning to full membership upon EU accession. This model would ensure that Ukraine's operational experience and combat-tested capabilities are embedded in European strategic decision-making from the outset.

Building on existing proposals to strengthen EU foreign, security and defence governance, an associate role for Ukraine would bridge the gap between partnership and membership. Given its unparalleled experience in defending Europe against Russian aggression, Ukraine is uniquely placed to inform the continent's deterrence posture, military planning and strategic outlook. Early inclusion would ensure that European security policy is shaped not only by institutional logic but by battlefield realities.

The ESC should be designed as a decision-making body, not a purely consultative forum. In the current threat environment, it should operationalise Article 42(7) of the Treaty on European Union by establishing clear mechanisms for identifying, attributing and responding to crises, including hybrid and sub-threshold threats. Decision-making should be based on qualified majority voting, avoiding the paralysis associated with unanimity and external interference.

---

74 EEAS, 'Military Planning and Conduct Capability (MPCC)'.

75 I. Ciolan, 'Europe Needs a Security Council of Its Own', *Wilfried Martens Centre for European Studies*, 16 February 2026.

Properly designed, an ESC would strengthen the European pillar of NATO while reinforcing commitments to increased defence spending, interoperability and joint capability development. It would also ensure accountability in resource optimisation and defence–industrial cooperation, without undermining market competitiveness.

The role of associate members would need to be clearly defined and commensurate with the capabilities they contribute. Countries such as the UK and Norway—alongside Ukraine—bring significant military, technological and strategic assets and should therefore have meaningful influence within the Council.[76] The UK, in particular, remains central to European security due to its nuclear deterrent, naval capabilities, leadership of the Joint Expeditionary Force and role in initiatives such as the Maritime Capabilities Coalition for Ukraine. Norway, meanwhile, is emerging as a key defence innovation actor, underpinned by substantial financial resources and growing industrial capacity. Iceland could also be considered as a future associate participant.

In an era of hybrid warfare, ESC partnerships should extend beyond geography to include values-based coalitions with like-minded democracies. A separate category of 'strategic partners' could include countries such as Canada, Japan and South Korea. These states bring complementary strengths—from Arctic security and Indo-Pacific engagement to defence–industrial capacity—and would enable an ESC to project influence globally through aligned regional frameworks.

Finally, an ESC could introduce theatres of responsibility to better coordinate responses to complex, cross-regional threats. These could include Europe, the Arctic, the Middle East and Africa. This would reflect the increasingly interconnected nature of security challenges, which span the military, economic and energy domains.

Ukraine's integration into Europe's security architecture will not be defined by a single institutional step, but by a phased embedding across industrial, operational and political structures. Taken together, these pathways would position Ukraine not as a future participant, but as a foundational pillar of Europe's emerging defence system.

[76] Ibid.

Policy recommendations: institutional cooperation

Institutionalise Ukraine's role in political and diplomatic structures.

Ukraine should be granted permanent observer status of the PSC and integrated into structured dialogue within the EEAS. This would ensure consistent political coordination and early input into EU decision-making.

Integrate Ukraine into military governance and planning.

Ukraine's chief of defence should be granted observer status of the EU Military Committee, alongside being included in planning processes within the Military Planning and Conduct Capability. This would formalise Ukraine's role in shaping European military readiness and operations. This could also pave the way to integrating the Ukrainian armed forces—in terms of force structures, doctrine and planning cycles—into a future European defence framework.

Deepen defence integration through DG DEFIS.

Ukraine should be embedded within DG DEFIS as a quasi-accession industrial partner, with full participation in European Defence Fund consortia and joint procurement frameworks. This would position Ukraine as a core contributor to Europe's defence–industrial base.

Advance capability integration via the EDA.

Ukraine's cooperation with the EDA should be upgraded to that of structured associate status, enabling participation in capability-development projects and selected steering groups. This would anchor Ukraine within Europe's long-term defence planning ecosystem.

Expand intelligence and space cooperation.

Cooperation with the EU Satellite Centre should be deepened through a Ukrainian liaison presence and enhanced intelligence-sharing arrangements. Over time, this should evolve into selective participation in EU space and geospatial security programmes.

Establish an ESC with Ukraine as an associate member.

An ESC should be created as a decision-making body, with Ukraine granted associate membership that transitions to full participation upon EU accession. This would ensure that Ukraine's operational experience directly informs European strategic planning and crisis response.

Expand values-based security partnerships.

The EU should deepen structured cooperation with like-minded democracies, including the UK, Norway, Canada, Japan and South Korea, to extend its strategic reach. These partnerships should focus on technology, supply chains and coordinated responses to shared security challenges.

Conclusion: from middle power to global actor — Europe's strategic opportunity

The cumulative effect of these developments—the deepening of partnerships, the creation of new functional bodies with clear mandates and decision-making authority, and their underpinning through EU financial instruments—points to the emergence of a new European security architecture, one that will increasingly supersede the constraints of the post-war order. While its foundational purpose remains unchanged—defending sovereignty, freedom and the principles of liberal democracy—the form through which these objectives are pursued must evolve to meet the demands of a far more contested and fragmented geopolitical environment.

In this transformation, Ukraine represents Europe's decisive strategic advantage. As the most battle-hardened nation on the continent, it brings not only capabilities, but hard-earned operational insight that the EU itself lacks. Integrating Ukraine is therefore not an act of solidarity alone—it is a strategic necessity that will strengthen the EU's ability to deter, defend and act.

Ukraine's contribution goes beyond battlefield resilience. It offers Europe a unique combination of combat-tested innovation, from unmanned systems and AI-enabled warfare to cyber-defence and hybrid threat response, alongside a rapidly evolving defence–industrial ecosystem and proven public–private partnerships. Its experiences of large-scale mobilisation, civil resilience and real-time adaptation to high-intensity conflict provide a blueprint for modern defence that Europe can neither replicate quickly nor ignore. Integrating these capabilities into European structures would not only enhance operational effectiveness but could fundamentally reshape Europe's approach to security in the twenty-first century.

The disruption of the global security environment, coupled with accelerating geopolitical fragmentation, creates a rare window for Europe to move beyond the limitations that have long defined it. Too often described as a 'middle power', in reality the EU possesses the scale, resources and political weight of a global actor—and yet lacks the institutional coherence and strategic ambition to fully realise this role.

Remodelling—and where necessary rebuilding—its security and defence architecture, embedding Ukraine within it and redefining partnerships with like-minded states will set the EU on a credible path towards global strategic relevance. This is not merely institutional reform—it is the redefinition of Europe's role in the international system.

At a time when authoritarian powers are expanding their capabilities and leveraging emerging technologies to shift the balance of power, the EU must develop the agency and strength required to defend its values. As a union of states committed to freedom, sovereignty and human rights, it cannot afford strategic passivity. A new international order is already taking shape. The question is not whether Europe will be affected by it but whether it will help to shape it.

Bibliography

Ae.metu.edu, 'Information About Ukrainian Space Industry. Composition of the Ukrainian Space Industry', accessed at https://www.ae.metu.edu.tr/news/ukrainecoop/ukranianspace.pdf on 9 April 2026.

Axon, L. et al., 'Private Initiatives for Public Cybersecurity in Ukraine', *Journal of Cyber Policy* (2025), 1–24, accessed at https://gcscc.ox.ac.uk/private-initiatives-public-cybersecurity-ukraine on 9 April 2026.

Bailey, C., 'Are We at War With Russia? How Warden's Rings Map Russia's Hybrid Strategy', *RUSI*, 4 December 2025, accessed at https://www.rusi.org/explore-our-research/publications/commentary/are-we-war-russia-how-wardens-rings-map-russias-hybrid-strategy on 8 April 2026.

Basset, L., 'Silicon Shadow: The Influence of Big Tech in Russo-Ukrainian Cyber Warfare', *Cambridge Journal of Political Affairs* 5/1 (2024), 70–116.

Berezutsky, S., 'Why Ukraine Is a Space Nation', *Ukraine World*, 14 June 2022, accessed at https://ukraineworld.org/en/articles/russian-aggression/why-ukraine-space-nation on 9 April 2026.

Bergmann, M., Svendsen, O. and Burchell, J., 'Europe Needs an ASAP Program for Air Defence', *CSIS*, 23 March 2026, accessed https://www.csis.org/analysis/europe-needs-asap-program-air-defense on 8 April 2026.

Bienvenue, E. et al., 'Private Tech Companies, The State and the New Character of War', *Carnegie Endowment for International Peace*, 1 December 2025, accessed at https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies on 8 April 2026.

Blockmans, S., *Addressing the EU's Collective Action Problem in Defence Through Institutional Reform*, Wilfried Martens Centre for European Studies (July 2024), accessed at https://www.martenscentre.eu/wp-content/uploads/2024/09/Addressing-the-EUs-Collective-Action-Problem-in-Defence-Through-Institutional-Reform.pdf on 6 April 2026.

Bondar, K., *From Production to Procurement: How Europe and Ukraine are Transforming Defence Supply Chains*, CSIS (10 December 2025), accessed at https://www.csis.org/analysis/production-procurement-how-europe-and-ukraine-are-transforming-defense-supply-chains on 8 April 2026.

Bondar, K., *Ukraine's Future Vision and Current Capabilities for Waging AI Enabled Autonomous Warfare*, CSIS (6 March 2025), accessed at https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare on 8 April 2026.

Chernoherenko, K., 'The Battlefield Video Analysis Platform Known as VEZHA Is Now Accessible Within the DELTA Combat System', Ministry of Defence of Ukraine, 14 October 2024, accessed at https://mod.gov.ua/en/news/kateryna-chernohorenko-the-battlefield-video-analysis-platform-known-as-vezha-is-now-accessible-within-the-delta-combat-system on 8 April 2026.

Chernohorenko, K., 'Why Does Ukraine Need Military Space? Answering the 5 Most Common Questions', *Militarnyi*, 9 April 2025, accessed at https://militarnyi.com/en/articles/why-does-ukraine-need-military-space-answering-the-5-most-common-questions/ on 9 April 2026.

Ciolan, I., 'Europe Needs a Security Council of Its Own', Wilfried Martens Centre for European Studies (February 2026), accessed at https://www.martenscentre.eu/wp-content/uploads/2026/02/EU-Security-Council-In-Brief.pdf on 4 April 2026.

Clapp, S. et al., *ReArm Europe Plan/Readiness 2030*, European Parliamentary Research Service, Briefing PE 769.566 (April 2025), accessed at https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf on 6 April 2026.

Cohen, J. et al., 'The Future of European Defense', *Goldman Sachs Global Institute*, June 2025, accessed at https://www.goldmansachs.com/pdfs/insights/articles/the-future-of-european-defense/article.pdf on 8 April 2026.

Council of the European Union, 'European Peace Facility', accessed at https://www.consilium.europa.eu/en/policies/european-peace-facility/#ukraine on 6 April 2026.

Dennis, H. D. and Fink, A. L. *Defense Primer: U.S. European Command (EUCOM)*, Congressional Research Service (5 February 2026), accessed at https://www.congress.gov/crs-products/product/pdf/IF/IF11130 on 3 April 2026.

Di Mizio, G. and Gjerstad, M., 'Ukraine's Ground-Based Air Defence: Evolution, Resilience and Pressure', *IISS*, 24 February 2025, accessed at https://www.iiss.org/online-analysis/military-balance/2025/02/ukraines-ground-based-air-defence-evolution-resilience-and-pressure/ on 8 April 2026.

EDA, 'EDA's Relations With Third Parties' (Factsheet, 2025), accessed at https://eda.europa.eu/who-we-are/third-parties on 19 April 2026.

EEAS, 'EU Response to Hybrid Threats' (2024), accessed at https://www.eeas.europa.eu/eeas/eu-action-countering-hybrid-threats on 3 April 2026.

EEAS, 'EU–Ukraine Relations', accessed at https://www.eeas.europa.eu/ukraine_en on 19 April 2026.

EEAS, 'Military Planning and Conduct Capability (MPCC)', accessed at https://www.eeas.europa.eu/eeas/military-planning-and-conduct-capability_en on 19 April 2026.

EU, 'Niinistö Report: Shifting From Crisis Response to Resilience' (31 October 2024), accessed at https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf on 9 April 2026.

EU Agency for the Space Programme, 'Galileo', accessed at https://www.euspa.europa.eu/eu-space-programme/galileo on 3 April 2026.

European Commission, 'Defence Industry and Space', accessed at https://commission.europa.eu/about/departments-and-executive-agencies/defence-industry-and-space_en on 3 April 2026.

European Commission, 'EDIP: Forging Europe's Defence', accessed at https://defence-industry-space.ec.europa.eu/eu-defence-industry/edip-forging-europes-defence_en on 3 April 2026.

European Commission, 'EU and Ukraine Deepen Cooperation on Cyber Security at 4th Cyber Dialogue' (18 October 2025), accessed at https://digital-strategy.ec.europa.eu/en/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue on 9 April 2026.

European Commission, 'Introducing the White Paper for European Defence and the ReArm Europe Plan – Readiness 2030' (23 December 2025), accessed at https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en on 8 April 2026

European Commission, *Joint Framework on Countering Hybrid Threats*, Joint Communication, JOIN (2016) 18 final, 6 April 2016.

European Commission, 'NIS2 Directive: Securing Network and Information Systems', accessed at https://digital-strategy.ec.europa.eu/en/policies/nis2-directive on 9 April 2026.

European Commission, 'SAFE', accessed at https://commission.europa.eu/strategy-and-policy/eu-budget/eu-borrower-investor-relations/safe_en on 8 April 2026.

European Commission, 'The 2028–2034 EU Budget for a Stronger Europe', accessed at https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/eu-budget-2028-2034_en on 6 April 2026.

European Commission, *Ukraine Report 2025*, Staff Working Document, SWD (2025), 759 final, 4 November 2025, accessed at https://enlargement.ec.europa.eu/ukraine-report-2025_en/ on 6 April 2026.

European Commission, DG DEFIS, 'IRIS² – Secure Connectivity', accessed at https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en on 3 April 2026.

European Commission, DG DEFIS, 'Security Action for Europe', accessed at https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en on 6 April 2026.

European Council, *European Council Conclusions, 23–24 June 2022, EUCO 24/22* (24 June 2022), accessed at https://www.consilium.europa.eu/media/57442/2022-06-2324-euco-conclusions-en.pdf on 6 April 2026.

European Council, 'European Union Military Committee (EUMC)', accessed at https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/european-union-military-committee/ on 19 April 2026.

European Council, 'Political and Security Committee', accessed at https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-and-security-committee/ on 19 April 2026.

European Innovation Council, 'Commission Boosts Support to Ukraine Deep Tech Innovators' (1 April 2026), accessed at https://eic.ec.europa.eu/news/commission-boosts-support-ukrainian-deep-tech-innovators-2026-04-01_en on 8 April 2026.

EU Satellite Centre, 'About SatCen', accessed at https://www.satcen.europa.eu on 19 April 2026.

Fitz-Gerald, A. M. and Padalko, H., 'The Need for a Strategic Approach to Disinformation and AI Driven Threats', *RUSI*, 25 July 2024, accessed at https://www.rusi.org/explore-our-research/publications/commentary/need-strategic-approach-disinformation-and-ai-driven-threats on 9 April 2026.

France 24, 'Ukraine Makes Fastest Battlefield Gain in 2.5 Years', 16 February 2026, accessed at https://www.france24.com/en/europe/20260216-ukraine-makes-fastest-battlefield-gain-in-2-5-years on 10 April 2026.

Gurkov, N., *Behind the Lines: How Ukraine Has Outgunned Russia in Sabotage*, ACLED, 27 November 2025, accessed at https://acleddata.com/report/behind-lines-how-ukraine-has-outgunned-russia-sabotage on 8 April 2026.

Hakmeh, J., 'What Ukraine Can Teach Europe and the World About Innovation in Modern Warfare', *Chatham House*, 5 March 2025, accessed at https://www.chathamhouse.org/2025/03/what-ukraine-can-teach-europe-and-world-about-innovation-modern-warfare on 8 April 2026.

Halstian, M., 'A First Point View: Examining Ukraine's Drone Industry', *Georgetown Security Studies Review* (2025), accessed at https://gssr.georgetown.edu/the-forum/regions/eurasia/a-first-point-view-examining-ukraines-drone-industry/ on 8 April 2026.

Healey, J., 'Joint Expeditionary Force Launches Enhanced Partnership With Ukraine as Allies Step Up Further', UK Ministry of Defence, 5 November 2025, accessed at https://www.gov.uk/government/news/joint-expeditionary-force-launches-enhanced-partnership-with-ukraine-as-allies-step-up-further on 8 April 2026.

Hlivco, A., 'Russia's Wartime Influence Inside Ukraine', in S. Šrāders and G. T. Terry (eds.), *The Paradox of Power: Ukraine's Struggle, Russia's Dilemmas, and Global Consequences. The Conference of Russia Papers 2024* (Baltic Defence College, 2024), 11–22, accessed at https://media.voog.com/0000/0051/2796/files/Rusconf_24_veeb.pdf on 8 April 2026.

Hoffman, F., 'Flight of the Flamingo Spells Trouble for Russia', *Centre for European Policy Analysis*, 8 September 2025, accessed at https://cepa.org/article/flight-of-the-flamingo-spells-trouble-for-russia/ on 9 April 2026.

Ilves, L., 'Ukraine Teaches Europe Cyber Lessons', *Centre for European Policy Analysis*, 20 March 2025, accessed at https://cepa.org/article/ukraine-teaches-europe-cyber-lessons/ on 9 April 2026.

Irish, J., 'Macron Says France Now Providing Two Thirds of Intelligence to Ukraine', *Reuters*, 15 January 2026, accessed at https://www.reuters.com/business/aerospace-defense/macron-says-france-now-providing-two-thirds-intelligence-ukraine-2026-01-15/ on 8 April 2026

Jacobs, B., 'Maximator: European Signals Intelligence Cooperation From a Dutch Perspective', *Intelligence and National Security* 35/5 (2020), 659–68, accessed at https://www.tandfonline.com/doi/epdf/10.1080/02684527.2020.1743538?needAccess=true on 8 April 2026.

Kabachynskyi, I., 'What You Need to Know About Ukraine's Own Neptune Missile', *United 24 Media*, 5 June 2024, accessed at https://united24media.com/war-in-ukraine/what-you-need-to-know-about-ukraines-own-neptune-missiles-used-to-strike-inside-russia-571 on 9 April 2026.

Kelly, T. and Shiraki, M., 'Gulf States Eye Cheap Ukrainian Interceptor Drone as Iranian Attacks Drain Missile Stocks', *Reuters*, 7 April 2026, accessed at https://www.reuters.com/world/middle-east/gulf-states-eye-cheap-ukrainian-interceptor-drone-iranian-attacks-drain-missile-2026-04-08/ on 8 April 2026.

Kendall-Taylor, A. and Fontaine, R., 'The Axis of Upheaval', *Foreign Affairs*, 23 April 2024, accessed at https://www.foreignaffairs.com/china/axis-upheaval-russia-iran-north-korea-taylor-fontaine# on 3 April 2026.

Khomenko, V., 'Ukraine and Greece to Jointly Manufacture Naval Drones', *Militarnyi.com*, 18 November 2025, accessed at https://militarnyi.com/en/news/ukraine-and-greece-to-jointly-manufacture-naval-drones/ on 8 April 2026.

Litnarovych, V., 'Denmark Makes History: First NATO State to Host Ukrainian Arms Production', *United24*, 3 December 2025, accessed at https://united-24media.com/latest-news/denmark-makes-history-first-nato-state-to-host-ukrainian-arms-production-13964 on 8 April 2026.

Merrow, W. and Bricknell, M., 'Comparing the Size and Capabilities of the Russian and Ukrainian Militaries', *Council on Foreign Relations*, 3 June 2025, accessed at https://www.cfr.org/articles/comparing-size-and-capabilities-russian-and-ukrainian-militaries on 8 April 2026.

Munich Security Conference, *Munich Security Report 2025: Multipolarisation* (2025), accessed at https://securityconference.org/en/publications/munich-security-report-2025/ on 3 April 2026.

Myronyshena, T., 'Ukraine, Portugal Sign Partnership to Produce Sea Drones', *Kyiv Independent*, 20 December 2025, accessed at https://kyivindependent.com/ukraine-portugal-sign-partnership-to-produce-sea-drones-zelensky-says/ on 8 April 2026.

National Security and Defence Council of Ukraine, 'Ukrainian Experience Is Shaping Global Cybersecurity' (26 January 2026), accessed at https://www.rnbo.gov.ua/en/Diialnist/7376.html on 9 April 2026.

Padalko, H., 'AI for Freedom: Ukraine's Digital Strategy in the Information War', *Forum for Ukrainian Studies*, 28 November 2025, accessed at https://ukrainian-studies.ca/2025/11/28/ai-for-freedom/ on 8 April 2026.

Presl, D., 'Russia Is Winning the Global Information War', *RUSI*, 7 May 2024, accessed at https://www.rusi.org/explore-our-research/publications/commentary/russia-winning-global-information-war on 8 April 2026.

Quantum Systems, 'Deliveries on Schedule: Quantum Frontline Industries Sends First Batch of Drones to Ukraine', Press Release, 1 April 2026, accessed at https://quantum-systems.com/news/qfi-first-drone-delivery-to-ukraine/ on 8 April 2026.

Reuters, 'Romania Signs Deal With Ukraine on Joint Defence Production Including Drones', 12 March 2026, accessed at https://www.reuters.com/business/aerospace-defense/romania-signs-deal-with-ukraine-joint-defence-production-including-drones-2026-03-12/ on 8 April 2026.

Romandash, A., *Hybrid Warfare: Ukraine, Russia and Western Lessons*, Centre for International Governance Innovation (29 September 2025), accessed at https://www.cigionline.org/publications/hybrid-warfare-ukraine-russia-and-western-lessons/ on 8 April 2026.

Rozouvan, T., 'UK to Provide Ukraine With Thousands of Octopus Interceptor UAV's Each Month', *Janes.com*, 13 January 2026, accessed at https://www.janes.com/osint-insights/defence-news/air/uk-to-provide-ukraine-with-thousands-of-octopus-interceptor-uavs-each-month on 8 April 2026.

Saab, 'Saab and Joint Stock Company "Ukrainian Defense Industry" Sign Memorandum of Understanding', Press Release, 13 February 2026, accessed at https://www.saab.com/newsroom/press-releases/2026/saab-and-joint-stock-company-ukrainian-defense-industry-sign-memorandum-of-understanding on 8 April 2026.

Shumlianskyi, D., 'Germany's Auterion and Ukraine's Airlogix to Jointly Produce Autonomous Strike Drones', *Militarnyi.com*, 13 February 2026, accessed at https://militarnyi.com/en/news/auterion-airlogix-autonomous-strike-drones/ on 9 April 2026.

Slusher, M., 'Lessons From the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information and Resilience', *CSIS*, 2 May 2025, accessed at

https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience on 8 April 2026.

Smith, B., 'Digital Technology and the War in Ukraine', *Microsoft*, 28 February 2022, accessed at https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/ on 10 April 2026.

Swedish Civil Contingencies Agency, *Building Resilience for the Future: Lessons From Ukraine* (September 2023), accessed at https://www.mcf.se/siteassets/dokument/publikationer/english-publications/building-resilience-for-the-future---lessons-from-ukraine.pdf on 9 April 2026.

Tokariuk, O., 'Ukraine's Secret Weapon: Artificial Intelligence', *Centre for European Policy Analysis*, 20 November 2023, accessed at https://cepa.org/article/ukraines-secret-weapon-artificial-intelligence/ on 9 April 2026.

Toporkova, V., 'Ukraine, the Overlooked Powerhouse of Missile Production', *United 24 Media*, 27 August 2024, accessed at https://united24media.com/war-in-ukraine/ukraine-the-overlooked-powerhouse-of-missile-production-1960 on 9 April 2026.

Treyger, E., Cheravitch, J. and Cohen, R. S., *Russian Disinformation Efforts on Social Media*, RAND (7 June 2022), accessed at https://www.rand.org/pubs/research_reports/RR4373z2.html on 9 April 2026.

UK Foreign, Commonwealth and Development Office, *Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy* (19 September 2025), accessed at https://committees.parliament.uk/writtenevidence/138112/pdf/ on 8 April 2026.

UK Government, 'Hundreds of Missiles Delivered to Ukraine Months Ahead of Schedule as UK Leads Kyiv Trade Delegation', Press Release, 10 October 2025, accessed at https://www.gov.uk/government/news/hundreds-of-missiles-delivered-to-ukraine-months-ahead-of-schedule-as-uk-leads-kyiv-trade-delegation on 8 April 2026.

UK Government, 'Octo-Puss: Ukrainian Battlefield Equipment Set to Go on Display in Downing Street' (20 November 2025), accessed at https://www.gov.uk/government/news/octo-puss-ukrainian-battlefield-equipment-set-to-go-on-display-in-downing-street on 8 April 2026.

Ukraine, Ministry of Defence, 'EU Launches €1.5 Billion Programme for the Development of the Defence Industries, Including Funding for Ukrainian Drones, Ammunition, and Innovation' (2 April 2026), accessed at https://mod.gov.ua/en/

news/eu-launches-1-5-billion-programme-for-the-development-of-the-defence-industries-including-funding-for-ukrainian-drones-ammunition-and-innovation on 8 April 2026.

Ukraine, Ministry of Defence, 'Order on Implementing DELTA Provides Defence Forces With Legal Framework for the System's Wide-Scale Use: Denys Shmyhal' (8 October 2025), accessed at https://www.kmu.gov.ua/en/news/nakaz-pro-vprovadzhennia-delta-dav-sylam-oborony-iurydychne-pidgruntia-dlia-ii-shyrokoho-zastosuvannia-denys-shmyhal on 10 April 2026.

Van Leeuwen, R., 'What We Can Learn From Ukraine About Countering Disinformation', *Westminster Foundation for Democracy*, 24 July 2023, accessed at https://www.wfd.org/commentary/what-we-can-learn-ukraine-about-countering-disinformation on 8 April 2026.

Welle, K., *The Defence Pyramid: Ten Building Blocks for a Viable European Defence Union*, Wilfried Martens Centre for European Studies (July 2024), accessed at https://www.martenscentre.eu/wp-content/uploads/2024/09/The-Defence-Pyramid-Ten-Building-Blocks-for-a-Viable-European-Defence-Union.pdf on 4 April 2026.

Williams, L., Rajic, T. and Badgi, K., 'Unpacking Ukraine's Future Cyber and Space Forces', *CSIS*, 20 October 2025, accessed at https://www.csis.org/analysis/unpacking-ukraines-future-cyber-and-space-forces on 9 April 2026.

About the author

Aliona Hlivco *is the Founder and CEO at the St. James's Foreign Policy Group, a Visiting Lecturer at the Department of War Studies at King's College London, and a member of the Academic Council at the Wilfried Martens Centre for European Studies. A former member of Ukraine's regional parliament, her expertise spans international security and defence, contemporary warfare, strategic communications, and geopolitical risk. She regularly contributes to public and policy discussions on Euro-Atlantic security, Russia's war against Ukraine, and the future of European defence, and has lectured at institutions across the UK and the US.*

Credits

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE 1000

For more information, please visit www.martenscentre.eu.

External editing: Pole Star Editing CommV
Typesetting: Victoria Agency
Printed in Belgium by ABIJ

This publication receives funding from the European Parliament.