REPORT

The Transformation of Central and Eastern Europe's Security Architecture and the Dual-Use Technology Market

English edition of the report
originally published in Japanese in August 2026

PUBLISHED

2026.11

PUBLISHED BY

ff Red&White

ff VENTURE CAPITAL

VOL. 01
ENGLISH / FULL TEXT EDITION

Authors' note

Message from the Authors

This is an English translation of the report originally published in Japanese in August 2026. Data and descriptions reflect information available at the time of the original publication.

ff Red & White is a venture capital fund established in Warsaw in 2023 by JBIC IG Partners, a joint venture between the Japan Bank for International Cooperation (JBIC) and IGPI Group, and ff Venture Capital. We primarily invest in early-stage start-ups across Central and Eastern Europe (CEE) and the DACH region (Germany, Austria and Switzerland).

Russia's invasion of Ukraine in February 2022 marked a historic turning point in Europe's security architecture. In CEE, particularly in Poland and other countries close to Ukraine, defence-tech and dual-use technologies have rapidly gained importance. Alongside defence technologies proven in combat, numerous start-ups are emerging in fields that support national and regional resilience. Recognising the growth opportunities in advanced technology fields arising from these geopolitical shifts, we have leveraged our presence in Warsaw to build close networks with start-up ecosystems and policy communities across the CEE and DACH regions.

This report provides an overview of the structural changes in European security, the rebuilding of the defence industry and ammunition production capacity, the transformation of the battlefield driven by drones and hybrid warfare, and dual-use technology fields including space, cyber, critical infrastructure protection and supply-chain resilience. In particular, it focuses on the complementarity between CEE, located on NATO's Eastern Flank; the DACH region, with a strong industrial base and strengths in R&D and capital markets; and Ukraine, which is building the institutional foundations of a defence-oriented state under wartime conditions.

While the defence-tech and dual-use markets in the CEE and DACH regions continue to expand rapidly, information available in Japanese remains limited. Drawing on our on-the-ground presence and our day-to-day work connecting Japanese companies and investors with the CEE and DACH regions, this report presents our perspective on market developments and strategic business opportunities across the region. We hope that this report will help deepen your understanding of defence-tech and dual-use fields, particularly in the region, and serve as a useful reference as you consider future business development and investment strategies.

The Authors

TEAM



Maciej Skarul
Partner, ff Red & White



Masayuki Ohta
Partner, ff Red & White



Mariusz Adamski
Partner, ff Red & White



Taro Hizume
Partner, ff Red & White

Message from the Authors 02

Introduction

Central and Eastern Europe (CEE) and the DACH Region

I The CEE Region 05
II The DACH Region 06
III NATO’s Eastern Flank 08

Part I

A Paradigm Shift in European Security

10
I The Return of Deterrence: The End of the ‘Peace Dividend’ 11
II Germany’s Zeitenwende (Turning Point) 13
III Geopolitical Realignment: NATO Enlargement – Sweden and Finland as New Members 15

Part II

Transition to a War Economy and the Reconstruction of the Defence Industry

17
I Ammunition and Production Capacity: Rebuilding the ‘Arsenal of Democracy’ 18
II Dynamics of Key Players 19
III Capital Allocation: Increased Defence Spending in NATO Countries 21
IV Supply Chain Risks 24

Part III

Transformation of the Battlefield and Hybrid Warfare

26
I The Drone Revolution 27
II A Region in the Crosshairs: Hybrid Warfare and Sabotage 29
III Technological Barriers: Physical and Digital Border Defence – ‘Eastern Shield’ and ‘Baltic Drone Wall’ 31

Part IV

The Next-Generation Defence Ecosystem

33

I The Critical Nature of Dual-Use Technology: Definition 34

II The Critical Nature of Dual-Use Technology: Impact on National Resilience 35

III Germany: Dual-Use Revolution 37

IV Poland: A Hub for Defence Innovation 39

V The Baltic States and the V4: Complementary Ecosystems 41

VI Ukraine and CEE: A Combat-Tested Ecosystem 42

VII Case Studies: Start-ups from the CEE and DACH Regions 43

Part V

Implications for Japan – Changes in the Security Environment and Strategic Opportunities for Japanese Companies

45

I Structural Changes in Japan’s Security Environment 46

II Japan’s Security Policy Shift – From ‘Restraint’ to ‘Readiness’ 46

III The Importance of Dual-Use Technologies – Why Japan’s Private-Sector Engagement Is Essential 47

IV Strategic Complementarity between Japan and the CEE and DACH Regions 48

Notes and References

50

Disclaimer

53

Introduction

Central and Eastern Europe (CEE) and the DACH Region

An analysis of Europe's development dynamics requires a precise definition and understanding of the interconnections between two key economic blocs: Central and Eastern Europe (CEE) and the DACH region (Germany, Austria and Switzerland). Although these two areas differ in terms of market maturity and historical institutional legacies, they currently form an integrated economic area in which capital and innovation from the West combine with the East's growth momentum and strategic determination, creating a distinctive dynamic.

I The CEE Region



MAP 01

Geographical Distribution of the 12 CEE Countries

Standard CEE region based on the OECD definition

CEE is a geopolitical and economic concept whose scope has evolved since the fall of the Iron Curtain. In the broadest sense, it encompasses the former Eastern Bloc countries that transitioned from socialist systems to market economies. According to the official definition of the Organisation for Economic Co-operation and Development (OECD), the term 'Central and Eastern European Countries' (CEECs) refers to a group of twelve states: Albania, Bulgaria, Croatia, the Czech Republic, Hungary, Poland, Romania, Slovakia, Slovenia and the three Baltic states – Estonia, Latvia and Lithuania. The foundation binding this region together is the shared aspiration for full integration into Euro-Atlantic structures, as evidenced by membership of NATO and the European Union, although the pace of this integration varies by country.

1

Key Economic Data for CEE Countries

The CEE region is diverse in terms of the size of individual markets, but as a whole it constitutes a powerful bloc with a combined GDP exceeding $2.7 trillion.

Table 1: Key Economic Data for CEE Countries (2025) *1

Country	Nominal GDP (USD billion)	Population (thousand)	GDP per capita (USD)	GDP growth
Poland	1,035.59	36,497	28,374	3.6%
Romania	427.94	18,832	22,725	0.7%
Czech Republic	389.02	10,904	35,678	2.5%
Hungary	246.89	9,560	25,826	0.4%
Slovakia	154.44	5,419	28,498	0.8%
Bulgaria	131.02	6,263	20,921	3.1%
Croatia	106.06	3,874	27,376	3.2%
Lithuania	94.93	2,891	32,839	2.9%
Slovenia	79.60	2,131	37,357	1.1%
Latvia	48.59	1,861	26,116	2.1%
Estonia	47.00	1,369	34,325	0.6%
Albania	30.28	2,695	11,235	3.7%
Total CEE	~2,791	~102,296	~27,287 (average)	–

II The DACH Region



MAP 02

DACH (Germany, Austria, Switzerland)

Combined population of around 100 million; combined GDP of around $6.7 trillion.

The region known as DACH is one of the world's most important economic hubs. The acronym derives from the international abbreviations of the three German-speaking countries: D – Deutschland (Germany), A – Austria and CH – Confoederatio Helvetica (Switzerland). In business and financial literature, this term is widely used due to the strong cultural, linguistic and economic ties linking these countries, allowing companies to apply uniform marketing and operational strategies across an area inhabited by around 100 million people.

1

The Economic Potential of the DACH Region

The DACH region forms the economic backbone of Europe, with a combined nominal GDP of approximately $6.7 trillion in 2025[*1]. Its strength is based on advanced industry, technological innovation and stable financial systems. The countries of the DACH region are characterised by a very high level of prosperity, as measured by GDP per capita, with Switzerland ranking among the top in the world in this respect.

Table 2: Key Economic Data for DACH Countries (2025) [*1]

Country	Nominal GDP (USD billion)	Population (thousand)	GDP per capita (USD)	GDP growth
Germany	5,048.06	83,524	60,439	0.2%
Switzerland	1,043.54	9,026	115,620	1.3%
Austria	579.93	9,182	63,161	0.6%
Total DACH	~6,672	~101,732	~65,579 (average)	–

Germany remains the world's third-largest economy, despite GDP growth of just 0.2% in 2025. The country is undergoing a process of profound structural transformation, moving away from a model based on cheap energy from Russia and channelling vast resources into modernising its armed forces and decarbonising its industry. Switzerland, despite its smaller scale, exerts a disproportionately large influence on the global economy thanks to its dominance in the innovation sector (15 consecutive years at the top of the Global Innovation Index[*2]) and financial services. Austria, with its highly developed services and tourism sectors, maintains a stable position, although its economy is closely linked to the state of German industry.

The DACH region is Europe's second-largest technology investment market after the UK. In 2021, it generated a GDP of €5.3 trillion, and the number of start-ups in the region (over 70,000) is seven times higher than in France[*3]. Investments in climate-tech and defence-tech are becoming new drivers of growth, as evidenced by funding rounds for companies such as Enpal and Quantum Systems. The private equity market has also seen rapid growth – assets under management by funds from the DACH region have risen by over 140% since 2018, reaching €238 billion in 2023[*4].

DACH start-ups (7× France)

70,000+

PE AUM growth (2018 → 2023)

+140 %

DACH PE fund AUM (2023)

€238 bn

III NATO’s Eastern Flank



MAP 03

NATO’s Eastern Flank (B9 + Finland)

Bucharest Nine members and Finland

NATO’s Eastern Flank is a term referring to the North Atlantic Alliance’s front line in Europe, constituting a direct protective barrier against potential aggression from the Russian Federation and its allies. The geopolitical significance of this region has undergone a fundamental shift – from a peripheral area, it has become the focal point of NATO’s deterrence strategy.

1

Composition and Origins of the Eastern Flank

The key political framework representing the states of this zone is the Bucharest Nine (B9), established on 4 November 2015 in Bucharest on the initiative of Romanian President Klaus Iohannis and Polish President Andrzej Duda. The states comprising the Eastern Flank are shown below.

Since 2022, Finland has effectively joined the group of states forming the Eastern Flank; in 2023, it became NATO’s 31st member, significantly extending the Alliance’s land border with Russia by over 1,300 kilometres. Although Finland is not a formal member of the B9 group, its role in defending the northern section of the flank is crucial.

B9 countries forming the Eastern Flank

01 **The region’s central logistics hub and the country with the greatest military potential**

- Poland

02 **Countries crucial to the security of the Black Sea region**

- Romania
- Bulgaria

03 **The Baltic states: the most limited strategic depth and the greatest exposure to threat**

- Estonia
- Latvia
- Lithuania

04 **Central European countries constituting the flank’s logistical and industrial hinterland**

- Czech Republic
- Slovakia
- Hungary

2

Defence Spending and Military Capabilities of the Eastern Flank

The countries of NATO's Eastern Flank have become global leaders in terms of the rate of growth in defence spending. In 2025, European allies and Canada invested a total of $574 billion in defence, representing a 20% increase in real terms compared to the previous year[*5].

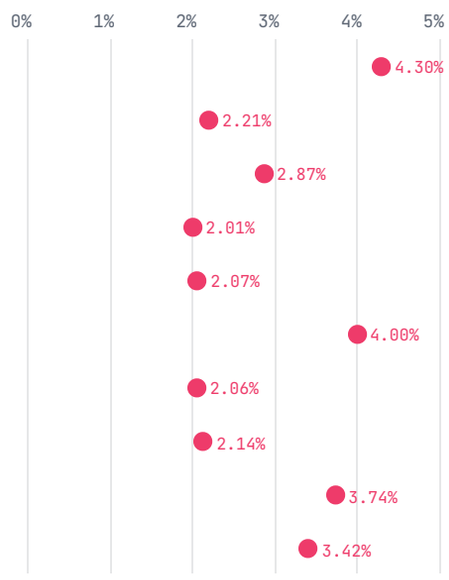
A key NATO objective is to spend at least 2% of GDP on defence. In 2025, all Alliance members met this target[*6]. Furthermore, at the 2025 Hague Summit, NATO members committed to a target of 5% of GDP by 2035.

Table 3: Comparison of NATO Average and Polish Defence Expenditure [*5]

Defence expenditure as % of GDP	2020	2021	2025 est.
NATO average (Europe and Canada)	1.69%	1.62%	2.33%
Poland's expenditure	2.21%	2.19%	4.30%

Table 4: NATO Member Defence Expenditure and GDP Ratios (2025 Estimate) [*5]

Country	Defence expenditure (USD billion, nominal, 2025 estimate)	% of GDP (2025 estimate, 2021 prices)
Poland	44.4	4.30%
Romania	9.3	2.21%
Finland	9.1	2.87%
Czech Republic	7.8	2.01%
Hungary	5.1	2.07%
Lithuania	3.8	4.00%
Slovakia	3.1	2.06%
Bulgaria	2.8	2.14%
Latvia	1.8	3.74%
Estonia	1.6	3.42%



With defence spending of $44.4 billion, Poland has become the 14th largest defence spender in the world, surpassing the United States in terms of its share of GDP. These investments include the purchase of Abrams and K2 tanks, HIMARS and K239 Chunmoo multiple launch rocket systems, and F-35 fighter jets, building an unparalleled conventional capability on the continent.

Meanwhile, Lithuania, under constant pressure from the Kaliningrad Oblast and Belarus, was among the first allies to raise its defence spending to nearly 4% of GDP, becoming a model of determination for the rest of the allies.

End of Introduction

I

PART I — CONTEXT & STRATEGY

A Paradigm Shift in European Security

Russia’s full-scale invasion of Ukraine on 24 February 2022 definitively ended the era symbolised by the fall of the Berlin Wall in 1989. Under the ‘peace dividend’ paradigm that prevailed for 30 years, Europe reduced defence spending and deepened economic interdependence, which in turn weakened its defence-industrial base and increased its external dependence. This part traces three structural changes: a shift in security perceptions, the rebuilding of defence capabilities, and the search for strategic autonomy.

CHAPTERS IN THIS PART

01 The Return of Deterrence: The End of the ‘Peace Dividend’

02 Germany’s Zeitenwende (Turning Point)

03 Geopolitical Realignment: NATO Enlargement

PART I Context and Strategy

A Paradigm Shift in European Security

24 February 2022, the day the Russian Federation launched a full-scale invasion of Ukraine, marks a fundamental turning point in the history of modern Europe, definitively ending the era shaped by the symbolic fall of the Berlin Wall in 1989. For three decades, European governments, protected by the American security umbrella, operated within the ‘peace dividend’ paradigm, reducing defence spending, abandoning conscription and promoting a foreign policy based on market expansion rather than the collective protection of citizens. This protracted process has led to the atrophy of Europe’s industrial and technological base in the defence sector, while increasing dependence on Russian raw materials and Asian supply chains.

For Japanese investors seeking stable markets with high innovation potential, Europe’s current transformation presents an unprecedented opportunity. The continent is not only returning to Cold War-era spending levels, but above all is redefining the concept of security by integrating civilian and military technologies within the framework of a rapidly expanding dual-use market. On NATO’s Eastern Flank, particularly in Poland, a new hub for land forces and technological innovation is emerging while the accession of Finland and Sweden has transformed the Baltic Sea into a maritime region of strategic importance for the entire Alliance.

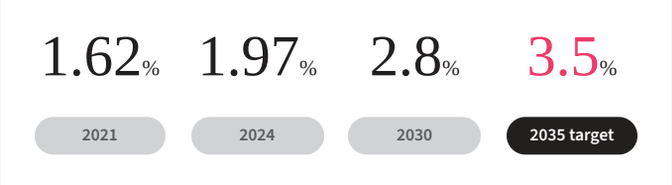
This inevitable and epoch-making change means that Europe must rebuild its technological sovereignty. This process requires massive investment in research and development (R&D), where the role of start-ups and Japanese companies, possessing unique know-how in precision manufacturing and automation, is becoming crucial. Investments in the CEE and DACH regions are no longer merely a business choice, but a strategic positioning within the new security architecture of the Free World.

I The Return of Deterrence: The End of the ‘Peace Dividend’

The collapse of the Soviet Union in the early 1990s was thought to promise global prosperity and a reduction in costly military apparatus. European security elites, ignoring warnings from the former Eastern Bloc states, prioritised trade with Russia over building deterrence capabilities. Enthusiasm for the Russian consumer and raw materials markets influenced decisions in Paris and Berlin, leading to structural underinvestment in the Bundeswehr and other Western armies.

Now, the ‘peace dividend’ has been exhausted. In 2021, prior to the invasion, the average defence spending of European NATO allies stood at a mere 1.62% of GDP. According to estimates for 2024, this figure has risen to 1.97% of GDP, which in nominal terms represents an increase from $358.7 billion to $515.3 billion annually. Poland, spending around 4% of GDP on defence in 2024, has become the undisputed leader of these changes, maintaining policy continuity regardless of the government’s composition.

Defence spending of European NATO allies (% of GDP; 2035 target refers to core defence spending)



The NATO summit held in The Hague in 2025 demonstrated the extent to which this trend had become irreversible. Russia's full-scale invasion of Ukraine and uncertainty regarding Trump's commitment to NATO mean that European governments have no choice but to invest more in collective defence. European NATO members agreed to increase spending on core defence, such as tanks and military salaries, from 2% to 3.5% of GDP by 2035 while adding a further 1.5% of GDP in security-related spending, including cyber defence and critical infrastructure protection, for a combined target of 5% of GDP. Key issues include, on the one hand, the sources of funding for increased military spending, and on the other, a race against time to rebuild not only the capabilities of the armed forces but, above all, the European industrial base.

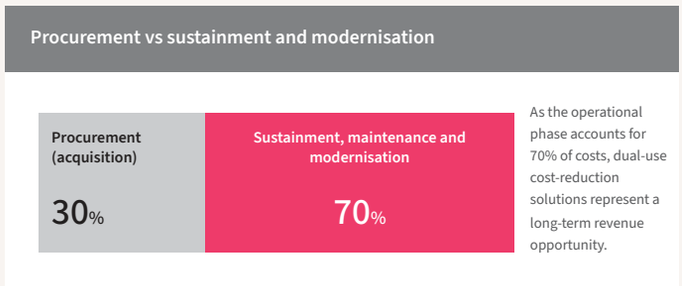
1

Modernisation Challenges

The modernisation of the armed forces is a process that goes beyond the mere purchase of equipment. It involves the development of physical infrastructure, the training of soldiers and the implementation of new tactical procedures, a process that takes anywhere from several years to a decade. Investors should note that the purchase of equipment itself accounts for only 30% of the total life-cycle costs (LCC), while 70% is spent on maintenance, servicing and modernisation. This creates enormous scope for companies offering dual-use solutions, which can reduce operating costs through civilian innovations.

Turkey and South Korea are examples of successful defence market development through R&D. Poland and other CEE and DACH countries are currently seeking to replicate this model, seeing start-ups and dual-use technologies as the driving force behind economic innovation. For Japanese companies, traditionally strong in precision engineering and AI, this is an ideal time to build partnerships.

Equipment life-cycle cost structure



> Compared to other NATO countries, we have become the absolute leader in defence spending, even overtaking the US, which allocates around 3.4% of GDP annually to this area. The minimum threshold adopted by NATO is 2%, but it is now widely recognised that this level of defence funding is far from sufficient, and there are calls for it to be raised to 3%, which is similar to our level under the Homeland Defence Act.
>
> — **Brigadier General (Ret.) Dr Adam Duda**, former Head of the Armaments Inspectorate · 2025.01

II Germany's Zeitenwende (Turning Point)

Russia's full-scale aggression against Ukraine has forced Germany to fundamentally revise its geopolitical and military identity. The term Zeitenwende (turning point), first used by Chancellor Olaf Scholz in February 2022, initially served primarily as a political slogan – a diplomatic banner intended to shield Berlin from criticism over failures in its eastern policy, including its relations with Russia, and systemic underinvestment in the Bundeswehr. However, following the federal elections of February 2025 and Friedrich Merz's assumption of the chancellorship, the concept is evolving from a temporary response into a permanent state doctrine.

Chancellor Friedrich Merz (since 2025) institutionalised the concept of Kriegstüchtigkeit (war-fighting capability). For the first time since 1991, Germany has met the 2% GDP target for defence spending, and projections for 2029 anticipate an increase in expenditure to €152.8 billion (3.5% of GDP)[*7].

The realisation of Germany's strategic ambitions is based on a complex and radically expanded financial framework. An analysis of budget data from 2024–2025 and projections up to 2029 reveals a multi-layered funding strategy that goes beyond the traditional budgetary framework, involving special debt instruments and constitutional reforms.

1

Defence Spending Trends and the 3.5% of GDP Target

In the 2024 financial year, Germany met the NATO target for the first time since 1991, allocating 2% of GDP to defence. However, this was mainly possible thanks to the ad hoc use of funds from the original special fund (Sondervermögen) worth €100 billion, established in 2022. Analyses indicated, however, that this fund, if the then-current rate of spending were maintained, would be exhausted by 2027, creating a so-called 'financial gap' estimated at €30–40 billion per year, necessary to maintain the 2% ratio in subsequent years.

The new administration led by Chancellor Merz has revised these assumptions, adopting a significantly more ambitious growth trajectory. According to official budgetary projections, total defence expenditure is set to rise from around €86 billion in 2025 to over €152.8 billion in 2029. This means that Germany plans to reach a spending ratio of 3.5% of GDP by the end of the 2020s.

Table 5: Projection of German Defence Expenditure [*8]

2025	2026	2027	2029
Estimated total expenditure	Estimated total expenditure	Estimated total expenditure	Estimated total expenditure
~86 (EUR billion)	~108 (EUR billion)	~121 (EUR billion)	152.8 (EUR billion)
2.4 % GDP	>2.5 % GDP	3.0 % GDP	3.5 % GDP
• F-35A • Heavy helicopters • 212CD ships	• Digitalisation of land platforms • Puma infantry fighting vehicles	• Modernisation of the Leopard 2A8 fleet	• Full implementation of SVIK

The key manoeuvre enabling such a drastic increase in expenditure without paralysing other sectors of the state was the reform of the constitutional 'debt brake' (Schuldenbremse). In March 2025, the Bundestag adopted an amendment to the Basic Law, introducing Article 143h, which establishes the Special Fund for Infrastructure and Climate Neutrality (SVIK) with a total value of €500 billion. The €500 billion fund is allocated as follows:

Special Fund for Infrastructure and Climate Neutrality (SVIK)

Established by constitutional amendment in March 2025

TOTAL
€500bn

Federal infrastructure investment Including the modernisation of rail and road networks and measures to address military mobility requirements for the rapid deployment of troops to NATO's Eastern Flank	60%	€300bn
Climate and Transformation Fund (KTF) Aimed at achieving energy independence, a key element of national security in the context of hybrid warfare	20%	€100bn
Local critical infrastructure for federal states and municipalities	20%	€100bn

Significantly, the constitutional amendment has exempted defence expenditure exceeding 1% of GDP from the debt limits set out in the debt brake. This effectively means the federal government has an unlimited capacity to incur liabilities for purposes related to external security, cybersecurity and civil protection, marking a historic departure from austerity policy (Schwarze Null).

Column

Allocation of Funds from the Sondervermögen in 2025 *8

An analysis of the Bundeswehr's special fund economic plan for 2025 indicates a precise prioritisation of missing capabilities. From a total of €100 billion, a record €24.06 billion has been allocated for 2025 alone. The structure of this expenditure reveals the greatest capability gaps in the German armed forces:

2025 Sondervermögen spending allocation

Category	Spending (EUR billion)	Notes
Air domain	10.248	This is the largest single category of expenditure. These funds are earmarked for the procurement of Tornado successors (F-35A), heavy transport helicopters (successor to the CH-53) and airborne weaponry.
Land domain	4.412	Modernisation of the armoured fleet, including the purchase of Leopard 2A8 tanks, Puma infantry fighting vehicles and wheeled transporters, as well as the digitalisation of land platforms.
Command and control and digitalisation	4.198	Investments in digital sovereignty, jamming-resistant communications systems and the integration of combat domains.
Naval domain	2.681	Construction of new frigates, corvettes and new-generation submarines (Type 212CD vessels).

2

Industrial Strategy and Technological Modernisation

The increase in financial expenditure goes hand in hand with a transformation in the approach to the industrial base. Germany, traditionally cautious about showcasing its defence industry, has adopted a 'war economy' strategy in selected sectors, aiming to maximise production capacity and secure independent supply chains.

The war in Ukraine has exposed critical shortages of artillery ammunition across NATO countries. In response, the German defence giant Rheinmetall has embarked on an aggressive

expansion strategy, backed by government purchase guarantees. The company has opened new production lines not only in Germany (the Unterlüß plant built in a record 15 months), but also on NATO's Eastern Flank – in Romania and Lithuania*9.

Germany has also launched the European Sky Shield Initiative (ESSI), aimed at creating an integrated air and missile defence system in Europe. The system is being built around the German IRIS-T SLM alongside non-European technologies, including Israel's Arrow 3 system (for intercepting ballistic missiles in the exosphere) and the US Patriot system. Berlin's decision caused tensions with France, but confirmed Germany's prioritisation of immediate operational capabilities over industrial protectionism.

Alongside this industrial transformation, the boundary between the civilian and military sectors in German R&D is rapidly blurring. Drawing on its strong scientific base, Germany has launched a series of initiatives to harness civilian innovation for national security. These include the establishment of the Bundeswehr Cyber Innovation Hub (CIHBw), a reassessment of universities' civil clauses (Zivilklausel), and strategic investment in quantum and hydrogen technologies, all of which are discussed in detail in Part IV.

The transformation of German security policy between 2022 and 2026 is structural and enduring. This is not merely a course correction, but the construction of a new strategic identity for the state. Germany is entering the second half of the 2020s as a state conscious of its military strength, ready to assume the role of leader in Europe's conventional defence, marking a fundamental turning point in the continent's post-war history.

III Geopolitical Realignment: NATO Enlargement – Sweden and Finland as New Members



MAP 04

The Strategic Transformation of the Baltic Sea: a 'NATO Lake'

NATO's enlargement to include Finland (2023) and Sweden (2024) is a historic change that brought an end to Helsinki's post-war pragmatism and Stockholm's two-century-long policy of neutrality. This decision was a direct response to Russian aggression, which demonstrated that remaining in a 'grey zone' was no longer an option as it encouraged further aggression.

1

The Baltic Sea as a 'NATO Lake'

The accession of the Nordic states has reshaped the operational map of Northern Europe. NATO has gained the ability to completely block the Russian Baltic Fleet in the Gulf of Finland and at the Baltiysk base. The Kaliningrad Oblast, despite being heavily armed with S-400 and Iskander systems, has become a 'hostage of geography', surrounded on all sides by Alliance territory. The most important strategic benefit is the provision of strategic depth for the Baltic states. Alternative sea lines of communication (SLOCs) via Sweden and the port of Gothenburg bypass the vulnerable Suwałki Gap*a, which fundamentally alters the defence plans for the Eastern Flank.

2

Implications for the European Security System

The accession of Finland and Sweden shifts NATO's centre of gravity northwards. The Alliance no longer focuses exclusively on the Fulda Gap*b or the Suwałki Gap, but must manage a continuous front stretching from the Barents Sea to the Baltic Sea. This strengthens cooperation among the Nordic-Baltic Eight (NB8) countries within NATO, which are promoting a robust deterrence policy towards Russia and increased defence spending.

Finland and Sweden's decision to join NATO, rather than rely on the EU's mutual defence clause (Art. 42.7 TEU), is a clear signal of NATO's primacy in the realm of hard security. This shows that in the face of an existential threat, European strategic autonomy is perceived as insufficient without the American nuclear umbrella and conventional capabilities.

NATO's enlargement to include Finland and Sweden is a historic change, bringing to a close the era of 'grey zones' in Northern Europe. It transforms the Baltic Sea region into a NATO stronghold, drastically hampering Russia's ability to project power and enhancing the security of the Baltic states by providing strategic depth. However, this process generates new challenges: the need to harmonise command structures, urgent investment in logistics infrastructure, exemplified by Rail Nordica*c, and constant confrontation with Russian hybrid activities.

End of Part 01

II

PART II — INDUSTRY & CAPITAL

Transition to a War Economy and the Reconstruction of the Defence Industry

Since the 1990s, Europe has reduced its ammunition stockpiles on the assumption that future conflicts would be limited and short. Poland is a symbolic example: after the end of the Cold War, large quantities of ammunition were disposed of as obsolete tanks were retired. Yet stockpiles that exceeded 125,000 tonnes in 1989 proved, three decades later, unable to keep pace with the rate of consumption in modern warfare. This part traces the changing view of war, the impact of disarmament and the challenges of rebuilding ammunition supply.

CHAPTERS IN THIS PART

01 Ammunition and Production Capacity: Rebuilding the ‘Arsenal of Democracy’

02 Dynamics of Key Players

03 Capital Allocation: Increased Defence Spending in NATO Countries

04 Supply Chain Risks

PART II Industry and Capital

I Ammunition and Production Capacity: Rebuilding the ‘Arsenal of Democracy’

Since the 1990s, ammunition stocks in Europe have been steadily dwindling, a result of misguided forecasts regarding the nature of future conflicts. The example of Poland, which disposed of hundreds of thousands of tonnes of ammunition following the withdrawal of T-54/T-55 tanks, illustrates the scale of the continent’s demilitarisation. In 1989, the Polish Army stored over 125,000 tonnes of ammunition in its depots alone*[10]; three decades later, these stocks proved inadequate for the needs of the modern battlefield.

1

From the ‘Peace Dividend’ to the ‘War Economy’

Prior to February 2022, the Western munitions industry was geared towards conflicts with terrorist organisations and armed groups (so-called asymmetric conflicts), focusing on the production of small quantities of sophisticated precision-guided munitions. Large-scale interstate wars of attrition involving the consumption of vast quantities of artillery shells, such as the war in Ukraine, were not anticipated, and mass-production capacity for conventional shells was not maintained. Production of 155 mm shells in the US stood at a mere 14,000 rounds per month, relying on infrastructure dating from the 1950s (e.g. the Scranton plant operating on a 1-8-5 single-shift schedule)*[11]. In Europe, the fragmentation of capabilities and lack of standardisation across various Joint Ballistics Memorandum of Understanding (JBMoU) standards meant that total continental production did not exceed 20,000 rounds per month.

The war in Ukraine has turned into a classic artillery war of attrition, with shell consumption reaching 4,000–7,000 rounds per day on the Ukrainian side and many times more on the Russian side*[12]. This forced a shift from stock management to flow management, the foundation of a wartime economy, where the key indicator is the current output of production lines rather than stock levels.

This immediate and massive demand led to the rapid depletion of Western strategic stocks. Analytical reports, such as ‘Empty Bins’ published by the Center for Strategic and International Studies (CSIS), one of the leading think tanks in the United States, highlighted critical shortages in US and allied stockpiles, which, at pre-war production rates, would have taken decades to replenish.

2

The United States: Rebuilding the ‘Arsenal of Democracy’

The Pentagon has implemented an ambitious modernisation plan, aiming to produce 100,000 rounds of 155 mm ammunition per month*[13]. Around $18 billion in investment over 15 years is expected to support the full automation and robotisation of production lines. Importantly for investors from the CEE region, the United States has granted European entities access to critical infrastructure. For example, MSM North America, a subsidiary of the Czech-based CSG Group, is building the $632.5 million Future Artillery Complex in Iowa*[14].

3

The European Union: The Challenges of Dispersed Production

The EU has responded with the Act in Support of Ammunition Production (ASAP; €500 million) and the European Defence Industry Reinforcement through common Procurement Act (EDIRPA; €310 million), which aim to remove bottlenecks in the production of gunpowder and explosives. An analysis of ASAP funding allocation shows that Europe suffers primarily from a lack of raw materials: €248 million was allocated to gunpowder production, while only €90 million went to projectile bodies. The EU had set a target of producing 2 million rounds per year by the end of 2025, although actual output remains constrained by shortages of nitrocellulose.

> Until recently, Russia produced more ammunition than all NATO members combined. But that is now a thing of the past. Across the Alliance, we are currently opening dozens of new production lines and expanding existing ones. We are producing more than at any time in the last few decades. We must capitalise on this progress in other areas, from advanced air defence systems to low-cost interceptor drones.
>
> — **Mark Rutte**, NATO Secretary General · 2025.11

II Dynamics of Key Players

1

Rheinmetall: The European Leader

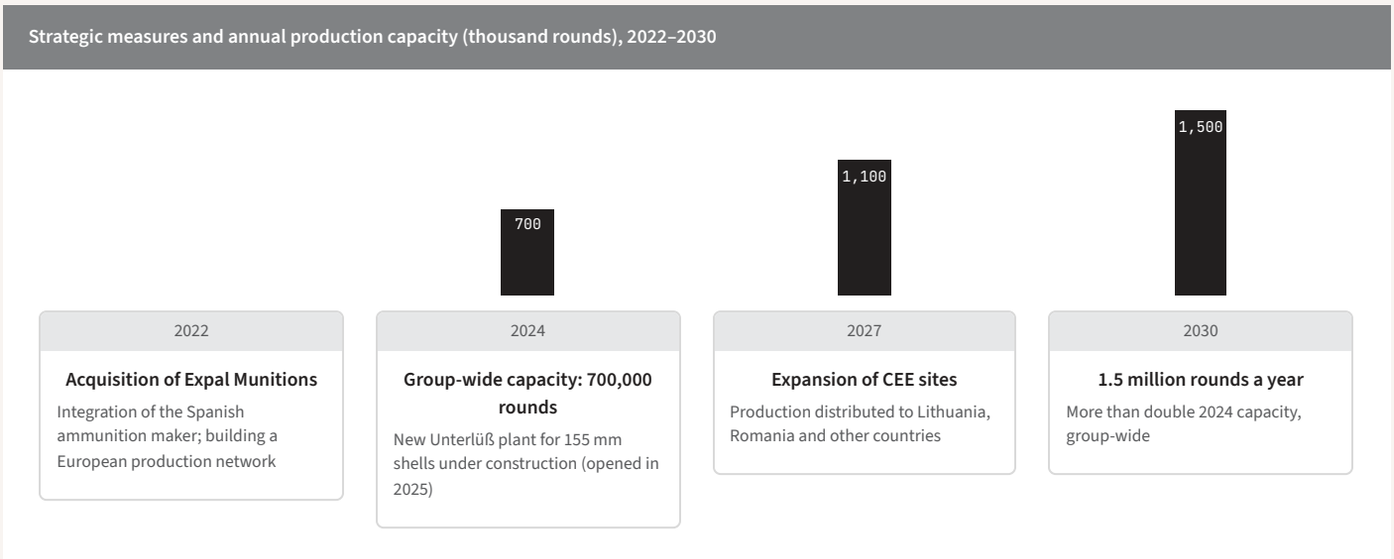
Rheinmetall has become a symbol of Europe's defence reindustrialisation. One of Germany's largest defence companies, it operates across a wide range of areas, including vehicles, artillery, ammunition, air defence and electronics, and has played a central role in addressing the shortages of ammunition, air defence systems and armoured vehicles faced by European countries since Russia's invasion of Ukraine.

Rheinmetall has been able to accelerate the expansion of its production capacity thanks to its solid financial base and the capital strength to undertake major investments and acquisitions. As European demand for ammunition surged after 2022, Rheinmetall acquired Spain's Expal Munitions, significantly strengthening its ammunition production capacity*15. The acquisition is an example of how the company has accelerated its long-standing strategy of expanding capacity through acquisitions in response to the post-invasion demand environment.

In Germany, Rheinmetall is also expanding production of large-calibre ammunition, particularly 155 mm shells, through its new plant in Unterlüß. The plant was opened within a short period and began with limited deliveries, with capacity scheduled to increase in stages. According to the group's 2024 annual report, its current group-wide large-calibre ammunition production capacity stands at 700,000 rounds per year and is planned to rise to 1.1 million rounds per year by 2027 and 1.5 million rounds per year by 2030*16.

Notably, Rheinmetall's production expansion is not confined to Germany. The company is developing ammunition, gunpowder and propellant charge production facilities in countries on NATO's Eastern Flank, including Lithuania, Latvia and Romania*9. In Lithuania, an ammunition plant is under development; in Latvia, an agreement has been signed for a new ammunition factory; and in Romania, plans are advancing for the production of gunpowder and modular propellant charges through a joint venture with the state-owned defence company Romarm. These moves indicate that Europe's defence industry is shifting from simply expanding existing production sites in Western Europe towards distributing production and supply capacity across the Eastern Flank, which is more directly exposed to the Russian threat.

Rheinmetall: large-calibre ammunition capacity roadmap



2

Central and Eastern European (CEE) Manufacturers: A New Production Hub

2.1

Poland

In Poland, modernisation is being advanced through the National Ammunition Reserve Programme and a PLN 2.4 billion (approximately €570 million*d) recapitalisation of the Polish Armaments Group (PGZ), with efforts focused on establishing three production clusters*17.

Three production clusters being built by PGZ

01	**Slovak-made shells (under licence from MSM)**	Aimed at ensuring compatibility with Krab self-propelled howitzers.
02	**British-made shells (under licence from BAE Systems)**	Aimed at diversifying technology and achieving compatibility with K9.1 self-propelled howitzers.
03	**Gunpowder production (Pionki plant)**	In partnership with Eurenco, aimed at establishing sovereign domestic production capabilities in multi-base propellants.

In Poland's private sector, the WB Group and the Niewiadów Group have demonstrated greater flexibility and have also succeeded in attracting foreign capital. For example, the Niewiadów Group received PLN 250 million (approximately €59 million) in investment from the London-based Fidera fund. The WB Group, in cooperation with South Korea's Hanwha Aerospace, is building a CGR-080 rocket production factory that is expected to secure Poland's sovereign production capability in long-range rocket artillery by 2028.

2.2

The Czech Republic and Slovakia

The Czech and Slovak industries operate in close symbiosis, often within the same corporate groups, effectively utilising the industrial heritage of Czechoslovakia.

Czechoslovak Group (CSG)

CSG is emerging as the most important player in CEE, integrating facilities in the Czech Republic, Slovakia and, more recently, Spain (Fábrica de Municiones de Granada). ZVS Holding (50% owned by CSG and 50% by the Slovak government) has launched modern production lines for cartridge-case manufacturing and loading in Snina and Dubnica nad Váhom. Investments of approximately €80–100 million are intended to increase production from around 20,000–30,000 rounds per year before the war to 360,000 rounds per year by 2026[*14]. A multi-year framework agreement worth up to €58 billion has been signed with the Slovak government, helping establish Slovakia as an ammunition export hub for the EU[*18]. CSG was also the first company to grant a Ukrainian company, Ukrainian Armor, a licence to produce 155 mm ammunition, and it also supplies components and know-how.

STV Group

STV Group, the Czech Republic's second major player, is investing CZK 5 billion (approximately €210 million[*e]) in plant modernisation and introducing projectile-body forging technology to eliminate dependence on imports. It aims to increase production of 155 mm ammunition from the current 200,000 rounds to 300,000 rounds per year by 2026.

2.3

Ukraine

Ukraine is undergoing an unprecedented transformation, shifting from post-Soviet calibres (122 mm and 152 mm) to NATO standards (105 mm and 155 mm) under wartime conditions. According to official data, in 2024 Ukraine increased its total ammunition production (mortar and artillery rounds) by 150% year on year to 2.5 million rounds[*19]. Production remains concentrated mainly in smaller calibres and drones, but the share of 155 mm ammunition is increasing.

Partnerships with foreign companies are also important means of expanding production capacity. Germany's Rheinmetall is building an ammunition plant in Ukraine as a joint venture. Although operations were initially expected to begin in 2025, security and administrative factors mean that a realistic start date is 2026–2027, with a target capacity of 100,000–300,000 rounds per year. Ukrainian Armor also planned to produce 100,000 rounds of 155 mm ammunition in 2025 using Czech technology under licence from CSG.

Table 6: Ammunition Production Capacity in Major European Countries

Company (country)	Planned 155 mm production capacity (2026–2028)	Key technology partners
Rheinmetall (Germany/CEE)	1,100,000 rounds/year[*16]	EU governments, Ukraine
CSG / ZVS (Czech Republic/Slovakia)	360,000 rounds/year[*14]	MSM Group, Ukraine
PGZ (Poland)	180,000 rounds/year[*17]	BAE Systems, Eurenco, MSM
Niewiadów PGM (Poland)	180,000 rounds/year[*20]	Northrop Grumman, ZVS

III Capital Allocation: Increased Defence Spending in NATO Countries

The year 2026 marks the implementation phase of the most ambitious financial plans since the Cold War. At the NATO Summit in The Hague in June 2025, a new target was set to allocate 5% of GDP to security by 2035: 3.5% for core defence spending and 1.5% for security-related investment, including cyber defence and critical infrastructure protection.

1

European Defence White Paper

The European Commission (EC) presented the European Defence White Paper – Readiness 2030 in March 2025. It contains measures aimed at eliminating critical capability gaps and building a strong industrial base for the defence sector. It sets out proposals for Member States on how to make major investments in defence, procure defence systems and build the long-term readiness of the European defence industry.

The ReArm Europe/Readiness 2030 plan envisages expenditure exceeding €800 billion and is structured around three pillars:

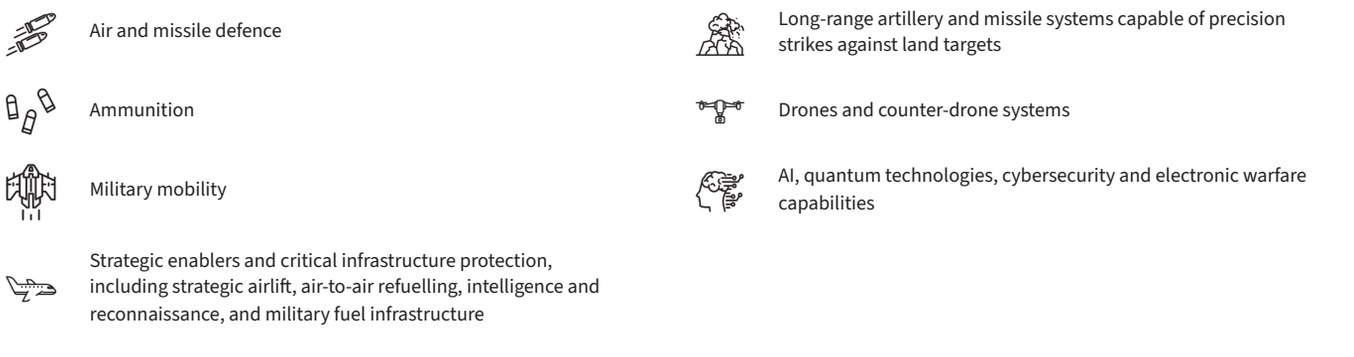
01 **Use of public funds for defence at national level**: the EC has called on EU Member States to activate the national escape clause under the Stability and Growth Pact, enabling them to increase defence spending within the EU fiscal framework.

02 **A new security financing instrument, SAFE**: the EC will raise up to €150 billion on capital markets to help Member States rapidly expand investment in defence capabilities. The funds will be made available to Member States in the form of long-term loans, and the programme will also be open to Ukraine, European Free Trade Association (EFTA) members and European Economic Area (EEA) members.

03 **Cooperation with the European Investment Bank (EIB) Group and mobilisation of private capital through the Savings and Investment Union**: the EIB Group will expand the scope of its lending to defence and security projects, while maintaining its capacity to finance other sectors.

The White Paper states that the EU should be capable of conducting military operations, including large-scale operations, but notes that Member States currently lack such capabilities. To address this gap, it identifies seven areas in which action is needed:

Seven military capabilities Europe must acquire (European Defence White Paper)



Member States have increased defence spending by nearly a third since 2021, reaching €326 billion in 2024, equivalent to 1.9% of the EU's total GDP*[21]. Nevertheless, the White Paper notes that spending remains 'significantly lower than in the US and, more worryingly, also than in Russia and China.'

The ReArm Europe/Readiness 2030 plan is intended to offset the effects of underinvestment. The EC has proposed the adoption, under the Treaty on the Functioning of the European Union, of a regulation that will enable Member States to obtain loans backed by the EU budget. This is Security Action for Europe (SAFE), worth up to €150 billion. SAFE is intended to support Europe's defence industry through joint procurement involving at least two countries, one of which must be a Member State receiving SAFE financial support. The other participating country may be another EU Member State, an EFTA country, an EEA country or Ukraine.

A further incentive is an escape clause allowing for a derogation from debt and deficit rules in respect of additional defence expenditure of up to 1.5% of GDP. According to the EC's calculations, the relaxation of fiscal rules, together with SAFE, will enable a total of €800 billion to be raised, of which the majority (over 80%) may come from Member States, with less than 20% coming from SAFE itself.

A third source of funding will consist of additional financing instruments involving investment banks and commercial financial institutions. This applies in particular to financing for companies to invest in arms production and infrastructure, and to a lesser extent, if at all, to arms purchases. The rules governing the EIB's financing of security-related activities are to be extended to cover specific defence capabilities, and not just dual-use items such as satellites. The EC will also support financing by commercial financial institutions and financial markets. In EU countries, these entities have often avoided financing defence projects (regarding them as 'dirty'), which has created difficulties in accessing finance, particularly for small and medium-sized enterprises in the sector. This is now set to change, through appropriate regulatory measures designed to ensure that, for example, investment funds in which private savings are invested can invest more widely in defence-related projects.

The White Paper emphasises that the EU should continue its mutually beneficial engagement and cooperation in security and defence not only with all European countries, but also with candidate and neighbouring countries – Albania, Iceland, Montenegro, Moldova, North Macedonia and Switzerland. It also expresses a commitment to partnership with Turkey and calls for exploring opportunities for defence-industrial cooperation with partners in the Indo-Pacific, particularly Japan and South Korea, with which security and defence partnerships were established in November 2024, as well as Australia and New Zealand.

2

The SAFE Programme (Security Action for Europe)

The SAFE programme is an EU financing instrument providing €150 billion in low-interest loans, at an interest rate of approximately 3.3% and with a repayment period of up to 45 years, to support joint arms procurement. Poland leads in allocations, having been granted €43.7 billion, representing nearly 30% of the programme's total budget.

01 A condition for financing is that components originating in the EU, EEA-EFTA countries or Ukraine account for at least 65% of the estimated cost of the components of the final product.

02 On 29 May 2026, Poland received the first disbursement of 15% of its allocation (€6.6 billion), becoming the first Member State to receive SAFE funding*22.

03 Notably, 89% of Poland's SAFE funds will go to domestic industry (PGZ and the WB Group), making this an unparalleled initiative in support of the domestic production base.

Allocation of SAFE Funds *23

Country	SAFE allocation (EUR billion) – total €150 billion	Key projects
Poland	43.7	Air defence (Narew) · Naval vessels (Miecznik) · Armoured vehicles (Borsuk) · Border defence infrastructure (East Shield)
Romania	16.7	Air defence · Ammunition · Gunpowder
France	15.1	Strategic autonomy · Air defence
Italy	14.9	Cybersecurity · Satellite systems
Finland	1.0	Border surveillance · Counter-UAS systems (C-UAS)
Other EU Member States	~58.6	

2.1

Participation of Third Countries

SAFE opens a new chapter in cooperation with third countries. Ukraine and EEA–EFTA countries will be treated on the same terms as EU Member States and may participate in joint procurement; purchases may also be made from companies operating in these countries. Acceding countries, candidate countries, potential candidate countries and countries that have concluded security and defence partnerships with the EU (such as the United Kingdom) may also participate in joint procurement. In addition, SAFE provides for the possibility of concluding additional bilateral or multilateral agreements with these third countries to broaden the eligibility criteria.

2.2

Eligible Actions

Defence-related products eligible for support under SAFE are divided into two categories based on the first list of priority areas identified by the European Council on 6 March 2025:

01 Ammunition and munitions; artillery systems, including precision deep-strike capabilities; ground combat capabilities and their support systems, including soldier equipment and infantry weapons; critical infrastructure protection; cybersecurity; and military mobility, including counter-mobility.

02 Air and missile defence systems; maritime surface and submarine capabilities; drones and counter-drone systems; force enablers, including strategic airlift, air-to-air refuelling, C4 ISTAR systems, space assets and space services; protection of space assets; AI; and electronic warfare.

Defence-related products falling within the second category will be subject to stricter eligibility conditions. In particular, contractors must have the authority to determine the specification, adaptation and development of the design of the defence-related product being procured, free from restrictions imposed by non-eligible third countries.

For both categories of products, procurement contracts will have to ensure that the cost of components originating from outside the EU, EEA-EFTA countries and Ukraine does not exceed 35% of the estimated cost of the components of the final product.

The EU is determined to further strengthen and deepen transatlantic cooperation and engagement in the field of security and defence, as well as complementarity with NATO. In this context, SAFE will seek to enhance interoperability, continue industrial cooperation and ensure mutual access – with trusted partners – to state-of-the-art technologies.

IV Supply Chain Risks

1

Vulnerabilities in Global Supply Chains

Global supply chains, whose vulnerabilities were exposed by the COVID-19 pandemic, are being subjected to even greater strain by the protracted war in Ukraine and the sharp escalation of conflict in the Middle East, accompanied by uncertainty over navigation through the Strait of Hormuz.

The semiconductor supply crisis that emerged during the pandemic made Europe and Japan acutely aware of their deep dependence on East Asia and the United States. By 2026, the competition for access to the most advanced technology hubs has become a key priority in the industrial policies of both regions. The pandemic also served as a wake-up call, exposing the fragility of the Just-in-Time model. As of 2026, the Just-in-Case model, based on diversification of supply sources and strategic stockpiling, has become the new norm.

Meanwhile, the war in Ukraine has become a testing ground for ‘material warfare’. It has demonstrated that supply chains must be capable of scaling production by thousands of per cent within a short period and that this is impossible without

domestic stockpiles of raw materials, such as TNT and nitrocellulose. The greatest strategic threat to European plans is dependence on Chinese cotton linters, a feedstock for nitrocellulose. A disruption to this supply could paralyse ammunition production across NATO. Poland's Łukasiewicz Research Network is developing technology to produce nitrocellulose from cellulose recovered from waste wood and waste cotton; such efforts are considered critical to Europe's supply-chain autonomy.

Furthermore, the latest escalation of conflict in the Middle East has created severe instability in oil transport, with energy shipments suffering the largest supply disruption on record. This is having a direct impact on Japan's energy sector and European logistics costs. Energy resources can no longer be treated as mere market commodities; they must be repositioned as strategic resources. The crisis in the Strait of Hormuz has prompted Europe and Japan to accelerate the build-up of strategic oil reserves.

2

Responses: Expanding Domestic Capabilities and International Cooperation

As demonstrated by the war in Ukraine and conflicts in the Middle East, drones have become one of the key combat systems. However, 70–80% of the components used in their manufacture – such as flight controllers, GPS modules and brushless motors – are still made in China or depend on Chinese components and rare minerals, including neodymium magnets and lithium-ion cells.

The path to reducing this dependence lies in investing in domestic capabilities, including the use of reverse engineering, and relocating production of dual-use components to countries that share the same democratic values. Nevertheless, dependence on China in areas such as lithium-ion batteries remains an 'Achilles' heel'. One potential solution is the solid-state batteries being developed in Japan, a next-generation technology that offers greater safety and efficiency than conventional batteries. This is why stronger technological cooperation between Japan and CEE countries is essential, a point also confirmed in the joint statement issued by the Prime Ministers of Japan and Poland in April 2026.

When supply chains are disrupted, attention is turning to the 3D printing of spare parts on the battlefield and the use of AI algorithms to predict supply disruptions in real time ('predictive supply chains'), particularly in the dynamic conflict environment of the Middle East.

Resilience is no longer an end in itself, but a prerequisite for maintaining national sovereignty. As CEE countries increasingly serve as Europe's physical shield, Japan can serve as a technological partner to the democratic world. The issue today is not finding the 'cheapest' suppliers, but securing the 'most reliable' suppliers, even at somewhat higher production costs. For Japanese investors with expertise in advanced chemical and materials technologies, this is an area that combines strategic importance with high profitability. In addition, Japan's experience and expertise in building resilient supply chains and automating production processes can bring significant value to European manufacturers.

End of Part 02

III

PART III — NEW DOMAINS OF OPERATION

Transformation of the Battlefield and Hybrid Warfare

The war in Ukraine has fundamentally changed the battlefield through the fusion of mass drone deployment and digital technology. Persistent surveillance and instant information-sharing are reshaping manoeuvre-centred operational concepts, while blurring the line between the military and civilian spheres and accelerating the spatial and technological expansion of war. These changes are turning not only the front line but also border zones and social infrastructure into new targets. This part traces the drone revolution, the region in the crosshairs, and the emergence of new technological barriers exemplified by the Eastern Shield and the Baltic Drone Wall.

CHAPTERS IN THIS PART

01 The Drone Revolution

02 A Region in the Crosshairs: Hybrid Warfare and Sabotage

03 Technological Barriers: Eastern Shield and Baltic Drone Wall

PART III New Domains of Operation

I The Drone Revolution

The war in Ukraine has triggered an unprecedented 'drone revolution' that has permanently altered the paradigm of conventional operations. The saturation of the front line with optical and thermal imaging sensors has created a 'transparent battlefield' (or 'radical transparency'), making it effectively impossible to concentrate forces covertly and leading to a paralysis of manoeuvre and a transition to positional warfare. Ukraine, being the materially weaker party, has managed to create an asymmetric advantage through the mass adoption of commercial off-the-shelf (COTS) technologies and the creation of a unique public-private innovation ecosystem under the auspices of the Brave1[*f] cluster.

> When full-scale war broke out in 2022, unmanned aerial vehicles were deployed on a large scale. And most of these unmanned aerial vehicles were commercial drones. They were brought into service based on the experience Ukraine had already gained from the ATO (Anti-Terrorist Operation – military operations in Donbas; ed.) since 2014. In 2022, drones were used for surveillance, for example in the defence of Kyiv. A special app was developed to report the movements of Russian Federation troops. Soldiers began to be trained to fly drones, and the training lasted just three days. The aim was to quickly provide information on the location of Russian units. Then came the Russian Federation's response, as it began doing the same. Even before the invasion, Russia had some experience, for example in using drones to direct artillery fire, but this was not on a large scale. A race began. Commercial drones were increasingly integrated; Bayraktar was enjoying its heyday, and our FlyEye drones had been in operation from the start. But it was 2023 that marked the turning point, with the Ukrainian Armed Forces' counter-offensive in Zaporizhzhia.
>
> — **Tomasz Darmoliński**, drone expert; President of the 'Żelazny' Foundation and the UAV Academy [*24]

1

The Origins and Nature of the 'Drone Revolution': The Democratisation of Precision Strikes

The evolution of FPV (First Person View) drones from hobbyist toys into the 'precision artillery of the 21st century' on the Ukrainian battlefield has created unprecedented economic asymmetry. Cheap commercial FPV drones costing $400–1,000 are capable of effectively neutralising main battle tanks (MBTs) worth millions of dollars (e.g. the T-90M 'Proryv') or air defence systems (e.g. Tor, Buk).

This phenomenon can be described as the 'democratisation of precision strikes'. Prior to 2022, the ability to direct precision fire over long distances was the preserve of aviation and advanced missile systems. Now, thanks to FPV drones, a single infantry platoon has its own tactical air force, capable of striking targets beyond visual line of sight (BVLOS) with surgical precision. This changes the command structure, flattening the hierarchy and giving lower-level commanders autonomy in deciding when to use force.

1.1

The 'Transparent Battlefield' and the Collapse of the Doctrine of Operational Surprise

In November 2023, the then Commander-in-Chief of the Ukrainian Armed Forces, General Valerii Zaluzhnyi, concluded in his landmark analysis that the war had reached a stalemate. The main cause of this state of affairs was the ubiquity of reconnaissance drones. The saturation of the airspace above the front line with optical, thermal imaging and radar sensors led to the emergence of the phenomenon of the 'transparent battlefield'.

Traditional military doctrine assumed the possibility of covertly concentrating forces for a breakthrough. In the Ukrainian context, where every square kilometre of the front line is constantly monitored by swarms of drones such as the Mavic, Autel or Leleka, any concentration of armoured vehicles is detected almost immediately. This results in an immediate response with counter-battery fire or kamikaze drone strikes, which paralyse the manoeuvre before it even begins. This has

forced both sides to disperse their logistics and switch to operations using small assault groups, which in turn contributes to the prolongation of the conflict and the ‘entrenchment’ of the front line.

2

The Brave1 Cluster and the Innovation Ecosystem

Ukraine has moved away from a slow military procurement model in favour of the Brave1 cluster, which has shortened the ‘from idea to battlefield’ cycle to a matter of weeks. By early 2026, the cluster had registered more than 3,300 projects and awarded more than 600 grants. In 2026 alone, it attracted an estimated $100 million in venture capital*[25]. Technology priorities for 2025–2026 include:

1

Swarm Tech

Algorithms coordinating swarms of drones by a single operator

2

Terminal Guidance

AI-based autonomy enabling a drone to hit its target despite electronic warfare (EW) jamming

3

Motherships

Platforms extending the range of FPV drones

It is worth highlighting the model of ‘reverse technology transfer’ that has been established, in which Ukraine has gone from being a recipient of Western solutions to becoming a provider of them. Solutions in the field of unmanned systems and missiles, proven on the Ukrainian battlefield, are in demand among manufacturers from CEE countries. Ukrainian companies are also relocating their production lines, for example to Poland and the Baltic states.

> What holds us back is the fact that we operate under peacetime bureaucracy, which means that a prototype cannot be used. We must reach level 9 (operational readiness), while the Ukrainians are already fighting with level 6 drones – in other words, drones that the Polish Army is formally not permitted to possess. When a drone reaches the front line and receives positive feedback from a Ukrainian operator, it can, within a short period, formally become level 9 and enter mass production. The process from level 6 to level 9 is quick and natural. Here, of course, there are lengthy tests and studies. These are our procedures; Ukraine had to simplify them because it is fighting a war.
>
> **Tomasz Darmoliński**, drone expert; President of the ‘Żelazny’ Foundation and the UAV Academy *[24]

3

The Ukraine–Russia Drone Production Race

Ukrainian drone production is growing exponentially. From approximately 5,000 drones in 2022, production reached around 2.2 million in 2024. The number of newly registered manufacturers each year also surged from 41 in 2022 to more than 183 in 2024*[26]. Russia has responded with scale and centralisation, using the Alabuga Special Economic Zone for the mass production of Iranian-designed Shahed (Geran-2) drones around the clock. According to the Foreign Intelligence Service of Ukraine, Russia doubled its production of long-range drones to approximately 30,000 in 2025 and also planned to produce around 2 million FPV drones in 2025*[27].

> The Russians have made up for lost ground in a big way. I’ll use the metaphor of a train: in 2014, the train set off and chugged along – sometimes faster, sometimes slower. At the time, Russia was observing what was happening in the Middle East, how the so-called Islamic State was using drones, and adapted certain things, but did not make such significant progress. By 2022–2023, it had become a high-speed train. A Ukrainian is the chief driver of this train, while a Russian stands behind him in the locomotive, occasionally taking the reins; the rest of the world travels in first or second class respectively – China, which supplies the technology, travels in first class, while Western Europe and the US travel in second or even third class.
>
> **Tomasz Darmoliński**, drone expert; President of the ‘Żelazny’ Foundation and the UAV Academy *[24]

4

Counter-UAS Systems (C-UAS) and the Role of Electronic Warfare

In the face of the drone threat, electronic warfare (EW) systems have become a key element of national defence. Russian systems such as Pole-21 and Zhitel jam GPS signals on a massive scale, and Ukraine has responded with the nationwide 'Pokrova' system, which uses advanced spoofing. Interceptor (fighter) drones, which ram enemy UAVs, and laser weapons supplied by allies are also being developed.

5

Impact on CEE

The Polish WB Group has become one of the biggest beneficiaries of Ukrainian combat experience. FlyEye reconnaissance drones and Warmate loitering munitions are recognised as world-leading thanks to their combat-proven status. The Polish Armed Forces are implementing the 'Gladius' system, which integrates reconnaissance and strike drones with an artillery fire control system. The Baltic states and Romania have also accelerated their procurement of VSHORAD (very short-range air defence) systems, allocating billions of dollars to this end.

The drone revolution in Ukraine has redefined the modern battlefield. It should be assumed that any future conventional conflict will be fought under conditions akin to a 'transparent battlefield', where concealing manoeuvres is impossible. This necessitates decentralisation, camouflage and speed of action. In the drone domain, cheap, mass-produced FPV drones often outperform expensive, limited-production systems. The industrial war for production volume is the key to victory.

In turn, the technology lifecycle at the front has been reduced to weeks. Systems that are not updated (e.g. control frequencies) become useless when faced with the enemy's adaptive EW. The success of Ukraine and the Brave1 cluster demonstrates the superiority of flexible, networked innovation structures over rigid large-scale organisations. CEE countries are no longer merely customers of Western technology, but are becoming producers and innovators (Poland, Estonia, Ukraine), creating a new dimension within NATO's security system.

II A Region in the Crosshairs: Hybrid Warfare and Sabotage

1

The Changing Nature of Hybrid Warfare

Since Russia's invasion of Ukraine, the nature of hybrid warfare in Europe has changed. Alongside traditional disinformation, cyberattacks and diplomatic pressure, physical acts of sabotage targeting logistics facilities, commercial sites, energy infrastructure, undersea cables and border control have increased since 2024.

These can be understood as 'sub-threshold' attacks designed to undermine Western support for Ukraine, social stability, supply chains and critical infrastructure while avoiding triggering NATO's Article 5. The countries particularly targeted are those on NATO's Eastern Flank, including Poland, the Baltic states and the Nordic countries. These countries are both logistics hubs for military aid to Ukraine and frontline states bordering or in close proximity to Russia, Belarus and Kaliningrad. As a result, railways, ports, warehouses, energy facilities, telecommunications cables, undersea infrastructure and border-control facilities have become critical security assets.

2

Specific Targets and Cases

2.1

Attacks on Undersea Infrastructure: Balticconnector and EstLink 2

The risk of attacks on undersea infrastructure has become increasingly apparent in the Baltic Sea. In October 2023, the Balticconnector gas pipeline and telecommunications cables linking Finland and Estonia were damaged. The investigation attributed the damage to the anchor of the Hong Kong-flagged container ship Newnew Polar Bear being dragged along the seabed.

In December 2024, the EstLink 2 power cable linking Estonia and Finland was also damaged. The incident was attributed to the tanker Eagle S, reportedly part of Russia's 'shadow fleet'. The vessel is believed to have dragged its anchor for approximately 90 kilometres, damaging EstLink 2 as well as several telecommunications cables.

The key point is that such attacks do not require sophisticated military means. A commercial vessel, an anchor and unclear navigational intent may be enough to disable infrastructure supporting energy supply, communications, financial transactions and military mobility for an extended period. Protecting undersea infrastructure in the Baltic Sea is therefore no longer solely a naval mission, but a broader resilience challenge spanning ports, telecommunications, power, insurance, satellite surveillance and maritime data analytics.

2.2

Attacks on Logistics Infrastructure: DHL / DPD Parcel Incidents

Logistics infrastructure has also become a target. In 2024, reports emerged of a plot to use logistics networks such as DHL and DPD to send parcels containing incendiary devices to logistics hubs in Europe. Parcels intended to be loaded onto air cargo bound for the United States and Canada reportedly caught fire in warehouses near Birmingham and in Leipzig.

Investigators have indicated that the operation may have been a 'dry run' to test Western air-cargo and logistics security procedures. Had the devices activated in flight, the result could have been a major incident threatening the safety of air logistics as a whole, rather than simply warehouse fires.

The incident illustrates the increasingly blurred boundary between military supply networks and civilian logistics networks. Aid for Ukraine, defence components, commercial freight and e-commerce parcels generally pass through the same warehouses, airports and delivery networks. Logistics security is therefore no longer merely a matter of operational risk management for private companies; it has become part of defence supply-chain protection.

2.3

Sabotage Against Civilian Facilities: Arson Attacks on Commercial Sites and Warehouses

Civilian facilities on land have also become targets. In May 2024, a major fire broke out at the Marywilska 44 shopping centre in Warsaw, destroying more than 1,400 retail outlets. The Polish government subsequently stated that the fire was an arson attack carried out at the direction of Russian intelligence services[*28].

Related incidents include the arson attack on an IKEA store in Vilnius, Lithuania, and an arson attack on a warehouse near Warsaw. These cases suggest that commercial and logistics facilities can be targeted to create social unrest, while also underscoring the growing importance of monitoring civilian infrastructure, anomaly detection, facility security and logistics security.

The perpetrators of such acts of sabotage are often not Russian intelligence officers, but young people recruited through the Telegram messaging app in return for payments ranging from a few hundred to several thousand euros, as well as war refugees from Ukraine or Belarus facing financial hardship. The underlying aim of using Ukrainians in particular is to undermine public trust in refugees and provoke social tensions.

3

Response to Hybrid Threats

As grey-zone incidents involving logistics, civilian facilities, undersea infrastructure and border control continue to occur, countries in CEE and the Baltic Sea region are moving to integrate critical infrastructure protection with border defence. Poland's 'Eastern Shield' and the Baltic states' 'Drone Wall' are emblematic of this approach.

These initiatives go beyond physical barriers, combining sensors, drones, counter-drone systems, AI analytics, communications and command-and-control systems into a new form of defence infrastructure. The next section examines the technological elements underpinning this physical and digital border defence.

III Technological Barriers: Physical and Digital Border Defence – 'Eastern Shield' and 'Baltic Drone Wall'

Countries in the region are implementing the 'Total Defence' doctrine. Poland's 'Eastern Shield' (Tarcza Wschód) initiative, with a budget of PLN 10 billion (approximately €2.36 billion), is a large-scale technological undertaking. It comprises:

01 **Densification of communications infrastructure**

`BTS network – dual-use`

A denser network of base transceiver stations (BTS) to provide redundant military communications (dual-use)

02 **AI analysis of border sensor data**

`Detection cables – reduced false alarms`

AI systems to analyse signals from detection cables installed along the border and reduce false alarms

03 **SAN system (integrated counter-drone)**

`Contracted January 2026 – largest in Europe`

An integrated, intelligent counter-drone system, contracted in January 2026, comprising 18 batteries and 703 vehicles and unmatched in scale in Europe

The 'Baltic Drone Wall' initiative (Poland, the Baltic states, Finland and Norway) aims to create a continuous C5ISR (command, control, communications, computers, cyber, intelligence, surveillance and reconnaissance) surveillance zone stretching from the Arctic to the Carpathians, utilising interceptor drones from Estonia's Defsecintel and Latvia's Origin Robotics.

As part of the 'Eastern Shield', permanent observation towers are also planned along the border, equipped with integrated counter-drone and EW capabilities and optoelectronic systems, creating a kind of 'anti-access bubble' across the border zone.

1

Dual-Use and Omni-Use Technologies in Building Resilience

Modern security systems must transcend the division between civilian and military technologies. The omni-use concept assumes that technologies such as 5G, AI and satellite analytics are fundamental to the functioning of the state in both peacetime and wartime.

1.1

Space and Satellite Domains

Data from space is playing an increasingly important role in the security of infrastructure, particularly maritime infrastructure.

The use of synthetic aperture radar (SAR) satellites enables the detection of ships that have switched off their AIS transponders

('dark ships') near undersea cables. Historical analyses of the routes of ships such as the Newnew Polar Bear and the Eagle S were made possible precisely thanks to the archiving of satellite data.

Starlink technology, which has become popular in Ukraine, is being adopted for civilian and government use in the Baltic states. The Latvian airline airBaltic is installing Starlink terminals on its aircraft, while border services in the US are testing these systems to ensure connectivity in border dead zones. Poland is closely monitoring these developments. The use of Starlink ensures communications independent of ground infrastructure and undersea cables, which are easy targets for sabotage.

Starlink is also being considered in Poland as part of an emergency communications system, both at the local government level and by state institutions such as the Police, the State Fire Service and even the Ministry of Foreign Affairs (to maintain communication with diplomatic missions).

1.2

AI in the Fight Against Disinformation

In response to cognitive threats such as deepfakes (e.g. the doctored video featuring President Zelensky), Poland and the Baltic states are investing in AI-driven defence tools. Research projects, such as those carried out under Horizon Europe, focus on developing algorithms to detect anomalies in audio-visual content and identify bots on social media in real time. A key challenge is protecting the AI models themselves from 'data poisoning' by adversaries, which is the subject of work under the EU's digital security strategy.

In the face of Russia's hybrid activities, including those related to disinformation, which have essentially been ongoing since 2014, building the cognitive resilience of societies and states is one of the main tasks of NATO members. Given the experience and resources of the Russian disinformation apparatus, the challenge facing CEE countries, among others, is enormous.

> Wind farms provide an excellent example of dual-use energy infrastructure, as they need not be merely a source of energy. These farms are 'living' signal organisms. Each turbine acts as a sensor for wind, movement, vibrations and temperature, capable of forming a network that monitors the surrounding area, from coastal waters to land borders. In an omni-use world, it is not just a power station, but a radar, a sentinel and a communication hub all in one. It is only natural that modern wind farms should become the backbone of a sensory network for security. Their turbines, equipped with radar and communication modules, could effectively monitor borders, the sea and airspace. This is how a dual-use infrastructure – serving both energy and defence purposes – can be built, one that not only generates power but also sees, hears and reacts.
>
> **Dr Andrzej Fałkowski**, Lieutenant General (Ret.), former Deputy Chief of the General Staff of the Polish Armed Forces; expert and strategic adviser, Polish Dual-Use Chamber of Commerce

2

Responding to New Challenges

Changes in the European security architecture between 2022 and 2025 lead to the conclusion that traditional military deterrence (deterrence by punishment) must be supplemented by a strategy of 'resilience by denial'. This means building a system in which a hybrid attack is so difficult to carry out and so easy to detect that it becomes unprofitable for the aggressor.

Critical infrastructure (ports, undersea cables, data centres) is also often privately owned. Effective defence requires deep operational integration – for example, incorporating sensors from private wind farms into the 'Baltic Sentry' surveillance system. The state must offer financial and legal incentives to companies implementing security-by-design technologies.

Looking ahead, threats involving swarms of autonomous drones and even more advanced AI-driven sabotage are likely to become a reality. Investment in projects such as NATO DIANA*g or the 'Eastern Shield' is not a one-off expense, but a process of continuous adaptation. Success depends on the ability to rapidly scale innovations from start-ups to the operational level of the armed forces and border guards.

Poland and the Baltic states are on the front line of a war that is already underway, though it has not been declared. Resilience to these threats depends on the synergy between an informed public, modern legislation and advanced technology that allows us to see more, react faster and protect more effectively.

End of Part 03

IV

PART IV — TECH & INNOVATION

The Next-Generation Defence Ecosystem

Russia's full-scale invasion of Ukraine has fundamentally changed the technology and innovation landscape of Central and Eastern Europe (CEE). Moving beyond its traditional role as an IT outsourcing base, CEE is becoming a core region for defence and strategic technology development. At the same time, dual-use technologies, used by both the military and civilians, have come to be seen as a critical foundation for national security, industrial competitiveness and societal resilience. As the strategic importance of AI and other emerging technologies grows, CEE's combat-tested ecosystem has become a new driving force behind Europe's strategic autonomy. This part traces the importance of dual-use technology, national defence innovation strategies and the development of start-up ecosystems in the CEE and DACH regions.

CHAPTERS IN THIS PART

01 The Critical Nature of Dual-Use Technology: Definition

02 The Critical Nature of Dual-Use Technology: Impact on National Resilience

03 Germany: Dual-Use Revolution

04 Poland: A Hub for Defence Innovation

05 The Baltic States and the V4: Complementary Ecosystems

06 Ukraine and CEE: A Combat-Tested Ecosystem

07 Case Studies: Start-ups from the CEE and DACH Regions

PART IV Tech and Innovation

I The Critical Nature of Dual-Use Technology: Definition

The geopolitical transformation triggered by Russia's full-scale aggression against Ukraine has fundamentally altered the innovation landscape in the region. CEE has ceased to function merely as an outsourcing base for Western IT corporations, evolving into a strategic hub for the production of sovereign defence technologies. A clear shift is evident: the concept of 'dual-use' has evolved towards 'omni-use' – technologies designed from the ground up to meet the demands of the battlefield (resilience to electronic warfare, absence of Chinese components), thereby actually gaining an advantage in the civilian market as well.

In 2025, investment in the defence and dual-use sector in Europe reached a historic record of $3.88 billion[*29]. It should be emphasised, however, that this was not merely a regional surge in investment, but a sign of a global shift in capital allocation. In its report on AI in dual-use technologies, the European Commission emphasises that Europe is entering a critical phase in which the ability to integrate AI into defence ecosystems will determine the continent's strategic autonomy[*30]. AI, although not formally classified as a weapon, has become a 'decisive enabler' in areas ranging from logistics to decision-making systems. In this context, start-ups from CEE, with their strong engineering base, have gained strategic importance for NATO.

It is worth highlighting the main factors shaping the potential of the dual-use ecosystem:

01 the ability to more readily foster individual innovations with potential applications in existing or new weapon systems, military equipment, uniformed services, and special services (including intelligence services)

02 the ability to achieve a better balance between cost and effectiveness, particularly given the clear trend towards increasing budgets for the development of conventional armaments programmes (cheaper does not always mean worse)

03 the potential for civil-military applications that can support the economy over the long term not only in wartime and crisis, but also in peacetime

First and foremost, the dual-use ecosystem, regardless of scale, enables the fulfilment of three critical tasks in the modern world.

The first is to stimulate innovation that may subsequently lead to the development of military and intelligence capabilities not previously covered by the research and development of the traditional defence sector. Of course, this assumes that not every innovation from the civilian sector will ultimately find its way into the military or the special services. However, it is crucial to demonstrate new possibilities and encourage freedom in exploring new avenues of research. The military and special services can treat the dual-use sector, so to speak, as a 'Team B' that continually challenges the established research and industrial sectors with which they collaborate on a daily basis.

The second aspect concerns the search for the necessary balance between two factors: cost and effectiveness. In the post-Cold War era, most major arms manufacturers and exporters moved towards technologically sophisticated production, but this was accompanied by higher production costs and lower production throughput. This reflected the assumption that the armed forces would primarily be engaged in limited armed conflicts, crisis response missions, counter-terrorism/counter-insurgency operations, or occupation and stabilisation missions – or, at most, conflicts of high initial intensity that did not require large, costly stockpiles. This was in line with, amongst other things, the American 'shock and awe' doctrine, which was intended to overwhelm and destroy the enemy in the initial strikes. Furthermore, this may have resulted from misinterpreting lessons learnt from operations during NATO's Allied Force campaign in the Balkans in 1999 or in Libya in 2011.

Since 2022, there has been an almost panic-driven departure from this paradigm. According to analyses by both warring sides, dual-use technologies are precisely the remedy for quantitative shortfalls and the accelerating pace of armament. In a sense, this means militarising sectors that previously had no contact with the military and drawing even their limited production capacity – and above all, their ideas – into the military sphere. The dual-use sector can therefore be viewed in the West as a conventional response to the needs of a war economy and, more importantly, to the needs of operations below the threshold of war. A system of incentives and measures to promote such activities is thus being built to encourage companies first to consider the possibility of dual-use activities and, eventually, to engage with the military and special services.

The third aspect to be taken into account is the desire to achieve a degree of flexibility in supporting one's own research and development sector and industry during periods of cumulative technological challenges for the entire nation. It should be noted that fierce technological competition has emerged globally, with a particular emphasis on so-called new and breakthrough technologies. The traditional poles of this competition are the Asia-Pacific (Indo-Pacific) region and the US. This motivates other countries to take action aimed at acquiring at least some ability to compete and thereby achieve a degree of technological sovereignty. However, this requires synergy between military and non-military sectors, for example through the allocation of resources to research and development from a dual-use perspective.

Dr Jacek M. Raubo, Head of the Defence24 Analysis Department; lecturer at Adam Mickiewicz University in Poznań; security and defence specialist

II The Critical Nature of Dual-Use Technology: Impact on National Resilience

The contemporary national security environment is characterised by a structural blurring of the boundaries between the civilian and military spheres, which necessitates a redefinition of traditional concepts of defence. The traditional dividing line between war and peace is eroding, and dual-use technology is becoming central to the new paradigm of national resilience. In an era of intensifying hybrid warfare and great-power competition, resources that were previously associated solely with the everyday comfort of citizens – such as access to water, electricity, stable telecommunications networks or efficient transport infrastructure – are becoming just as strategic as weapons systems.

For countries situated on NATO's strategic Eastern Flank, the adoption of dual-use technology is not merely an economic choice, but an existential necessity. National resilience today is built not only on military training grounds, but also in design offices and research laboratories, and forward-looking investments in infrastructure that stimulate economic growth in peacetime and can perform defensive, rescue or humanitarian functions in times of crisis.

The implementation of dual-use solutions brings tangible economic benefits to the state, allowing for the optimisation of budgetary expenditure and the stimulation of innovation in domestic industry. Market analyses indicate that the use of products proven in the civilian sector allows for significantly lower unit costs compared to systems designed from scratch exclusively for military purposes.

The scale and agility of commercial innovation allow governments to avoid costly duplication of research and development processes. Instead of investing in dedicated R&D programmes, states can act as partners that absorb the risks involved in adapting mature civilian technologies to military applications. This approach accelerates the so-called 'time-to-field', i.e. the time from identifying an operational need to deploying a ready-to-use solution, which is of decisive importance in modern conflicts.

Table 7: Benefits of Adopting Dual-Use Technologies

Benefit	Mechanism of action	Impact on security
Cost-effectiveness	Avoiding duplication of R&D investment	More systems for the same budget
Time advantage	Use of existing supply chains	Faster response to evolving threats
Access to talent	Attracting engineers from the BigTech sector	Innovative approach to technical problems
Scalability	Mass production for the civilian market	Ability to quickly replenish war losses

> Dual-use could also become a magnet for foreign investors seeking a stable manufacturing environment within the EU. Poland, due to its location and developing technological capabilities, could serve as a regional export hub for defence and civilian technologies, including unmanned systems, software, communications equipment and specialist vehicles. Furthermore, the use of European funds enables the financing of research infrastructure and the development of innovative solutions without placing an excessive additional burden on the state budget.
>
> — **Dr Andrzej Fałkowski**, Lieutenant General (Ret.), former Deputy Chief of the General Staff of the Polish Armed Forces; expert and strategic adviser, Polish Dual-Use Chamber of Commerce

1

Dual-Use Infrastructure as the Backbone of National Resilience

The concept of dual-use infrastructure goes beyond the traditional understanding of military logistics. It encompasses systems that support public welfare and social development during normal state operations but become defence tools in a crisis. The key features of such infrastructure are substitutability (the ability of civilian functions to substitute for military ones without major modification) and complementarity (the ability of multiple systems to reinforce one another in a crisis).

In Poland's strategic context, investment in transport infrastructure through the Connecting Europe Facility (CEF)[*h] and the EU's military mobility programmes is a key pillar. Poland secured more than €129 million in the latest CEF call for proposals, making it the largest beneficiary among EU Member States.

These investments aim to eliminate so-called bottlenecks in the transport network, enabling the rapid and smooth movement of heavy military equipment and personnel along NATO's Eastern Flank.

The flagship project in this area is the Central Communication Port (Centralny Port Komunikacyjny; CPK), which has been designed from the planning stage as infrastructure of strategic importance, combining the function of a global aviation hub with a key role in the national security system and the capacity to receive large-scale allied support.

2

Space Domain: Dual-Use in the Orbital Dimension

Space is the area where dual-use technology manifests itself most clearly. Satellites launched into orbit almost always perform hybrid functions, serving both civilian operators and the armed forces. Poland, aspiring to the status of an 'emerging space power', is stepping up its activities within the European Space Agency (ESA), building national capabilities across three key pillars: remote sensing, navigation and Earth observation.

Remote Sensing and Reconnaissance (SAR)

Satellite remote sensing uses sensors to acquire data on objects and installations with high accuracy. The key technology is synthetic aperture radar (SAR), which allows for imaging of the Earth's surface regardless of weather conditions or time of day. ICEYE, a Finnish company co-founded by a Pole and supplying Poland's armed forces through its Polish subsidiary, has

become a global leader in this segment, providing data that is critical for monitoring enemy troop movements, detecting camouflaged fortifications and verifying disarmament treaties.

PIAST (Polish Imaging Satellites)

For Poland, developing sovereign capabilities in this area through initiatives such as the PIAST (Polish Imaging Satellites) project means intelligence independence and access to objective, real-time data, which is essential for anticipating future threats and planning military operations.

Positioning, Navigation and Timing (PNT)

Satellite navigation systems (GNSS), such as the European Galileo or the American GPS, form the foundation of positioning, navigation and timing (PNT) functions. This function is essential for:

01 the precise guidance of munitions, including ballistic missiles and loitering munitions, during the terminal phase of flight

02 the synchronisation of joint operations and integrated command and logistics systems

03 detecting the adversary's critical infrastructure, such as command posts or communication nodes

Strengthening the Galileo system's resilience to jamming by state actors is one of the EU's security priorities, particularly in the Baltic Sea region.

Table 8: Key Examples of Dual-Use Technologies

Area	Civilian application	Military application
SAR remote sensing	Flood, glacier and land subsidence monitoring	Night-time reconnaissance; detection of concealed positions
Optical and hyperspectral Earth observation	Precision agriculture; disaster and environmental monitoring	Target identification; battle damage assessment (BDA)
GNSS positioning	Civil transport and logistics	Precision guidance of munitions; troop navigation
Communications	Internet access in remote areas	Secure communications for battlefield units
Autonomous flight and drones	Surveying, infrastructure inspection, agricultural spraying, logistics	Reconnaissance, loitering munitions, counter-drone interception
Underwater and maritime robotics (AUV/USV)	Undersea cable inspection; offshore wind maintenance	Undersea infrastructure protection, mine detection, anti-submarine and coastal surveillance
Cybersecurity	Protection of financial services and critical infrastructure	Offensive and defensive cyber operations
Quantum technology	Drug discovery, materials simulation, cryptography	Post-quantum cryptography, inertial navigation, high-sensitivity sensing

III Germany: Dual-Use Revolution

As detailed in Part I, Germany's transition to a war economy is increasingly blurring the boundaries between the civilian and military sectors in R&D. Germany, with its formidable scientific base, has launched a series of initiatives aimed at harnessing civilian innovation for national security.

1

Cyber Innovation Hub (CIHBw)

The Bundeswehr Cyber Innovation Hub (CIHBw) has become a key instrument in the digital transformation of the armed forces. Acting as a kind of 'catalyst for change', this unit bridges the gap between rigid military structures and the dynamic start-up ecosystem. The CIHBw's operating model is based on the so-called 'Innovation Funnel', which enables the identification, validation and prototyping of solutions within a 12–24-month cycle, bypassing lengthy procurement procedures.

Projects carried out by CIHBw cover a wide spectrum of dual-use innovations[*31]:

01 **Logistics and management**: the Yarded project has developed software that revolutionises the management of equipment and vehicle relocation at transhipment points, reducing operation times from days to seconds. This is a key technology given Germany's role as a logistics hub within NATO

02 **Reconnaissance and security**: the Mine-GeoJSON project introduces digital mapping of areas contaminated with unexploded ordnance, which is critical for mine clearance operations. Meanwhile, the ImageAware system uses AI to detect disinformation and deepfake content on social media, supporting situational awareness

03 **Electronic warfare**: as part of the Spectra Challenge, carried out in collaboration with the cyber agency, solutions are being developed to defend unmanned systems against electronic attacks

04 **Battlefield medicine**: applications such as Medical Video Consultation and faLKE (mobile light sources for medics) bring civilian telemedicine standards to the battlefield

2

Science and Defence

A paradigm shift is also underway in academia to promote dual-use initiatives. Traditionally, many German universities have applied the so-called 'Civil Clause' (Zivilklausel), voluntarily committing themselves not to conduct research for the military. In the face of new threats, however, the federal government and the state authorities (particularly in Bavaria) are seeking to lift these restrictions. Bavaria has introduced a new Higher Education Act, which, in effect, promotes cooperation between universities and the Bundeswehr, creating a legal framework to counter civil clauses that hinder research for security or defence purposes. Meanwhile, the Federal Ministry of Education and Research (BMBF) has published a position paper calling for deeper cooperation between civilian and military research institutions and the establishment of financial incentives for dual-use projects.

However, these changes are meeting with resistance from parts of the academic community and trade unions (such as Verdi), which fear the 'militarisation of science' and a loss of research autonomy. Despite the protests, the trend towards integration is accelerating, driven by EU funding through the European Defence Fund and by national funding.

3

Quantum and Hydrogen Technologies

The Bundeswehr Centre for Digitalisation and Technology Research (dtec.bw) funds projects of high strategic importance carried out at military universities in Munich and Hamburg.

01	**Munich Quantum Valley**	Munich Quantum Valley is a consortium involving Ludwig Maximilian University of Munich (LMU), the Technical University of Munich (TUM), the Fraunhofer Society, the Max Planck Society, the Bavarian Academy of Sciences and Humanities (BAdW), the German Aerospace Center (DLR) and Friedrich-Alexander University Erlangen-Nuremberg (FAU). With support from dtec.bw, the consortium aims to build competitive quantum computers. These technologies are crucial for cryptanalysis and battlefield simulation.
02	**QuESt project**	The QuESt project is a joint initiative between DLR and academic partners that uses quantum computers to simulate electrochemical processes in batteries and fuel cells. This has a direct impact on the performance of submarine propulsion systems and drone power systems.
03	**Defence use of hydrogen**	The defence use of hydrogen is being advanced through the QuESt project and joint research on new catalysts with the Max Planck Institute for Chemical Physics of Solids (MPI CPfS), with the aim of securing alternative energy sources for autonomous systems and military bases. This is expected to strengthen logistical resilience.

IV Poland: A Hub for Defence Innovation

Poland is actively building an ecosystem that supports dual-use innovation, utilising both national and international mechanisms. A record increase in defence spending (from 2.2% to 4.3% of GDP) presents a unique opportunity for the country's technological modernisation.

> The development of dual-use technology also strengthens the resilience and operational independence of the armed forces. Domestic production of components and systems used in both the civilian and military sectors reduces the risk of dependence on foreign supplies. In the event of a crisis, conflict or disruption to supply chains (which are already very lengthy), a country with its own industrial base can switch production from civilian to military use more quickly. This approach enhances security of supply, logistical stability and the resilience of the defence system to disruptions.
>
> — **Dr Andrzej Fałkowski**, Lieutenant General (Ret.), former Deputy Chief of the General Staff of the Polish Armed Forces; expert and strategic adviser, Polish Dual-Use Chamber of Commerce

1

National Defence Innovation Model

The Ministry of Development and Technology has established the 'Support for Competence in the Field of Dual-Use Innovation' programme for the years 2025–2029, with a budget of PLN 22 million (approximately €5.2 million)[*32]. The programme is built around three pillars:

01	**Start-up acceleration**: offering technical support, access to research infrastructure and opportunities to validate solutions under operational conditions
02	**Venture building**: forming interdisciplinary teams from the concept stage and facilitating technology transfer from universities to industry
03	**Building a network of mentors**: recruiting and training experts who will help innovators navigate the complex world of military procurement

The Polish Armaments Group (PGZ) and the Polish Development Fund (PFR) act as integrators, giving Polish companies access to a global financing network.

2

Engagement with NATO and the EU

Poland participates in the Defence Innovation Accelerator for the North Atlantic (DIANA) and the European Defence Fund (EDF), enabling national priorities to be aligned with NATO-wide objectives. Polish centres in Kraków and Gdańsk serve as 'living labs' where autonomy, AI and quantum technologies are tested.

Table 9: NATO, European and National Funding Programmes

Fund / programme	Budget / objective	Poland's role
NATO Innovation Fund	€1 billion for deep-tech	PFR contribution of €42 million*33 *34
EDF (European Defence Fund)	€1 billion annually for R&D*35	Active participation in industrial consortia
CEF (Military Mobility)	€1.69 billion for infrastructure*36	Largest number of projects in the EU
Ministry of Development and Technology programme (national)	PLN 22 million for capability development*37	Building a start-up ecosystem

DIANA has become a gateway for start-ups seeking to enter NATO's military procurement system. DIANA operates on a distributed model, integrating 16 accelerator sites and more than 200 test centres across the Alliance*38. In CEE, this architecture has been designed to reflect the specific characteristics of local innovation ecosystems. The 2026 cohort comprises 150 companies, including Poland's Vidoc Security Lab (AI-based code security) and Germany's Enclaive (post-quantum 5G) and VISS (hardware endpoint protection).

Poland hosts both a DIANA accelerator and one of the largest national networks of test centres in the region, making it a key hub in the DIANA architecture on NATO's Eastern Flank. This concentration of resources reflects Warsaw's ambition to become a leader in defence technologies within the Three Seas region.

Table 10: Key Technologies from the CEE Region in the DIANA Programme

Technology / solution	Company (country)	Defence application (dual-use)
Passive microsensors (MicroWire)	RVmagnetics (Slovakia)	Condition monitoring of hulls, engines and infrastructure without a power supply
LiquidRAN™ (5G software)	IS-Wireless (Poland)	Restoration of mobile networks in combat conditions; damage resilience
5G millimetre-wave technology	Microamp (Poland)	High-bandwidth, low-latency secure communications resistant to electromagnetic interference and jamming
Post-quantum cryptography	ResQuant (Poland)	Protection of communications against cryptographic attacks by quantum computers
Nanotechnology-based camouflage	InfraHex (Czech Republic)	Concealment of thermal signatures from drones and thermal imaging
Autonomous USV (uncrewed surface vessel)	Blue Armada Robotics (Poland)	Protection of wind farms, undersea cables and pipelines
Disinformation analytics	GATE Institute (Bulgaria)	Detection of disinformation campaigns and deepfakes
Composite structures	INCAS (Romania)	Rapid production of spare parts for drones in field conditions

2.1

Kraków DIANA Accelerator

At the heart of Poland's DIANA ecosystem is the Kraków Accelerator, established jointly by Kraków Technology Park (KPT) and the AGH University of Science and Technology. This model, based on cooperation between academia, industry and government, aims to 'commercialise' military technologies and adapt civilian solutions to defence needs.

AGH brings a strong research base to the consortium. The university files approximately 100 patent applications annually and has expertise covering nine of NATO's ten priority Emerging and Disruptive Technology (EDT) areas, including AI, engineering materials and space technologies*[39]. It also operates Poland's largest supercomputing infrastructure, an essential resource for simulating and training AI models.

The Kraków Technology Park is responsible for the business side of the acceleration programme, providing mentoring, access to market experts and pathways to commercialisation. The aim is not simply to create a prototype, but to build a scalable business model that can remain viable in the market.

2.2

Network of 10 Test Centres

Poland provides 10 highly specialised test centres to the DIANA network*[40], representing one of the largest national contributions in Europe. These centres enable the validation of technologies at high technology readiness levels (TRL) under conditions close to operational reality.

This diversity allows for comprehensive support for innovators, including testing quantum algorithms at the Poznan Supercomputing and Networking Center (PSNC) in Poznań, evaluating resistance to GPS jamming at the Center for Geospatial and Satellite Analysis (CENAGIS) in Warsaw, and conducting physical armour-resistance tests at the Military Institute of Armoured and Automotive Technology (WITPiS) in Sulejówek.

An analysis of dual-use technology and infrastructure leads to a clear conclusion: in the 21st century, national security is inseparable from the strength of the civilian innovation ecosystem. Traditional defence based solely on military resources is insufficient in the face of hybrid and technological threats.

The ultimate form of national resilience is the ability to rapidly reconfigure civilian resources – technological, logistical and energy-related – for defence purposes. As a frontline country, Poland must strive for full interoperability between its critical infrastructure and allied requirements.

Poland possesses all the necessary assets – intellectual, geographical and financial – to become a leader in dual-use technology in CEE. However, effectively implementing this strategy requires breaking down inter-ministerial silos and building, through sustained effort, a 'hidden army' of modern, resilient and flexible infrastructure and technologies that serve citizens every day and, when necessary, can defend the state.

V The Baltic States and the V4: Complementary Ecosystems

1

Estonia and the Baltic States

Estonia, host of the DIANA Regional Hub, acts as a coordinator for the Baltic Sea region. Building on its reputation as a 'digital state', Tallinn focuses on intangible technologies: cybersecurity, AI and autonomy.

1.1

The Tehnopol Accelerator and the Start-up Ecosystem

The Estonian accelerator, run by the Tehnopol Startup Incubator in Tallinn and the Tartu Science Park, is the gateway to one of the most integrated innovation ecosystems in Europe. Key areas include AI, cybersecurity and robotics. Estonia contributes eight test centres to the DIANA network, including the CR14 Foundation (cyber range) and the Estonian Academy of Security Sciences.

The Estonian company Wayren (tactical communications) has been selected for the second phase of the DIANA programme, confirming the high quality of local solutions in the field of secure communications. Another example is GaltTec, which is developing fuel cells, in line with the priority of energy resilience.

1.2

Lithuania and Latvia: Complementary Capabilities

The other Baltic states complement Estonia's offering. Latvia focuses on 5G technologies. The UniLab Defence accelerator in Riga and the 5G test site at the Ādaži base create a unique environment for testing next-generation connectivity in field conditions. Lithuania, in turn, leverages its expertise in laser technologies and a strong biotechnology sector. DIANA test centres, including the National Cyber Security Centre and the Vilnius University Life Sciences Center, support innovation in the fields of life sciences and cybersecurity.

2

Visegrad Group: Industrial and Research Synergies

Apart from Poland, the Visegrad Group (V4) countries – the Czech Republic, Slovakia and Hungary – bring significant assets to DIANA, combining industrial traditions with modern technologies.

VI Ukraine and CEE: A Combat-Tested Ecosystem

Ukraine has built a globally unique ecosystem of military innovation. The Brave1 cluster is the central mechanism, having funded hundreds of projects by 2025. Ukraine also serves as a unique testing ground for new solutions and technologies, utilised by major players such as international defence contractors (both American and European), technology firms (e.g. Anduril) and start-ups. Consequently, the Ukrainian front sees the deployment of both mass-produced weapon systems and prototypes of new solutions (e.g. unmanned systems), while new technologies, including electronic warfare systems, are tested under demanding combat conditions on the actual battlefield.

Building on Ukraine's experience, the start-up ecosystem in CEE reached a level of maturity between 2024 and 2026 that allows for genuine competition on global markets. This is no longer a market of 'novelties', but an integrated system delivering technologies battle-tested on the Ukrainian front. Poland acts as a manufacturing and financial hub, Ukraine as an R&D laboratory, and the Baltic states as pioneers of digitalisation. A clear division of roles is increasingly taking shape.

Scaling remains the main challenge. Companies that have undergone acceleration (DIANA) and created prototypes face barriers in public procurement. Army procurement systems remain slow and favour large players. On the other hand, companies such as the WB Group and PGZ are opening up to cooperation with smaller entities, which should enable them both to offer new solutions addressing the current and future needs of the military and to achieve the production volumes required by the Ministry of National Defence.

The outlook for 2026 is optimistic. Rising funding (a record $3.88 billion in 2025[*29]), a strong presence in NATO programmes, and integration with industry (as seen with FlyFocus and Lloyds) suggest that dual-use technologies are likely to replace traditional B2B software as the region's main driver of innovation.

The dual-use sector in CEE countries also has significant potential for growth due to the acceleration of military

spending. It should be noted that NATO's entire Eastern Flank – or, more broadly, its northern, eastern and, to some extent, southern flanks – is currently leading the way in defence spending, and most countries in these regions intend to maintain this course. However, they are not financially able to rely solely on the most expensive, purely military solutions (especially imported ones). Consequently, in the coming years, the market may be far more open to adopting dual-use solutions, particularly with a view to filling equipment gaps, addressing shortages of equipment and armaments, and countering Russia's 'game-changing' capabilities observed in Ukraine and elsewhere. Furthermore, many CEE countries are expanding the size of their armed forces, building up operational forces and territorial defence, and investing in the replenishment of reserves. It must therefore be emphasised that both the transformation under way in response to current threats and strategic thinking about future challenges create significant opportunities to explore dual-use technologies and, above all, pursue innovation.

Access to scientific and research resources is also becoming easier. In CEE, ethical and philosophical constraints on research related to military and security matters are comparatively limited. Moreover, technical universities and research centres are innovative, yet at the same time are in great need of funding. These institutions are therefore likely to have high expectations for dual-use technologies and broader cooperation in the fields of security and defence. Such cooperation, however, would not be bound by the traditional terms of the arms industry, which suffer from structural deficiencies.

CEE combines competitiveness and a willingness to take risks in the field of innovation, particularly with regard to military and security technologies. The region recognises that innovation is the only means by which it can compete or cooperate in one form or another, with leading exporters of military and intelligence solutions in the transatlantic, European and global arenas.

VII Case Studies: Start-ups from the CEE and DACH Regions

Satellite Systems and Reconnaissance

	**Constellr** Germany	Deploys a high-precision thermal infrared satellite constellation, a dual-use technology with applications in infrastructure anomaly detection and security.
	**Satim** Poland	Develops AI-based analysis of SAR imagery to automatically extract actionable information. It also partners with Synspective, a Japanese company developing SAR satellites.
	**KP Labs** Poland	The 'Intuition-1' satellite, which processes hyperspectral data directly in orbit using AI.
	**Scanway** Poland	Supplier of optics for the CAMILA constellation and ESA missions.
	**ENPULSION** Austria	Electric propulsion systems for small satellites, enabling orbital control and manoeuvrability for commercial and defence applications.

Communications and Cybersecurity

	**Microamp** Poland	5G millimetre-wave technology providing high-bandwidth, low-latency secure communications resistant to electromagnetic interference and jamming.
	**ResQuant** Poland	Post-quantum cryptography securing communications against attacks by quantum computers.
	**Wire** Germany	A fully end-to-end encrypted messenger for the government and corporate sectors.

Unmanned Systems and New Propulsion Systems

Quantum Systems Germany	Fixed-wing VTOL drones for reconnaissance and surveillance, supplied to the armed forces of more than six countries, including Ukraine.
ARX Robotics Germany	Autonomous unmanned ground vehicles configurable for multiple roles, including carrying reconnaissance radar, mine-clearing equipment, medical stretchers, as well as transporting ammunition. The company has secured a contract with the British Army.
Blue Armada Robotics Poland	Autonomous USVs for the protection of critical maritime infrastructure.

C-UAS (Counter-Drone Systems)

Alpine Eagle Germany	Develops Sentinel, an air-to-air C-UAS system combining airborne sensors, AI and a software-defined defence architecture. The Bundeswehr is an initial customer, and counter-drone trials have also been conducted in Ukraine.
Molfar Defence Ukraine/Poland	Develops tactical radar specialised in detecting and tracking small, low-flying drones, including fibre-optic-controlled drones that are less susceptible to electronic warfare jamming.
Frankenburg Technologies Estonia	Mark-1 missiles costing less than their target. Combat trials in Ukraine were scheduled for April–June 2026. The company has signed an MoU with South Korea’s Hanwha Aerospace.

AI Defence Platforms

Helsing Germany	Focuses on AI-driven battlefield awareness and decision support, while mass-producing systems such as the HX-2 loitering munition drone in Europe.

End of Part 04

V

PART V – IMPLICATIONS FOR JAPAN

Changes in the Security Environment and Strategic Opportunities for Japanese Companies

Russia's invasion of Ukraine has forced a fundamental rethink of the security environment not only in Europe but also in Japan. Emerging technologies such as unmanned systems, AI, directed-energy weapons (DEW), quantum technologies and space applications are rapidly changing the battlefield, blurring the line between the military and civilian spheres and widening the scope of security itself. Security advantage is increasingly determined not by military power alone but by national capability as a whole, including technology development, the industrial base and civil-military collaboration. Japan, meanwhile, faces an extremely complex geopolitical environment, confronting security challenges from China, Russia and North Korea at the same time. This part traces the structural changes in Japan's security environment, the shift in its security policy, the importance of the private sector in dual-use technology, and the strategic complementarity between Japan and the CEE and DACH regions.

CHAPTERS IN THIS PART

01 Structural Changes in Japan's Security Environment

02 Japan's Security Policy Shift – From 'Restraint' to 'Readiness'

03 The Importance of Dual-Use Technologies – Why Japan's Private-Sector Engagement Is Essential

04 Strategic Complementarity between Japan and the CEE and DACH Regions

PART V Implications for Japan

I Structural Changes in Japan's Security Environment

Russia's invasion of Ukraine has raised fundamental questions not only for Europe's security environment, but also for Japan's. The military domain is expanding at an unprecedented pace, while emerging technologies such as unmanned systems, AI, directed-energy weapons (DEW), quantum technologies and space applications are transforming the nature of the battlefield. As demonstrated on the battlefield in Ukraine, many of these technologies were developed in the civilian sector, and the traditional boundary between 'military' and 'civilian' is becoming increasingly irrelevant.

The threats that Japan is facing mirror those confronting Europe. China's defence spending grew to approximately 2.1 times its 2014 level over the following decade*41, while the possibility of a contingency involving Taiwan remains the single greatest variable in Japan's security planning. North Korea is advancing the development of hypersonic weapons, creating threats that are difficult for existing interception systems to counter. Russia is strengthening its military cooperation with China, repeatedly conducting joint bomber flights and joint naval operations. Japan therefore finds itself in an extremely challenging geopolitical environment, facing all three countries simultaneously.

At the same time, Japan must confront vulnerabilities specific to its own circumstances. Japan depends on imports for approximately 90% of its primary energy*42, while around 90% of its crude oil imports pass through the Strait of Hormuz from the Middle East*43. This exposure is no longer a theoretical risk, but a real-world crisis. In February 2026, following large-scale US and Israeli attacks on Iran, Iran's Islamic Revolutionary Guard Corps declared a ban on passage through the Strait of Hormuz, effectively bringing the strait under blockade. The number of vessels transiting the strait fell to just 191 in April*44, while major global container shipping companies including Maersk, CMA CGM and Hapag-Lloyd suspended passage through the strait. Described as the largest disruption to energy supplies since the oil crises of the 1970s, the situation caused a surge in crude oil prices and widespread disruption to global supply chains. For Japan, which depends heavily on Middle Eastern crude oil transported through the strait, the crisis has once again highlighted the vulnerability of its energy security. Combined with the inherent fragility of supply chains arising from Japan's geography as an island nation and its lagging cybersecurity measures, these factors could become critical bottlenecks in a contingency.

The 'Total Defence' doctrine and the concept of dual-use infrastructure adopted by CEE and DACH countries, as detailed in this report – supporting the economy in peacetime and protecting the state in a crisis – offer precisely the kind of approach to resilience from which Japan can learn. The Baltic states' approach of using wind farms as sensor networks and Poland's 'Eastern Shield', which incorporates civilian communications infrastructure into military redundancy, offer valuable models for Japan in integrating energy and security.

II Japan's Security Policy Shift – From 'Restraint' to 'Readiness'

Against this backdrop, Japan's security policy is undergoing its most significant transformation of the post-war era.

The three strategic documents formulated in 2022 – the National Security Strategy, the National Defense Strategy and the Defense Buildup Program – were groundbreaking in identifying China as the greatest strategic challenge Japan has ever faced and setting out a shift towards a more proactive defence posture, including the acquisition of counterstrike capabilities. Japan's defence budget for FY2026 reached a record high of approximately JPY 9.035 trillion, marking the 14th consecutive annual increase. Now in the fourth year of its five-year plan to double defence spending to 2% of GDP, the government is considering bringing forward the revision of the three strategic documents to the end of 2026*45.

The following three developments are particularly noteworthy:

01	**Strengthening Stand-Off Defence Capabilities**	More than JPY 970 billion has been allocated to stand-off missile capabilities in the FY2026 budget[*45], as Japan continues to build long-range strike capabilities, including an upgraded version of the Type 12 Surface-to-Ship Missile.
02	**Fundamental Revision of the Three Principles on Transfer of Defense Equipment and Technology**[*46]	In April 2026, under the Takaichi administration, the Three Principles on Transfer of Defense Equipment and Technology and their Implementation Guidelines were revised, abolishing the previous five categories – rescue, transport, warning, surveillance and minesweeping. The transfer of 'weapons' with lethal capabilities became permissible in principle, opening overseas markets to Japan's defence industry. However, as of May 2026, transfers remain limited to countries that have concluded agreements with Japan on the transfer of defence equipment and technology. In Europe, only five countries currently meet this requirement: the United Kingdom, France, Germany, Italy and Sweden. Negotiations are under way to conclude such an agreement with Poland, a key country in CEE, and such an agreement would represent an important milestone in advancing concrete defence-industry cooperation between Japan and the CEE region.
03	**Building the Institutional Framework for Economic Security**	Japan's security clearance system, established under the Act on the Protection and Utilization of Critical Economic Security Information, came into force in May 2025, creating a legal framework for Japanese companies to access sensitive security information. The Key and Advanced Technology R&D through Cross Community Collaboration Program (K Program) promotes research and development across four domains: maritime; space and aviation; cross-domain and cyberspace; and biotechnology. In addition, the government designated AI and semiconductors as 'national strategic technologies' in FY2026 and announced plans to raise its public- and private-sector science and technology investment target from JPY 120 trillion to JPY 180 trillion[*47].

III The Importance of Dual-Use Technologies – Why Japan's Private-Sector Engagement Is Essential

Technological capability is key to building military power, and the source of that capability is increasingly shifting to the civilian sector. Innovation in areas such as AI, quantum computing, advanced materials and autonomous systems is being driven by universities, research institutions and private companies, including start-ups.

In Japan, putting this recognition into practice presents a distinct set of challenges. The Science Council of Japan has repeatedly expressed caution towards research for military purposes, and many universities have historically refrained from engaging in defence-related research. Together with the restrictions imposed by the Three Principles on Transfer of Defense Equipment and Technology until their revision in April 2026, these factors reflect a broader public aversion to military affairs that has hindered the accumulation of technological capabilities. At the same time, as Japan's reliance on procurement through the US Foreign Military Sales (FMS) programme has increased, concerns have been raised that increasing dependence on technologies that remain effectively 'black boxes' could hollow out Japan's domestic technological base.

However, the rapid changes in the security environment since 2022 are transforming this structure. The establishment of the K Program, the introduction of the security clearance system and the revision of the Three Principles on Transfer of Defense Equipment and Technology are all lowering barriers to private-sector participation in the security field. Dual-use technologies have the capacity both to drive economic growth and to provide military advantage, making public-private collaboration essential to their development and implementation.

IV Strategic Complementarity between Japan and the CEE and DACH Regions

As detailed throughout this report, the CEE and DACH regions, located in close proximity to Ukraine, play a central role in Europe's defence-tech and dual-use sectors and have produced many promising start-ups. The ecosystems in these regions offer an exceptionally high degree of strategic complementarity for Japanese companies and investors. The following sections outline the institutional, technological and economic factors underpinning this complementarity, as well as specific opportunities for Japanese companies.

Progress in Institutional Frameworks

Institutional cooperation between Japan and Europe is advancing rapidly. In November 2024, Japan and the EU concluded the first Security and Defence Partnership of its kind between the EU and a country in the Indo-Pacific region, establishing a framework to promote cooperation in areas including maritime security, cybersecurity and responses to hybrid threats. Japan is positioned as one of the partner countries expected to participate in the EU's SAFE programme, a €150 billion financing instrument for defence procurement, creating the potential for joint procurement with EU Member States and for products from Japanese companies to become eligible for purchase under the programme.

Progress is also being made at the bilateral level. In April 2026, Prime Minister Takaichi and Polish Prime Minister Tusk held a summit meeting and upgraded bilateral relations to a 'Comprehensive Strategic Partnership'. An Action Plan for 2025–2029 was signed, and the two sides agreed to promote security cooperation, including in the defence industry and dual-use sectors, and to accelerate discussions towards establishing a framework for information protection. Poland is the largest economic and military power in CEE, and deepening the strategic partnership with Poland will provide an important foothold for Japan in strengthening cooperation across the CEE and DACH regions.

Technological Complementarity

The CEE and DACH regions possess a growing body of engineering expertise and solutions that have been combat-tested on the Ukrainian front, while facing a structural shortage of scaling capital for growth-stage companies. Although investment in Europe's defence and dual-use sectors reached a record $3.88 billion in 2025*[29], private investment across the broader technology sector in CEE remains at just 0.03% of GDP, well below both the United States (0.74%) and the European average (0.17%)*[48]. Japan possesses world-class technological capabilities in advanced materials, precision manufacturing, semiconductors, optical equipment and robotics. Addressing the funding gap while bringing together these complementary technological strengths could create significant value for both sides.

In cybersecurity, the CEE and DACH regions have accumulated practical cyber-defence expertise, led by Estonia, home to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), while Japan, led by the National Institute of Information and Communications Technology (NICT), is taking a leading role in the international standardisation of quantum cryptographic communications. In autonomous unmanned systems, combining combat-tested drone technologies from the CEE and DACH regions with Japan's sensors, precision motors and solid-state battery technologies could deliver significant improvements in performance. In satellite remote sensing, technological cooperation between ICEYE, a global leader in SAR satellites, and Japan, with its long track record in satellite operations, could significantly enhance reconnaissance and surveillance capabilities. In energy resilience, there is also considerable potential for collaboration between the defence applications of fuel-cell and hydrogen technologies exemplified by Germany's QuESt project and Japan's hydrogen and solid-state battery technologies. By bringing together the CEE and DACH regions' strengths in 'combat validation and rapid implementation' with Japan's 'depth of fundamental technologies and manufacturing quality', the two sides have the potential to create significant value.

‘Friend-Shoring’ and Supply-Chain Restructuring

Amid deepening US-China tensions, Europe is accelerating efforts to build ‘China-free’ supply chains. Under the SAFE programme, components originating from outside the EU, EEA-EFTA countries and Ukraine are limited to 35% of the final product’s component costs. Japan is positioned within this framework as a ‘trusted partner’ and can help address supply-chain vulnerabilities in areas ranging from raw materials for nitrocellulose to advanced semiconductors and sensor technologies. The advanced chemical and materials technologies and quality-control expertise of Japanese companies could also bring significant value to initiatives such as the development by Polish research groups of technologies to produce nitrocellulose from waste wood and waste cotton.

The Strategic Imperative for International Cooperation

Japan’s K Program and security clearance system represent important steps, but it is unrealistic to expect domestic initiatives alone to fill, within a short period, the gaps in technological accumulation created by Japan’s longstanding aversion to military technology. Cooperation with the CEE and DACH regions, where technologies continue to be refined on the Ukrainian front – the world’s largest testing ground – is a strategic imperative for both Japan’s security and economic growth.

For Japan, partnership with the CEE and DACH regions is not merely an investment opportunity. It is a means of building a global technological security network and represents the most rational response to the geopolitical challenges of the 21st century. Deepening engagement with a region that has become a frontline of modern defence will directly strengthen Japan’s own security foundations.

End of Part 05

Notes and References

Notes

*a **Suwałki Gap**
An approximately 65-km land corridor along the border between northeastern Poland and Lithuania. It is bordered by the Russian exclave of Kaliningrad to the west and Belarus to the east. As its closure would isolate the Baltic states, it is considered a vulnerability in NATO's defence of its Eastern Flank.

*b **Fulda Gap**
A corridor near Fulda in the central German state of Hesse. Its relatively traversable terrain lies between the Vogelsberg and Rhön mountain ranges and provides access westwards towards Frankfurt and the Rhine-Main region. During the Cold War, NATO regarded it as a particularly critical potential route for a Warsaw Pact invasion of Western Europe.

*c **Rail Nordica**
A railway infrastructure project aimed at connecting Finland and Sweden using the European standard gauge (1,435 mm).

*d **PLN–EUR conversion**
The conversion from Polish zloty (PLN) to euros (EUR) in this report is based on the average exchange rate from 2 January to 8 May 2026 (EUR 1 = PLN 4.24).

*e **CZK–EUR conversion**
The conversion from Czech koruna (CZK) to euros (EUR) in this report is based on the average exchange rate from 2 January to 8 May 2026 (EUR 1 = CZK 24.34).

*f **Brave1**
A defence technology cluster established by the Ukrainian government in 2023 to support the country's private-sector start-ups.

*g **NATO DIANA (Defence Innovation Accelerator for the North Atlantic)**
NATO's defence innovation accelerator.

*h **Connecting Europe Facility (CEF)**
A key EU infrastructure investment programme that supports the development of trans-European networks across three sectors: transport, energy and digital.

References

01 IMF, World Economic Outlook, April 2026
https://www.imf.org/external/datamapper/datasets/WEO

02 WIPO, Global Innovation Index
https://www.wipo.int/gii/

03 Scaleway Blog, "DACH region: the world's 2nd largest market for SaaS"
https://www.scaleway.com/en/blog/how-to-make-it-in-the-dach-region-the-worlds-2nd-largest-market-for-saas/

04 Preqin / GlobeNewsWire, "Private capital DACH-based fund managers grow AUM to €238bn," 14 December 2023
https://www.globenewswire.com/en/news-release/2023/12/14/2795999/0/en/Private-capital-DACH-based-fund-managers-grow-AUM-to-238bn-Preqin-reports.html

05 NATO, Secretary General Annual Report 2025

06 NATO, "Defence expenditures and NATO's 5% commitment"
https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment

07 AP News, "Germany to raise defense spending to 3.5% of GDP in 2029"
https://apnews.com/article/germany-defense-spending-budget-nato-169e869922af3d349329ac1a921e634d

08 Business Sweden, "Germany's record defence modernisation drive"
https://www.business-sweden.com/insights/blogs/germany-a-new-era-for-investment/germanys-record-defence-modernisation-drive-as-of-22-october-2025/

09 FW-Mag.com, “Rheinmetall pursues its industrial expansion in Europe”
https://www.fw-mag.com/shownews/779/rheinmetall-pursues-its-industrial-expansion-in-europe-germany-romania-lithuania

10 Defence24, “Amunicyjny ‘głód’ w Europie”
https://defence24.pl/sily-zbrojne/amunicyjny-glod-w-europie

11 Khurana, M., “Inside the U.S. city churning out Ukrainian weapons,” NPR, 16 September 2024
https://www.npr.org/2024/09/15/nx-s1-5090966/scranton-munitions-factory-ukraine-war-russia-howitzer-rounds

12 Stoltenberg, J., Interview with The Guardian, “Nato chief: west must brace to support Ukraine in a long war,” 23 March 2023
https://www.theguardian.com/world/2023/mar/22/jens-stoltenberg-nato-chief-west-support-ukraine-for-long-war

13 U.S. Army, “Army seeks to expand and accelerate 155 mm production,” 2024
https://www.army.mil/article/283210/army_seeks_to_expand_and_accelerate_155_mm_production

14 Defense Daily, “MSM North America Awarded $632.5 Million To Build Army’s ‘Most Advanced’ 155mm Ammo Facility,” 2025
https://www.defensedaily.com/msm-north-america-awarded-632-5-million-to-build-armys-most-advanced-155mm-ammo-facility/army/

15 Rheinmetall AG, “Rheinmetall completes acquisition of Expal Systems,” Press Release, 2023
https://www.rheinmetall.com/en/media/news-watch/news/2023/8/2023-08-01-rheinmetall-completes-acquisition-of-spanish-defence-contractor-expal-systems

16 Rheinmetall AG, Annual Report 2024
https://www.rheinmetall.com/Rheinmetall%20Group/Investor%20Relations/Ver%C3%B6ffentlichungen/Pr%C3%A4sentationen%20und%20Berichte/2025/GB/Rheinmetall-Annual-Report-2024.pdf

17 L. Prus, “PGZ outlines development of three artillery ammunition production sites in Poland,” Defence Industry Europe, 9 July 2025
https://defence-industry.eu/pgz-outlines-development-of-three-artillery-ammunition-production-sites-in-poland/

18 Czechoslovak Group, “ZVS Holding has concluded a framework agreement with the Ministry of Defense of the Slovak Republic for the supply of ammunition to EU member states, worth up to 58 billion EUR”
https://czechoslovakgroup.com/en/news/zvs-holding-has-concluded-a-framework-agreement-with-the-ministry-of-defense-of-the-slovak-republic-for-the-supply-of-ammunition-to-eu-member-states-worth-up-to-58-billion-eur-with-the-potential-use

19 U.S. Department of Defense, Fact Sheet on Efforts of Ukraine Defense Contact Group National Armaments Directors, 10 January 2025
https://www.globalsecurity.org/wmd/library/news/ukraine/2025/01/ukraine-250110-dod01.html

20 Reuters, “Northrop Grumman and Polish arms maker aim to produce more than 180,000 artillery shells a year in Poland,” 11 February 2026
https://www.investing.com/news/stock-market-news/northrop-grumman-and-polish-arms-maker-aim-to-produce-more-than-180000-artillery-shells-a-year-in-poland-4501059

21 European Defence Agency, Coordinated Annual Review on Defence (CARD) Report 2024

22 “Poland receives first €6.6 billion payment under SAFE”
https://defence-industry-space.ec.europa.eu/poland-receives-first-eu66-billion-payment-under-safe-2026-05-29_en

23 “SAFE | Security Action for Europe - European Commission”
https://defence-industry-space.ec.europa.eu/eu-defence-industry/safe-security-action-europe_en

24 “Russian Drones Create a Kill Zone. Poland Is Left Behind [INTERVIEW]”
https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/rosyjskie-drony-tworza-strefe-smierci-polska-zostaje-z-tylu-wywiad

25 EY, Navigating Ukraine’s Defense Tech Market, October 2025
https://www.ey.com/content/dam/ey-unified-site/ey-com/en-ua/insights/defense-tech/navigating-ukraine-defense-tech-market.pdf

26 K. Nieczypor, S. Matuszak, “Game of drones: the production and use of Ukrainian battlefield unmanned aerial vehicles,” OSW Centre for Eastern Studies, 14 October 2025
https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned

27 Politico, “China is helping Russia build a lethal drone war machine”
https://www.politico.eu/article/china-russia-lethal-drone-war-race-ukraine-war-invasion-manufacture-putin-tech/

28 CNN, “Poland blames Russian intelligence for arson attack on Warsaw shopping center last year,” 11 May 2025
https://www.cnn.com/2025/05/11/europe/poland-blames-russian-intelligence-fire-shopping-center-latam-intl

29 Balnord, Casimir Pulaski Foundation, PFR, Dual-use Founder’s Handbook: From Foundation to Scale, Vol. 2, 2025
https://resources.balnord.vc/dual-use-handbook

30 AI-enabled Dual-Use Tech and the role of the EU’s Startup Ecosystem
https://digital-strategy.ec.europa.eu/en/library/ai-enabled-dual-use-tech-and-role-eus-startup-ecosystem

31 Cyber Innovation Hub der Bundeswehr, “Innovation Projects”
https://www.cyberinnovationhub.de/en/innovation/innovation-projects

32 Ministerstwo Rozwoju i Technologii, Program Ministra na lata 2025-2029
https://www.gov.pl/web/rozwoj-technologia/program-ministra-na-lata-20252029-wsparcie-kompetencji-w-obszarze-innowacji-dual-use

33 PFR Ventures, “Polish Development Fund invests in NATO Innovation Fund”
https://pfrventures.pl/en/artykul/polish-development-fund-invests-nato-innovation-fund

34 Business Insider Polska, “Obronność: Polska zainwestuje miliony w start-upy. To część projektu NATO”
https://businessinsider.com.pl/wiadomosci/obronnosc-polska-zainwestuje-miliony-w-start-upy-to-czesc-projektu-nato/gmg4lyk

35 “European Defence Fund (EDF) - Official Webpage of the European Commission. - Defence Industry and Space”
https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

36 Sprawozdanie specjalne 04/2025: Mobilność wojskowa w UE – Uchybienia w koncepcji i przeszkody napotkane w trakcie realizacji spowalniają postępy
https://www.eca.europa.eu/ECAPublications/SR-2025-04/SR-2025-04_PL.pdf

37 “Program Ministra na lata 2025-2029 „Wsparcie kompetencji w obszarze innowacji dual-use” - Ministerstwo Rozwoju i Technologii - Portal Gov.pl”
https://www.gov.pl/web/rozwoj-technologia/program-ministra-na-lata-20252029-wsparcie-kompetencji-w-obszarze-innowacji-dual-use

38 NATO DIANA, “About DIANA”
https://www.diana.nato.int/about-diana.html

39 “Krakow DIANA Accelerator”
https://diana.krakow.pl/

40 NATO DIANA, “Test Centres”
https://www.diana.nato.int/test-centres.html

41 Ministry of Defense of Japan, Defense of Japan 2024
https://www.mod.go.jp/j/publication/wp/wp2024/pdf/index.html

42 IEA, World Energy Balances 2025

43 Ministry of Finance, Japan, Trade Statistics of Japan.

44 CNN, “Visualizing shipping through the Strait of Hormuz since war began”
https://www.cnn.com/2026/04/29/world/iran-war-gulf-hormuz-shipping-maps-intl-vis

45 Ministry of Defense of Japan, Progress and Budget in Fundamental Reinforcement of Defense Capabilities – Overview of FY2026 Budget
https://www.mod.go.jp/j/budget/yosan_gaiyo/fy2026/yosan_20251226.pdf

46 Ministry of Defense of Japan, “Partial Revision of the Three Principles on Transfer of Defense Equipment and Technology and Related Guidelines,” 21 April 2026
https://www.mod.go.jp/j/press/news/2026/04/21a.html

47 Cabinet Office, Government of Japan, Seventh Science, Technology and Innovation Basic Plan, Cabinet Decision, March 2026
https://www8.cao.go.jp/cstp/kihonkeikaku/index7.html

48 Atomico, State of European Tech 2025

Disclaimer

01 This material has been prepared by an authoring team comprising four Partners of ff Red & White for the purpose of providing readers with information on changes in the security architecture and developments in the dual-use technology market in Central and Eastern Europe. It has not been prepared or distributed for the purpose of soliciting, recommending, offering or selling any particular securities, financial instruments, investment products, services or other transactions.

02 This material has been prepared on the basis of information that the authoring team considers reliable; however, no representation or warranty is made as to the accuracy, completeness or timeliness of such information. The contents of this material are current as of the date of preparation and are subject to change without notice.

03 ff Red & White and JBIC IG Partners assume no responsibility or liability whatsoever for any investment, business or other decisions or actions taken in reliance on the information or views contained in this material, or for any loss or damage arising therefrom.

04 The views expressed in this material are those of the authoring team and do not represent the views of JBIC IG Partners, a shareholder of ff Red & White, or of the Japan Bank for International Cooperation and IGPI Group, which are shareholders of JBIC IG Partners.

05 This material is provided solely for the use and information of its recipient. No part of this material may be reproduced, copied, modified, provided to any third party or otherwise used for any purpose other than that for which it was provided without the prior written consent of ff Red & White.

Published by

Company name	ff Red & White Ventures sp. z o.o. *i
Address	Poznańska 37/lokal B23, 00-689 Warszawa, Poland
Website	https://ffrw.vc/

Contact

Masayuki Ohta	masayuki@ffvc.com
Taro Hizume	taro@ffvc.com

*i ff Red & White Ventures sp. z o.o. is a Poland-based investment advisory company that advises ff Red & White, a venture capital fund investing in start-ups across the CEE and DACH regions.