

Think Tanks Essentials

ISSUE 9 · SEPTEMBER 2026

Security Architecture for a Changing Europe

DETERRENCE
RESILIENCE
ENLARGEMENT
ENERGY SECURITY
A STRONGER AGENCY

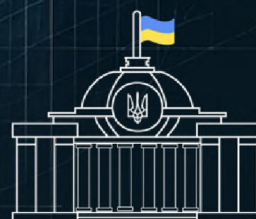
PEOPLE
BORDERS
OPPORTUNITIES

AN OPEN
EUROPE
A STRONGER
TOMORROW

UDO
NATION



EEYES
EASTERN EUROPE YOUTH
EMPOWERMENT SPACE



STRATEGY TODAY
A STRONGER TOMORROW

IDEAS
PEOPLE
POLICY
IMPACT

A MORE
RESILIENT
EUROPE

A
WIDER
SAFER
STRONGER
EUROPE

SECURE
DIVERSE
SUSTAINABLE

IDEAS
FOR A MORE
SECURE
AND UNITED
EUROPE



Think Tanks Essentials

Issue №9

Kyiv, 2026

In a rapidly changing world, think tanks have become key players in shaping international debates and strategies. They not only generate ideas but also define the direction of political decision-making and influence public opinion.

The magazine “ThinkTanks Essentials” was created to summarize and analyze the most important expert research, demonstrating how it shapes our understanding of the global order.

This publication is valuable for anyone seeking to navigate the increasingly complex landscape of international politics. It allows readers to track key trends and explore the arguments of leading experts who influence the decisions of governments and international organizations. For researchers and students, it serves as a convenient source of analytical insights and up-to-date case studies; for diplomats and policy experts, it is a tool for understanding global processes and anticipating possible scenarios; and for a broader audience, it offers an opportunity to look beyond news headlines and grasp the deeper context behind them.

CONTENTS

Building Comprehensive Deterrence on NATO's Eastern Flank: Ukrainian Experience and Alternative Russian Identity.....	8
Section 1. Overview of think tanks analyses.....	12
NATO and the New European Security Architecture.....	13
The potential US withdrawal from NATO under American law.....	14
The Ankara Summit: It's Trump's NATO – Europe just lives in it.....	15
NATO's Eastern Flank Frontier.....	16
Legality and Reality: The Eastern Flank and the Ottawa Convention.....	17
When Old Certainties No Longer Hold: Nordic-Baltic Foreign Policy Adaptation.....	18
European Defense and Strategic Autonomy.....	21
Strategic autonomy and Europe's new logic of intervention.....	22
Not just an addendum: Making resilience a key pillar of Europe's defence.....	23
The FCAS Collapse and Europe's Enduring Coordination Problem.....	24
NATO's digital arsenal: How Europe can avoid a new dependence on America.....	25
EU Defence Series: Europe's Tech Challenge.....	26
Buzzkill: How to defend Europe against drones.....	27
The Russian-Ukrainian War.....	29
The Trap Closes: How Russia Suppresses Resistance in Occupied Ukraine and How We Can Still Help.....	30
Empowering Ukraine: Spend smarter, support harder.....	31
The Special Tribunal for Ukraine: Turning the Wheels of International Justice.....	32
Facing the North Korea–Russia alliance: EU–ROK strategies for deterrence and cooperation.....	33
A Declining, but More Dangerous Power: Russia's Receding Reach in the Neighbourhood...	34
EU Enlargement and Ukraine in Europe.....	37
The Future of EU Enlargement Policy: Four Scenarios for Enlargement in Wartime Europe..	38
The magnificent ten: A coalition of the willing to drive the EU's next enlargement.....	39
Ukraine and the Next MFF: The Strive for Predictability.....	40
Escalating the Polish-Ukrainian dispute: Russia's operational objective in Poland.....	41
Economic Security, Sanctions, and Strategic Dependencies.....	43
Europe's energy security in 2026: More resilient, but systemically exposed.....	44
The European Union faces "China Shock 2.0".....	45
Countering the use of crypto-assets to circumvent sanctions against Russia.....	46
Strategic Corruption: The Nexus Between Russian Illicit Financial Flows and Offshore Finance.....	47
The results and limits of European states' interventions against the Russian shadow fleet....	48
The Transformation of the West and European Political Agency.....	51
France and Germany: Overcoming Differences to Strengthen European Sovereignty (fr. France - Allemagne : dépasser les différends pour renforcer la souveraineté européenne)..	53
The tragedy of "Westalgia".....	54
Europe in an Age of America First Economics.....	55
If Marine Le Pen wins: A European guide to a far-right France.....	56

Section 2. Insight Lab Analytical Materials.....	59
Popovych, Oleksandra. A Russian drone on the territory of NATO member states: what does it mean?.....	61
Vasylyk, Yaryna. From Shahed to joint production: what Russia and Iran have learned from each other.....	65
Kot, Kateryna. Sabotage as a Tool of Foreign Policy: How Is Russia Testing the Limits of the West's Response?.....	68
Lonchyna, Yuliia. When Sabotage Becomes an Attack: Does NATO Article 5 Apply to Russian Hybrid Operations?.....	72
Melkonova, Olena. Can the Defense Industry Become Ukraine's New Economic Specialization Within the EU?.....	76
Troian, Andrii. Ukraine's Defence Industry after the War: A Driver of Economic Development or a Temporary Advantage?.....	80
Pomohaibo, Nazarii. Deterrence Without War: Are the Baltic States Prepared for Russian Hybrid Threats?.....	85
Team.....	90
References.....	92
Photos and Images.....	103

BUILDING COMPREHENSIVE DETERRENCE ON NATO'S EASTERN FLANK: UKRAINIAN EXPERIENCE AND ALTERNATIVE RUSSIAN IDENTITY

Eastern flank and Russian threat

The Eastern Flank covers NATO's border region from the Baltic Sea and Estonia to the Black Sea in Bulgaria. Finland and Norway, which also border the Russian Federation, are included in the Northern Flank and constitute a separate area of operations. The borders of the Eastern Flank were established in 2004, when the threat posed by the Russian Federation was not yet fully recognized. Today, the region is an operational zone whose primary objective is to deter potential Russian aggression.

Following the Russian Federation's invasion of Ukraine in 2014, NATO's Eastern Flank became a strategic priority. As Putin continued to weaponize anti-Western rhetoric, the threat to NATO became increasingly tangible. In the aftermath of hybrid and cyberattacks against NATO member states, strengthening the Eastern Flank became a matter of collective security. Following the 2016 Warsaw Summit, an Enhanced Forward Presence (EFP) composed of multinational forces was established to deter potential aggression by the Russian Federation. The presence of multinational brigades on the Eastern Flank meant that, in order to advance, Russian forces would have to attack troops from multiple NATO member states, thereby increasing the likelihood of the application of Article 5 of the North Atlantic Treaty.

Originally, the EFP focused on ensuring the defense of the NATO member states bordering the Russian Federation: Poland, Lithuania, Latvia, and Estonia. However, after 2022, when the Russian Federation launched a full-scale invasion of Ukraine using an army of hundreds of thousands of troops, the EFP was further expanded to include Slovakia, Hungary, Romania, and Bulgaria, thereby covering the entire Eastern Flank.

However, the mere presence of EFP forces does not guarantee the Eastern Flank's protection against a potential Russian attack. The initial concept behind the deployment of the EFP was not that these forces would be capable of independently repelling a large-scale attack, but rather that an attack on EFP brigades would draw the majority of NATO member states into the war. The bulk of the forces consists of infantry, which may not be sufficient to withstand the Russian Federation's forces, given Russia's advantages over NATO in drone warfare, resulting from its combat experience, logistics, and established production capacity. Another concern is logistical: the Suwałki Gap between Poland and Lithuania could potentially be cut off by the Russian Federation, leaving parts of the Eastern Flank vulnerable.

In 2024, Poland decided to construct the East Shield, a defensive line along its border with the Russian Federation. The project reportedly draws on lessons learned from the Russian-Ukrainian War. According to publicly available plans, the defensive system will extend several hundred meters inland, with significant emphasis placed on the construction and maintenance of infrastructure near the border.

To sum up, the initial reasoning behind the structural defense of the Eastern flank has become outdated. It does not take into account the modern developments of warfare and geopolitical situation.

Drone revolution

For now, The Russian Federation is constrained by the war in Ukraine. Any peace deal or truce with Ukraine would free up significant forces, some of which would likely be stationed along Russia's western border.

The army stationed there would not resemble the Russian army of today. These would be experienced units proficient in the use of FPV drones, including fiber-optic drones, as well as mid-range and deep strikes. A defensive line consisting of positions less than one kilometer deep would not be sufficient to withstand an assault. The right combination of drone types, together with the unavoidable overstretching of anti-drone systems, could result in the elimination of front-line defensive positions within minutes, provided there had been preliminary reconnaissance and prior weakening of logistics through mid-range strikes.

Moreover, no defenses can hold without properly trained and equipped soldiers. EU countries simply do not have the relevant type of military experience comparable to prolonged warfare in Ukraine. Specialized anti-drone training for infantrymen and the creation of their own drone units are absolutely necessary to make these defenses combat-ready, but current military doctrines do not sufficiently address these needs. The existing means of countering drones are either too scarce and costly for widespread deployment or become obsolete too rapidly to keep pace with advances in drone technology.

Poland and the Baltic states should closely review Ukraine's experience in drone warfare. Ukrainian instructors have real battlefield experience that is incomparable to any theoretical preparation NATO instructors may be able to provide. At the same time, Ukraine has established a so-called kill zone along the front line, which has proved effective against more numerous and constantly advancing Russian forces. This system consists of more than a single defensive line. The kill zone includes multiple positions that may stretch dozens of kilometers deep and are properly disguised, connected, and coordinated. Drone-enabled logistics sustains the front line, where personnel rotation is complicated. The lessons of the war in Ukraine are not being used to build appropriate defenses for East Shield, and this is a fatal flaw that may result in a successful Russian advance during the initial phase of an invasion.

Sub-threshold warfare

At the same time, the Russian Federation continues to carry out subversive, subthreshold activities. The use of proxy forces, intimidation (including diplomatic pressure), information operations, sabotage, cyberattacks, lawfare, economic coercion, and political destabilization are among the methods typically employed below the threshold of conventional warfare to achieve political goals. The frequency of these subversive actions has risen dramatically across Europe since 2022 compared with the period before the full-scale invasion. While defenses and resilience are being strengthened, attributing subversive actions and providing a timely response remain highly challenging. The statistics do not include aspects of cognitive warfare and political destabilization, which are even more difficult to identify and counteract. We can, however, reliably determine that at least one-third of all operations were dedicated to election and information campaigns.

As some studies note, the Russian Federation has been successful in at least some of its endeavors when subversive actions, combined with other factors, have led to the desired behavioral changes in Belgium and Poland. While the ultimate objectives of Russian hybrid influence remain unachieved, the Russian Federation has managed to weaken support for Ukraine and sabotage infrastructure.

Moreover, the success of these subversive actions has exposed decision-making delays, an inability to produce a coordinated response, and polarization within the alliance.

Currently, Poland and the Baltic states have come to recognize the hybrid nature of the threats posed by Russia. Nevertheless, cohesive operational frameworks for countering Russian subthreshold warfare have not yet been established, although the threat is widely discussed and recognized on paper.

Russian identity within the frameworks of strategic deterrence

Any concept of strategic deterrence and hybrid warfare inevitably includes cognitive and social dimensions. Awareness of hybrid threats requires strengthening one's own resilience while pursuing the political, social, and cognitive destabilization of a rival. A defensive line cannot hold an enemy for long if one's own population advocates surrender and the rival's system of governance remains untouched. The decision to construct East Shield is an obligation related to deterrence in terms of hard power. But what about soft power?

The Russian Federation should not only be deterred; it should also be studied critically and substantively. Europe must increase its readiness not only in terms of hard power, but also in the field of cognitive warfare. First, The Russian Federation must be recognized as a rival. The war against Ukraine has shown that The Russian Federation has become a rogue state, and any normalization of relations after a peace deal or truce would create more opportunities for Russian subthreshold warfare. Second, a new effort must be made to strengthen alternative centers of power, knowledge, and science related to Russia. The Russian regime should be delegitimized through a common international effort. At the same time, the Russian armed opposition should be strengthened as the main alternative center of resistance to Putin's Russia.

The lack of pro-Ukrainian Russian-language media hinders the development of narratives that provide an alternative to those promoted by the Russian government. Weakening the Russian regime requires sustained efforts to delegitimize both its institutions and the narratives on which it relies.

Regime change in The Russian Federation is not possible without Russians. Poland, and especially the Baltic states, still have large Russian-speaking minorities that remain vulnerable to Russian propaganda. Support for an alternative Russian identity—peaceful, Ukraine-friendly, and pro-European—would distance these communities from the institutions and narratives of the Russian Federation and encourage their inclusion in a broader anti-Putin movement. The core of this resistance consists of Russian volunteers who are defending Ukraine with weapons in hand.

Toward a New Comprehensive Deterrence Strategy

The drone revolution in the Russian-Ukrainian war and the hybrid nature of contemporary threats have changed the rules of warfare, but these changes are being integrated into national defense doctrines and military strategy only slowly. A new deterrence strategy for NATO's eastern flank should include more than the East Shield project. Any construction of defensive lines against a possible Russian invasion should take into account the most recent developments in the Russian-Ukrainian war. In other words, Ukraine's real-time military experience is indispensable.

Moreover, credible deterrence and the development of hard power should go hand in hand with special measures in the field of soft power. These measures should include a specific focus on Russian studies, a continued commitment to the impossibility of cooperation with the Russian Federation until all consequences of Russia's invasion of Ukraine are paid for, and the strengthening of alternative poles of Russian identity in Europe, with a focus on the Russian armed opposition, which remains the only legitimate Russian opposition recognized by Ukraine. Only by combining hard- and soft-power measures suited to modern challenges can the European security architecture be normalized and given the potential for improvement.



*IVAN YUROV,
director at Russian Identity & Governance Research Initiative*



*PETRO BAKUMOV,
senior lecturer at Kyiv-Mohyla Academy*

SECTION 1. OVERVIEW OF THINK TANKS ANALYSES

NATO AND THE NEW EUROPEAN SECURITY ARCHITECTURE

The potential US withdrawal from NATO under American law

Michał Doliński, Polish Institute of International Affairs (PISM), Poland
10.07.2026

The author of the study analyzes how realistic a U.S. withdrawal from NATO would be from the perspective of U.S. law. In general, a U.S. withdrawal from NATO is legally possible under Article 13 of the North Atlantic Treaty, but in practice, implementing it would be complicated. In the case of the U.S., this immediately creates a procedural and constitutional paradox, since Washington is the party that holds the original treaty and would, in effect, have to send a notice of withdrawal to itself.

The main problem is that the U.S. Constitution clearly defines the procedure for concluding treaties but does not establish rules for their termination. That is why a unilateral withdrawal from NATO by the president would trigger a dispute between the White House, Congress, and the courts. Of particular importance is Section 1250A—a provision included in the U.S. defense budget for 2024. It prohibits the president from unilaterally terminating the North Atlantic Treaty or withdrawing from it without the consent of two-thirds of the Senate or a separate act of Congress.

These discussions were sparked by Donald Trump's repeated statements questioning the value of U.S. membership in NATO and his ideas for a sweeping reform of the Alliance.



However, overall, the short-term risk of a U.S. withdrawal from NATO remains low, though it cannot be completely ruled out due to Donald Trump's unpredictability. If the president attempts to act unilaterally, Congress would likely take the matter to court. In such a case, the courts could apply the approach articulated by the U.S. Supreme Court in the 1952 case *Youngstown Sheet & Tube Co. v. Sawyer*. In that case, the court ruled that President Harry Truman's decision to place steel mills under federal control without clear authorization from Congress was unlawful. At that time, Justice Robert Jackson proposed dividing presidential powers into three categories: the strongest—when the president acts with the express authorization of Congress; the intermediate—when Congress has not taken a clear position; and the weakest—when the president acts contrary to the expressly stated will of Congress. In the case of a unilateral withdrawal from NATO, the situation would likely fall into the third category, since the aforementioned Section 1250A prohibits the president from terminating a treaty without the consent of two-thirds of the Senate or a separate act of Congress. Therefore, a court could rule that such actions by the president are unlawful. Consequently, even a procedure that is formally one year in duration could turn into a protracted constitutional crisis.

The Ankara Summit: It's Trump's NATO – Europe just lives in it

Felix Koesterke, Egmont Institute, Belgium

15.07.2026

The NATO summit in Ankara formally gave Europe cause for relief, as the declaration reaffirmed the unwavering commitment to Article 5, identified Russia as a long-term threat to Euro-Atlantic security, and reaffirmed support for Ukraine, including financial assistance from European allies and Canada. This strengthened deterrence, as it demonstrated to Moscow that the Alliance is not in a state of open disintegration.

At the same time, the author emphasizes that this summit did not resolve the main problem—NATO's growing dependence on Donald Trump's political will. The entire meeting was, in fact, structured to avoid conflict with the U.S. president, while his statements regarding Iran, Greenland, and Spain confirmed that Washington remains deeply unpredictable. Therefore, Europe cannot afford to be strategically complacent.

The key conclusion is that the future European security strategy must not only reaffirm the importance of NATO but also define exactly how Europe will develop its own capacity to act in the security sphere. To this end, the strategy must outline European priorities, available instruments, and the role of the defense industry. At the same time, Europe needs to strike a balance between the “Made in NATO” approach—which allows for the rapid procurement of necessary equipment within the Alliance—and the “Buy European” principle, which entails the long-term strengthening of its own defense-industrial potential. In a broader sense, this concerns Europe's ability to act alongside the United States, on its own in the absence of American support, and, if necessary, even independently of Washington's position.



NATO's Eastern Flank Frontier

Center for the study of democracy, Bulgaria

30.06.2026



The study analyzes NATO's eastern flank as an active arena of hybrid confrontation, where Russia and a broader revisionist coalition—comprising China, Iran, and North Korea—constantly test the resilience of the Euro-Atlantic order. The southern segment of the flank—the Black Sea region—also remains vulnerable, where Bulgaria and Romania face risks of military escalation, energy coercion, cyberattacks, disinformation, and sanctions evasion via Russia's "shadow fleet."

Defending the eastern flank cannot be reduced to a mere military presence. Romania is actively strengthening its role as a NATO stronghold through base modernization, air defense acquisitions, and participation in the European SAFE joint defense procurement funding instrument, while Bulgaria is increasing its defense spending but is held back by political instability. The B9 format and cooperation among Bulgaria, Romania, and Turkey should serve as the foundation for better coordination in maritime security, energy resilience, and countering hybrid threats.

Special emphasis is placed on technological sovereignty. Europe is lagging behind in AI, semiconductors, and the full technology value chain, so it must combine the development of its own technological base, adaptive regulation, and the expansion of its computing capabilities. At the same time, attention is drawn to a new threat—LLM grooming—that is, the deliberate flooding of the open internet with distorted or manipulative content that can subsequently influence the responses of artificial intelligence systems. Overall, this reaffirms that Europe needs a comprehensive approach to security that combines the development of the defense industry and technologies, the strengthening of societal resilience, media literacy, and the application of Ukraine's real combat experience.

Legality and Reality: The Eastern Flank and the Ottawa Convention

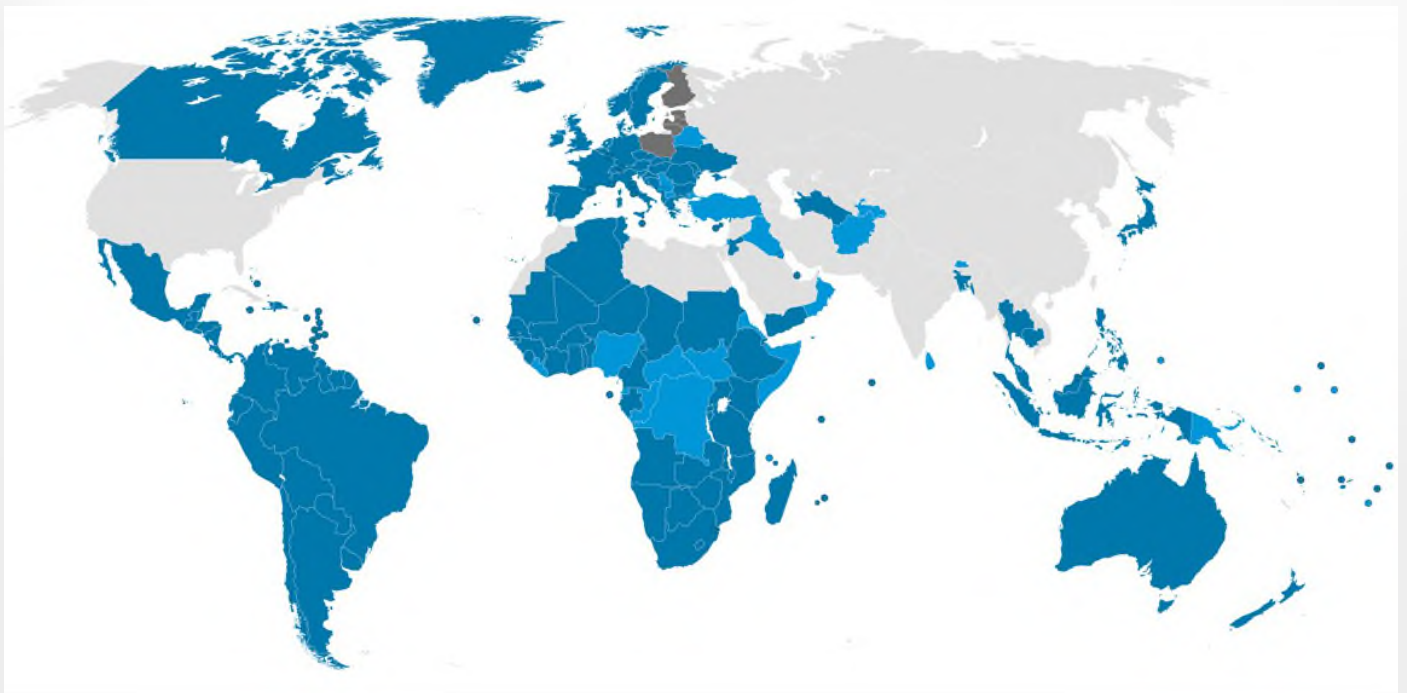
Théa Delval, Luca Rogers, International Centre for Defence and Security (ICDS), Estonia

15.06.2026

The authors analyze how Russia's war against Ukraine has reignited the debate in Europe over anti-personnel mines as an instrument of deterrence and defense. However, there is a dilemma: mines remain militarily effective, especially for the defending side, but their use poses serious humanitarian risks and legal constraints for states bound by the Ottawa Convention.

The Russia-Ukraine war serves as the central case study. Russia, drawing on the Soviet operational tradition, makes extensive use of minefields as part of a war of attrition. Ukraine has been forced to adapt and also employ mines, albeit more selectively and on a smaller scale. This has placed Kyiv in a complex legal situation: Ukraine remains a party to the Ottawa Convention, but due to the ongoing armed conflict, it cannot formally withdraw from it. Its attempt to suspend the application of the Convention on the grounds of a "fundamental change in circumstances" appears legally vulnerable.

It is precisely this Ukrainian precedent that explains the decision by the Baltic states, Finland, and Poland to withdraw from the Convention before they themselves might find themselves at war with Russia. For them, anti-personnel mines are viewed not as peacetime weapons, but as an element of potential defense, particularly within the framework of the Baltic Defense Line, the Eastern Shield, and the defense of the Suwałki Corridor. Mines can indeed strengthen deterrence and complicate Russian planning, but even after withdrawing from the Convention, states remain obligated to comply with international humanitarian law.



Status of States under the Convention on the Prohibition of Anti-Personnel Mines

Below: blue – signed and ratified; light blue – acceded; dark gray – withdrew from the Convention

When Old Certainties No Longer Hold: Nordic-Baltic Foreign Policy Adaptation

Kristi Raik, International Centre for Defence and Security (ICDS), Estonia
25.08.2026

The author analyzes the strategic dilemma facing the countries of Northern Europe and the Baltic states amid the simultaneous weakening of two key pillars of their security: the transatlantic alliance and the rules-based international order. Russia remains an existential threat to the region, while the United States remains its strongest ally. At the same time, Donald Trump's second administration has called into question Washington's traditional role as the guarantor of international law, allied solidarity, and the stability of the postwar order. The author emphasizes that the issue at hand is not about turning away from the U.S. or NATO, but rather about the need to adapt foreign policy to a situation in which Washington remains the most important ally but can no longer be viewed as the unconditional defender of international law and the postwar order.



Small states in the region are forced to balance security dependence with their own principles. They seek to uphold international law but avoid direct confrontation with the United States when American policy contradicts these norms. The examples of the Strait of Hormuz and Greenland are telling precisely because, in both cases, Estonia publicly demonstrates its willingness to support its ally but avoids directly assessing or criticizing U.S. actions. And this is precisely how the structural dilemma of small states manifests itself: they can affirm general principles such as the security of sea lanes, sovereignty, and the territorial integrity of Denmark, yet they lack sufficient political leeway to openly question U.S. policy.

Russia's war against Ukraine has shown that international law remains an essential foundation for supporting Kyiv and putting pressure on Moscow, but it does not, in and of itself, protect against aggression. Therefore, the North Baltic region must strengthen national, European, and regional defense, reinforce NATO, deepen cooperation with the United Kingdom, Germany, and Poland, and support Ukraine's integration into Europe as part of its own strategy for survival alongside Russia.

EUROPEAN DEFENSE AND STRATEGIC AUTONOMY

Strategic autonomy and Europe's new logic of intervention

Maria-Louise Clausen, Peter Albrecht, Danish Institute for international studies (DIIS), Denmark

09.06.2026

Russia's full-scale war against Ukraine has changed not only the scale but also the mechanisms of European intervention. Previously, the EU acted primarily through civilian instruments: supporting reforms, building state institutions, promoting the rule of law, and providing crisis management. Since 2022, these approaches have been supplemented by direct support for Ukraine's military capabilities, as the EU funds arms deliveries, training for Ukrainian military personnel, and joint procurement and production of weapons.



The authors attribute this shift to two factors. The first is the war itself, which forced European states to respond to a large-scale interstate conflict rather than a localized crisis. The second is uncertainty regarding the future role of the United States in European security. As a result, the EU's strategic autonomy is becoming increasingly relevant, as it is no longer just a matter of the ability to make decisions independently, but of the capacity to produce, procure, and supply weapons without critical dependence on external partners.

Ukraine's military experience is becoming a valuable resource for European defense policy. Ukrainian manufacturers can adapt weapons more quickly to the needs of the front lines, and Ukrainian military personnel possess practical knowledge of using drones, reconnaissance, electronic warfare systems, and other technologies in real combat conditions. Therefore, cooperation with Ukraine also gives the EU access to knowledge that cannot be obtained through ordinary peacetime procurement or training.

A good example is the Danish model. Ukraine identifies the weapons that its own industry can produce but cannot fully finance; Denmark and its partners channel external funds directly into contracts with Ukrainian manufacturers. One of the first examples of such cooperation was the 18 "Bogdan" howitzers, ordered in July 2024 and delivered to the front lines just two months later. In 2025, this model generated approximately \$1.8 billion for Ukrainian weapons production.

Thus, the European Union is becoming increasingly involved in the war economy and defense planning, but it does not yet have a fully coordinated system for joint production, procurement, and strategic decision-making. Ukraine has become a real-world test of European strategic autonomy. It demonstrates that the EU is capable of quickly creating new formats of support, but at the same time reveals its dependence on national governments, external funding, and U.S. security guarantees.

Not just an addendum: Making resilience a key pillar of Europe's defence

Nad'a Kovalčíková, Giuseppe Spatafora, European Union Institute for Security Studies (EUISS), EU-level think tank

06.07.2026

In this study, the authors analyze why civil preparedness and societal resilience should become a full-fledged pillar of European defense. Modern threats are increasingly blurring the line between the military and the civilian spheres. Sabotage, cyberattacks, information operations, economic coercion, drone incidents, and attacks on critical infrastructure directly impact Europe's ability to deter adversaries and respond to crises.

The starting point for such discussions is Ukraine's real-world experience, which has demonstrated that prepared citizens, local authorities, businesses, digital services, energy resilience, and crisis communication are not merely logistical elements but an integral part of defense capabilities. Europe is already moving in this direction through the European Preparedness Union Strategy, civil protection mechanisms, and cyber and infrastructure legislation, while NATO is increasingly viewing societal resilience as a prerequisite for effective deterrence. It is believed that if a state can quickly restore critical systems, support its population, counter disinformation, and continue to function during attacks, it becomes more difficult for an adversary to paralyze it and achieve its objectives.

However, the current system remains fragmented. There is a lack of common planning standards, clear criteria for measuring resilience, coordinated information sharing, and deeper civil-military integration. The Swedish "total defense" model and the Finnish "comprehensive security" model provide a framework, but cannot be mechanically applied to the entire EU.

The authors' main recommendation is to create a European mechanism that will identify society's vital functions, assess threats, coordinate capability development, and engage member states, EU institutions, local authorities, the private sector, and external partners, including Ukraine.



The FCAS Collapse and Europe's Enduring Coordination Problem

Tevian Thomson, International Centre for Defence and Security (ICDS), Estonia

22.06.2026

The author analyzes the failure of the Future Combat Air System program as a symptom of a deeper problem in European defense: a lack not only of resources, but also of the ability to subordinate national interests to a common strategic goal.

FCAS was intended to be the flagship of European defense integration—a joint project between France, Germany, and Spain to develop a sixth-generation fighter jet, with the participation of Dassault Aviation, Airbus, and Indra. Its significance lay not only in the aircraft itself but also in demonstrating that Europe's fragmented defense-industrial base is capable of jointly producing high-tech systems for future warfare.



The specific failure of FCAS stemmed from the partners' inability to agree on the basic terms for the division of responsibilities among the companies. The most acute dispute arose between France's Dassault Aviation and the German division of Airbus over the leading role in the fighter's development. Dassault insisted on the status of prime contractor and sought to retain control over key technologies, while Airbus demanded a more equitable distribution of work and access to intellectual property. As a result, the parties were unable for a long time to agree on the project's working structure, the allocation of technological areas, and decision-making rules.

Problems also arose regarding the distribution of industrial contracts among France, Germany, and Spain. Each country sought to guarantee its companies a significant share of the work, even if this did not always align with considerations of efficiency or expertise. As a result, the negotiations turned into a battle over national industrial interests. Different requirements for the future system became an additional source of tension: France focused more on strategic autonomy and the ability to use force independently, while Germany placed greater emphasis on the NATO framework, common standards, and political constraints.

For the countries on NATO's eastern flank, this is important not because they expected to receive such an aircraft, but because their security increasingly depends on Europe's ability to organize complex multinational defense projects. In conclusion, the author notes that FCAS does not prove that European defense integration is doomed, but it does show that money alone does not create military power. What is needed is trust, clear governance, political leadership, and a willingness to overcome industrial nationalism.

NATO's digital arsenal: How Europe can avoid a new dependence on America

Gustav Gressel, European Council on Foreign Relations (ECFR), EU-level think tank

29.07.2026

Modern armies are increasingly dependent on digital command-and-control systems, some of which have already been developed or are controlled by the United States. These systems help quickly collect, process, and transmit information between military units. While this can make joint operations among allies more effective, it also creates a new dependence on the United States for Europe. Following the NATO summit in Ankara, the allies agreed to develop drones, joint military information-sharing systems, artificial intelligence programs, and unified technical standards. However, the author emphasizes that whoever creates and controls the foundation of these systems effectively determines how armies will exchange data, update software, and use weapons.

Ukraine already has practical experience demonstrating how this can work. Its Delta system integrates data from various sensors, units, and types of weaponry into a single digital environment. Thanks to this, the military can more quickly coordinate artillery, drones, air defense, evacuations, and other operations. At the same time, the armies of European countries still use many systems that are incompatible with one another. Even the Link 16 standard, which is intended to facilitate data exchange among allies, no longer fully meets modern needs: it primarily transmits processed information about targets rather than raw data from sensors.

The U.S. Government Reference Architecture for drones could pose a separate problem. Although it is positioned as open and capable of working with various equipment, key decisions regarding its updates, certification, and portions of the source code remain under the control of the U.S. Air Force. Furthermore, U.S. ITAR regulations may restrict the export and use of European systems. A similar situation has already arisen with the Storm Shadow/SCALP missiles, when Ukraine's use of them depended on the political decisions of its partners.



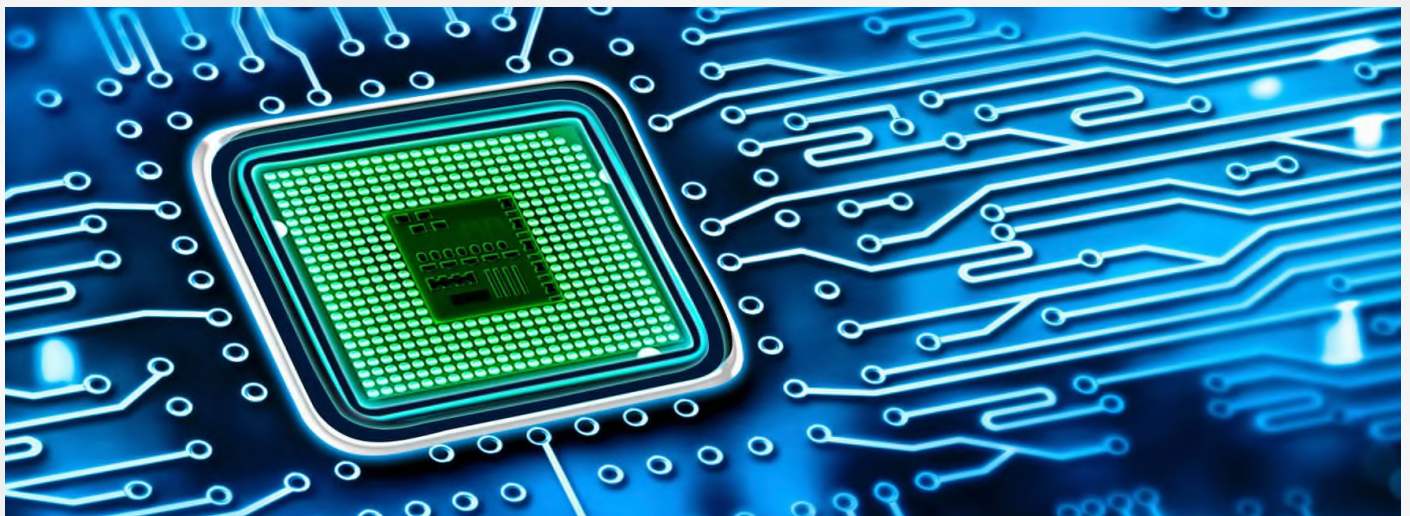
Therefore, in the author's view, NATO needs not just a joint system, but a truly open digital architecture with accessible code and independent international governance. If the U.S. does not agree to such an approach, Europe—together with Canada, Norway, the United Kingdom, and Ukraine—will have to develop its own system.

EU Defence Series: Europe's Tech Challenge

Pauline Le Grand, International Centre for Defence and Security (ICDS), Estonia

30.07.2026

The author analyzes why it is difficult for Europe to rapidly develop its own defense technologies. The wars in Ukraine and the Middle East have shown just how important drones, artificial intelligence systems, and satellite technologies have become. At the same time, Europe is struggling to keep up with these changes. The problem lies not only in a lack of funding. For many years, European countries have underinvested in defense, reduced their stockpiles of weapons, acted in a fragmented manner when making purchases, and failed to build sufficient production capacity to rapidly scale up the production of necessary equipment.



Attention is also drawn to two key dependencies of Europe. The first concerns China, which controls a significant portion of the market for critically important raw materials: it produces about 90% of the world's rare earth minerals and accounts for 98% of their imports into the EU. The second dependency relates to the United States, on which Europe relies heavily in areas such as missile defense, precision strikes, intelligence, and other advanced military technologies. This creates risks, especially if U.S. political priorities shift or restrictions arise regarding the supply of systems, their use, or access to software. The F-35 program is an example of such discussions.

The European Union is attempting to address these issues through a series of initiatives, including the Strategic Compass, the White Paper for European Defense – Readiness 2030, the EDF, EUDIS, PESCO, and EDIP. Particular attention is being paid to dual-use technologies, which can be used in both civilian and defense sectors. Among specific measures, the author mentions the JEWEL early warning project, €325 million for European Defense Projects of Common Interest, and €260 million for the Ukraine Support Instrument / BraveTechEU.

Therefore, Europe needs to act faster and invest more funds not only in the procurement of off-the-shelf weapons. It must develop its own research, support startups, scale up production, launch joint defense projects, and strengthen supply chains. Otherwise, Europe will continue to remain dependent on the U.S. and China for critically important technologies and resources.

Buzzkill: How to defend Europe against drones

*Ulrike Franke, European Council on Foreign Relations (ECFR),
EU-level think tank*

17.08.2026

The author describes two main drone threats to Europe. The first involves small drones that can be used for surveillance or attacks on critical infrastructure—airports, LNG terminals, military bases, nuclear power plants, and submarine bases. A telling example is the incident on August 5, 2026, at Leipzig Airport, where a small drone carrying explosives was discovered.

The second threat is military in nature. It involves drones crossing the airspace of countries on the eastern flank of the EU and NATO, particularly from Russia and Belarus. The most serious incident occurred in September 2025, when about 20 Russian drones entered Polish airspace. In response, NATO invoked Article 4 and launched Operation Eastern Sentry.

The current response system in Europe remains fragmented and excessively expensive. Drones can cost around 10,000 euros, while fighter jets or missiles costing millions are often used to intercept them. Therefore, Europe needs not just a single large-scale “drone wall,” but a multi-layered defense system. It should combine radars, passive sensors, optical and acoustic systems, electronic warfare capabilities, cyber-interception, kinetic countermeasures, and interceptor drones.

In addition, the author calls for the creation of a joint monitoring and response system along the entire eastern flank. The EU should support initiatives by Poland and the Baltic states, assist countries that do not yet have sufficient capabilities, and harmonize legal rules regarding the detection and interception of drones. Ukraine, which has long been fending off massive attacks, actively employs electronic warfare, and is constantly adapting its drone technologies, could serve as an important source of practical experience for Europe.



THE RUSSIAN-UKRAINIAN WAR

The Trap Closes: How Russia Suppresses Resistance in Occupied Ukraine and How We Can Still Help

Jade McGlynn, *International Centre for Defence and Security (ICDS), Estonia*
19.06.2026

The author analyzes how Russia maintains control over the occupied Ukrainian territories and why Western support should focus not on public demonstrations, but on the safety of people, the preservation of Ukrainian identity, and support for those living under occupation.



The Russian system combines repression, surveillance, information control, and Russification. Pre-prepared lists of activists, journalists, teachers, veterans, and volunteers are used for searches, abductions, and interrogations. More than 100 sites of illegal detention of civilians have been documented, and the number of detainees may reach at least 15,250. Ninety-two percent of former detainees surveyed reported torture or ill-treatment.

Control extends to everyday life: phones are checked, internet activity is monitored, SIM cards are linked to biometric data, and people are forced to obtain Russian passports. Without them, residents may lose access to healthcare, education, benefits, employment, and property.

Children are a separate issue. Nearly 20,000 Ukrainian children have been forcibly displaced to Russia or to territories under its control. They are being Russified, their contact with relatives is restricted, and Russian history is being imposed on them. In the occupied territories, children are also being drawn into militarized programs: for example, Voin trains teenagers in the use of weapons, tactics, and drones. In Mariupol, according to the study's estimates, approximately 63.8% of the education budget is allocated to ideological activities.

Under conditions of total surveillance, mass protests and public displays of symbols can lead to arrests, torture, and abductions. According to the author, more sustainable forms of resistance include preserving language and culture, sharing information, helping others, documenting crimes, and maintaining contact with Ukraine. Small, isolated groups, minimizing contact, and secure external coordination are crucial.

Therefore, Western support must be practical: assistance to IDPs, digital security, secure communications, support for independent lawyers, searching for the missing, humanitarian aid, and the safe documentation of crimes. The most important thing is to help people survive, preserve their Ukrainian identity, and continue their resistance without taking unnecessary risks.

Empowering Ukraine: Spend smarter, support harder

Ondrej Ditrych, Caspar Hobhouse, Nad'a Kovalčíková, Rossella Marangio, Tim Rühlig, Luigi Scazzieri, Giuseppe Spatafora, Bojana Zorić, European Union Institute for Security Studies (EUISS), EU-level think tank
20.07.2026

To strengthen Ukraine, it is not enough to simply increase support; it must be made more thoughtful, long-term, and coordinated among partners. As of early 2026, Ukraine is in a stronger position than before: its defense has become more stable, Ukrainian drones can now strike targets at distances of up to 3,000 km, and production of long-range drones increased by 53% between January and April 2026. At the same time, Russia is still capable of attacking civilian infrastructure, dragging out the war, and attempting to undermine the unity between Ukraine and Europe.



The authors propose several practical steps. First, they recommend more closely integrating the Ukrainian defense industry into the European system through joint ventures with EU companies. This should help Ukrainian manufacturers secure more investment, technology, production capacity, and access to European and NATO procurement markets. Second, they suggest paying special attention to the approximately five million Ukrainians currently living in the EU and viewing them as an important democratic community, especially ahead of the first post-war elections. Third, the proposal calls for gradually integrating Ukraine into European systems in areas such as energy, digital policy, transportation, standards, defense, and mobile communications—including through the “Roam Like at Home” initiative—even before Ukraine’s full accession to the EU.

A separate set of proposals concerns Ukraine’s reconstruction. These include creating a platform to attract investors based on DREAM, the “Big on Board” initiative to encourage more active private-sector participation, rebuilding the energy sector with an emphasis on distributed clean generation, and cautiously involving China in the reconstruction process through special safeguards. In addition, the authors propose creating a Peace and Prosperity Compact to improve coordination between the EU, the U.S., and the G7 countries, to build a network to counter Russian fraud schemes and recruitment efforts in Africa, and to capitalize on the current “pro-Ukrainian” momentum in Trump’s policy to locate the production of critically important American systems in Europe or Ukraine.

The Special Tribunal for Ukraine: Turning the Wheels of International Justice

Théa Delval, International Centre for Defence and Security (ICDS), Estonia
18.06.2026



The establishment of a Special Tribunal on the Crime of Aggression against Ukraine is intended to close a gap in international justice, as the International Criminal Court is currently unable to hold the Russian leadership accountable specifically for the aggression against Ukraine.

On May 15, 2026, in Chisinau, 34 Council of Europe member states, as well as Australia, Costa Rica, and the European Union, adopted a resolution establishing the Enlarged Partial Agreement. This agreement is intended to provide the administrative and financial framework for the future tribunal's operations.

The problem is that while Ukraine has recognized the ICC's jurisdiction over genocide, crimes against humanity, and war crimes since February 20, 2014, this does not extend to the crime of aggression. For the ICC to hear such cases, either the Kampala Amendment must be ratified or the situation must be referred by the UN Security Council. However, the second option is effectively blocked by Russia's veto power.

Therefore, a separate tribunal should serve as a special mechanism for prosecuting the highest political and military leadership responsible for initiating the aggression. Its work will be based on Ukraine's right to prosecute this crime, as well as on the provisions of the Rome Statute, UN General Assembly Resolution 3314, the practices of the Nuremberg and Tokyo tribunals, and the standards of the European Court of Human Rights.

At the same time, the author draws attention to important limitations. Trials in absentia should be conducted only in compliance with the defendant's right to a retrial. Furthermore, sitting heads of state and government, as well as foreign ministers, enjoy personal immunity, so it will be difficult to hold them accountable while they remain in office.

Thus, the establishment of the tribunal is an important step, but its success will depend on more than just the fact of its creation. To become a truly historic precedent, it must operate professionally, impartially, and with respect for the right to a fair trial.

Facing the North Korea–Russia alliance: EU–ROK strategies for deterrence and cooperation

Youngjun Kim, Elcano Royal Institute, Spain

24.07.2026

The author shows how North Korea's military support for Russia has influenced the course and scale of the war against Ukraine. Pyongyang is supplying Russia with large quantities of ammunition and has deployed thousands of troops. For the DPRK, this is the first large-scale military operation abroad since the Korean War. This move signals a departure from the traditional Juche policy, which emphasized maximum self-reliance and a cautious approach to dependence on China or Russia.

The author also emphasizes that the war in Ukraine has become a testing ground for new military cooperation among authoritarian states. China, Russia, and North Korea do not form a full-fledged ideological alliance, but they are united by a common pragmatic interest: to weaken the international order in which the United States plays a leading role.

If this cooperation continues to develop, it could extend beyond the current support for Russia. Possible future scenarios include joint military exercises involving China, Russia, and North Korea; access for Russian and Chinese ships to North Korean ports, particularly Wonsan; and coordination in the areas of nuclear deterrence, cyber operations, space technology, and information warfare. Command-and-staff exercises simulating potential strikes on targets such as Pyeongtaek, Okinawa, and Guam cannot be ruled out.

In the author's view, Europe and South Korea should respond simultaneously through deterrence and diplomacy. This involves regular multinational military exercises, enhancing military interoperability, exchanging military personnel, collaborating on cybersecurity and space technology, protecting critical infrastructure, and deepening defense-industrial cooperation between European countries and South Korea.



A Declining, but More Dangerous Power: Russia's Receding Reach in the Neighbourhood

Stefan Meister, International Centre for Defence and Security (ICDS), Estonia
29.06.2026

The study analyzes how Russia's war against Ukraine has accelerated Moscow's structural decline as a regional power. The full-scale invasion was intended to restore Russia's sphere of influence, but it had the opposite effect: Kazakhstan, Georgia, Moldova, Armenia, and the Central Asian states increasingly view Russia not as a guarantor of security, but as a risk from which they must distance themselves.

A key driver of this decline is the concentration of Russian resources on the Ukrainian front. Due to casualties and sanctions, Moscow has redeployed troops and weapons from Tajikistan, Armenia, Abkhazia, and South Ossetia, weakening its influence in neighboring regions. The most telling example is Nagorno-Karabakh: Russia had "peacekeepers" there after 2020, but did not prevent Azerbaijan from establishing control over the territory in 2023.

At the same time, sanctions have weakened the Kremlin's negotiating position. Russia needs new energy markets, routes to circumvent sanctions, and transit through Azerbaijan, Georgia, and Central Asia. This strengthens the agency of regional states: they are developing the Middle Corridor, coordinating policies among themselves, and engaging China, Turkey, the EU, the U.S., India, Iran, and Arab states. China stands to gain the most, as it takes over part of Russia's influence in trade, infrastructure, digital surveillance, and security.

Russian hegemony is coming to an end, but a weaker Russia does not become secure. It is losing its ability to dictate the order, yet it increasingly relies on force, disinformation, and coercion.



EU ENLARGEMENT AND UKRAINE IN EUROPE

The Future of EU Enlargement Policy: Four Scenarios for Enlargement in Wartime Europe

Katsiaryna Lozka, Jonas Althoff, Lavinia Klarhoefer, Maria Gargano, Maryna Yaroshevych, Egmont Institute, Belgium

02.07.2026

The authors examine four possible scenarios for the development of the EU's enlargement policy through 2029. Following Russia's full-scale invasion, enlargement has ceased to be merely a means of supporting democratic change in neighboring countries. Now it is also a matter of security for all of Europe. At the same time, the EU must strike a balance between the need to bring Ukraine, Moldova, and the countries of the Western Balkans closer to the European space more quickly and the necessity of adhering to its own rules: compliance with EU legislation, implementation of reforms, unanimous decision-making, budgetary constraints, and maintaining the Union's effectiveness.

Under a scenario of rapid expansion, Montenegro and, possibly, Albania could become full EU members. Ukraine and Moldova, meanwhile, could gain gradual access to certain parts of the single market and European security mechanisms, but without full rights to participate in the Union's political decision-making.

Under a more cautious scenario, the EU will continue to require candidates to consistently fulfill all conditions. Ukraine will be able to open new negotiation chapters, join the digital space, European energy networks, and defense industry support programs; however, full membership will be postponed.

Another option envisages different levels of participation in the EU. In this case, security would take priority: Ukraine and other candidates would be able to gradually join European defense cooperation, the single market, educational programs, energy projects, and the extraction of resources critical to industry. This would allow them to forge closer ties with the EU even before gaining full membership.

The worst-case scenario is a de facto freeze on enlargement. Populism, decision-blocking by individual states, economic difficulties, and slow reforms could halt the process. In that case, the EU would lose some of its influence, while Russia and China would gain more opportunities to strengthen their positions in the region.



The magnificent ten: A coalition of the willing to drive the EU's next enlargement

Engjellushe Morina, Gabrielė Valodskaitė, European Council on Foreign Relations (ECFR), EU-level think tank

23.07.2026

Ukraine's future membership will most likely be part of any peace settlement acceptable to Kyiv. However, the EU still lacks a concrete plan that would allow for the swift and secure integration of Ukraine, Moldova, and the countries of the Western Balkans.

The main proposal is to create a coalition of ten EU member states led by Germany. It would include Denmark, Germany, and Sweden, which consistently support enlargement provided the necessary requirements are met; Austria, France, Italy, and the Netherlands, which take a more cautious approach; as well as Lithuania and Poland, which view enlargement primarily as a security issue. Hungary is proposed to be considered separately—as a country that will potentially no longer be able to block this process.

The common basis for such a coalition should be the principle that each candidate country moves toward membership in accordance with its own progress in meeting the requirements. At the same time, the EU must provide safeguards, the ability to suspend certain stages of the process, control over migration risks, and limited access to European funds until full membership is achieved.

The authors consider Friedrich Merz's proposal for a special interim status for Ukraine to be the most promising. It would provide for Ukraine's participation in the work of the European Council, the European Commission, and the European Parliament without the right to vote. At the same time, full EU membership would remain the ultimate goal.

Over the next 18 months, the proposed coalition could develop this model, explain its benefits to European voters, and secure the support of EU leaders. In 2027, it could be tested in Albania, Moldova, Montenegro, and Ukraine.



Ukraine and the Next MFF: The Strive for Predictability

Luca Barana, Luca Cinciripini, Istituto Affari Internazionali (IAI), Italy
22.07.2026



The authors examine how the approach to funding Ukraine should change in the next long-term EU budget for 2028–2034. The main instrument should be a reserve for Ukraine, through which up to 100 billion euros could be mobilized under the “Global Europe” program, provided that accession requirements are met. The authors note that this amount is insufficient, as Ukraine’s reconstruction needs are estimated at more than 520 billion euros. At the same time, the reserve could serve as the foundation for a broader financing system.

The key point is that Ukraine’s reconstruction and its accession to the EU cannot be viewed as two separate processes. Funds must be simultaneously directed toward rebuilding destroyed infrastructure, implementing the reforms necessary for accession, and gradually aligning Ukraine with European standards in areas such as energy, digital technologies, transportation, and the defense industry. It is also important to improve the business environment to attract private investment.

The authors also emphasize the need to combine stability with flexibility. Ukraine and investors need clear, long-term guarantees, yet the course of the war and the extent of the destruction remain unpredictable. Therefore, the EU must coordinate among its members to provide grant aid, loans, guarantees, support from international financial institutions, and private investment.

Ultimately, Ukraine should be rebuilt not merely with the prospect of future EU accession in mind, but in accordance with the rules and standards of a future member state.

Escalating the Polish-Ukrainian dispute: Russia's operational objective in Poland

Filip Bryjka, Aleksandra Wójtowicz, Polish Institute of International Affairs (PISM), Poland

24.08.2026

Russia is actively exploiting Polish-Ukrainian tensions to weaken support for Ukraine. The authors emphasize that Moscow did not create the current crisis, but Russia stands to gain the most from its escalation. Its main goal is to weaken or destroy cooperation between Poland and Ukraine, complicate the transport of Western military aid through Polish territory, reduce support for Ukraine within Polish society, and exploit historical disputes to hinder Ukraine's European integration.



Russia has been employing this tactic since at least 2014. This includes anti-Ukrainian demonstrations, vandalism of UPA monuments, staged events designed to create the impression that the Polish minority is being persecuted in Ukraine, as well as attacks on Polish diplomatic missions. After 2022, claims about the alleged excessive influence of Ukrainians on the Polish economy and social sphere were added to this. Starting in 2023, Russia also began to resort more actively to sabotage and subversive activities.

One of the main propaganda narratives has been the so-called “Bandera Ukraine”—a state allegedly ruled by nationalists hostile to Poland. To spread this narrative, they use forged documents, selectively released archival materials from Russian intelligence agencies, and videos created using artificial intelligence. Such materials were disseminated, in particular, during the “Overload” disinformation campaign.

The scale of this campaign can already be measured. Between May 26 and July 13, 2026, the number of Polish-language posts containing overt anti-Ukrainian hate speech increased by 171%—to 364,000. The number of reactions to such posts rose by 345% and reached 1.2 million.

The authors warn that the disinformation campaign could escalate into physical provocations: property damage, attacks on Ukrainian facilities, false bomb threats, or provocations involving drones, which Russia will attempt to portray as actions by Ukraine.

ECONOMIC SECURITY, SANCTIONS, AND STRATEGIC DEPENDENCIES

Europe's energy security in 2026: More resilient, but systemically exposed

Izabela Surwillo, Julia Schwab, Danish Institute for international studies (DIIS), Denmark

19.08.2026

As of 2026, Europe is better prepared for energy shocks than it was in 2022. At the same time, it is still too early to speak of complete energy security. Dependence on Russian fossil fuels has decreased significantly, but new risks have emerged: Europe relies heavily on Norway for pipeline gas supplies, imports about 45% of its gas in liquefied form, and the United States has become its main supplier of liquefied natural gas. In addition, maritime routes, gas terminals, and global energy markets remain vulnerable.



The authors emphasize that diversifying suppliers does not mean complete independence. In 2024, the European Union still met 57% of its energy needs through imports. The transition to clean energy can enhance security but simultaneously increases the importance of power grids. The share of renewable sources in electricity generation rose from 38% in 2021 to 48% in 2024. However, due to grid capacity constraints, at least 120 GW of planned capacity may be connected with delays. By 2030, approximately 584 billion euros will be needed to develop the power grids.

Another challenge is European industry's dependence on China for the production of clean energy technologies. For example, the EU sources about 98% of its rare-earth magnets from China. Ukraine serves as an important case study for testing the resilience of the energy system. Russian attacks have shown that protecting the energy sector involves more than just air defense and cybersecurity. Equally important are stockpiles of transformers and other equipment, trained repair crews, rapid government procurement, reliable logistics, and the ability to quickly restore critical services.

The European Union faces “China Shock 2.0”

Justyna Szczudlik, Polish Institute of International Affairs (PISM), Poland
20.07.2026

The author analyzes the “China Shock 2.0”—a new wave of pressure from Chinese imports on the European Union. Unlike in the early 2000s, when China mainly exported low-cost, low-tech goods, it is now more actively selling high-value-added products: cars, electric buses, solar panels, wind power equipment, steel, ferroalloys, and chemical products. The author attributes this to a shift in China’s economic model following the pandemic and the 2023 real estate market crisis. In response, Beijing has stepped up state support for industry as part of the “Made in China 2025” strategy.



The scale of the problem can already be gauged by specific indicators. In 2025, the EU’s trade deficit with China reached 360 billion euros. Since 2015, imports from China have risen by 89%, while EU exports to China have increased by only 37%. That same year, the European Union imported more than 1.1 million new Chinese-made cars worth 15.1 billion euros. In addition, China supplied 98% of the solar panels and 61% of the inverters used in the EU. Online platforms such as Shein, Temu, and AliExpress are creating additional pressure: in 2024, the EU received 4.6 billion packages, mostly containing inexpensive goods costing up to 150 euros.

According to the author, the EU must more actively protect its market from unfair competition, particularly from goods whose production is supported by Chinese government subsidies. At the same time, a stronger industrial policy is needed, along with the development of domestic production, the search for more reliable suppliers, and a reduction in dependence on China. The European Union must also be prepared for possible restrictions from Beijing in response to such measures.

The main conclusion is that without a consistent industrial policy and diversification of supplies, the EU risks losing a significant portion of its industrial base.

Countering the use of crypto-assets to circumvent sanctions against Russia

Elżbieta Kaca, Polish Institute of International Affairs (PISM), Poland
17.07.2026

The study demonstrates how Russia uses cryptocurrencies to circumvent sanctions and create a parallel financial system with their help. Cryptocurrencies have not replaced traditional schemes involving banks, intermediaries, shell companies, and cash, but have supplemented them. They enable faster international payments, particularly when purchasing dual-use goods—such as drone parts, electronics, and other sensitive technologies.

According to TRM's estimates, in 2025, Russia accounted for the majority of approximately \$158 billion in cryptocurrency transactions related to sanctions evasion. The A7 network, the ruble-pegged cryptocurrency A7A5, and the Garantex and Grinex exchanges play a key role in this system. The A7 network, which is linked to Ilan Shor and the Russian defense bank Promsvyazbank, reported over \$90 billion in turnover in 2025. Exchanges and intermediaries in Kyrgyzstan, Georgia, and the United Arab Emirates are also involved in these schemes. They help exchange cryptocurrencies for local currencies.

Western countries are gradually shifting their approach to sanctions: instead of imposing restrictions on individual exchanges, they are increasingly attempting to shut down entire networks that include cryptocurrency issuers, brokers, banks, payment services, and other intermediaries. At the same time, Russia is adapting quickly. To conceal the origin of funds, they use anonymous cryptocurrencies, personal digital wallets, peer-to-peer exchanges, transaction mixing services, transfers between different blockchains, decentralized financial platforms, and services that allow users to exchange cash for cryptocurrency, such as Aifory Pro.

This is of direct relevance to Ukraine, as such financial channels help Russia purchase components for its military-industrial complex and sustain its ability to continue the war.



Strategic Corruption: The Nexus Between Russian Illicit Financial Flows and Offshore Finance

Martin Vladimirov, Dr. Tihomira Kostova, Marius Koeppen, Dr. Vanya Petrova, Center for the study of democracy, Bulgaria

28.07.2026

This study examines illicit financial flows from Russia as part of what is known as “strategic corruption.” It describes a system in which the state, big business, offshore companies, and opaque financial intermediaries work together to maintain the Kremlin’s influence. The authors demonstrate that following the start of the full-scale invasion of Ukraine, sanctions did not dismantle this system but instead forced it to become more extensive, covert, and flexible.

One of the study’s key findings is that the network of the 100 largest Russian companies has not shrunk but, on the contrary, has expanded. Between 2015 and 2025, the number of companies linked to it rose from 8,155 to 10,935, and the number of connections between owners and companies increased from 9,895 to 14,459. At the same time, direct Russian ownership in Europe decreased. Instead, the share of companies controlled through Cyprus, Luxembourg, the Netherlands, the United Kingdom, and the British Virgin Islands rose from 15.30% to 31.61%. This means that Russian capital is increasingly being concealed through complex chains of offshore companies.

New methods of money transfer—cryptocurrencies, gold-backed payments, and the A7A5 stablecoin—play a key role in this system. The associated A7 network has reported conducting transactions totaling over \$90 billion outside the SWIFT international system. This is of direct relevance to Ukraine, as such channels enable Russia to sell its resources, pay for imports, purchase dual-use goods, and support its military-industrial complex.

Thus, sanctions should not be directed solely against individual companies. The entire network must be monitored: ultimate owners, shell companies, banks, lawyers, cryptocurrency exchanges, payment services, and intermediaries in third countries.



The results and limits of European states' interventions against the Russian shadow fleet

Elżbieta Kaca, Polish Institute of International Affairs (PISM), Poland
25.08.2026



The author analyzes how effective European countries' actions against the Russian shadow fleet are and what limitations they face.

The shadow fleet remains one of the main ways to circumvent sanctions. At the same time, it poses a threat to the environment, the safety of shipping, and critical maritime infrastructure. Starting in 2025, the countries of Northern Europe and the Baltic region have stepped up their efforts to combat vessels that lack genuine state registration or sail under a false flag. The European Union has also expanded the powers of its maritime missions so that they can inspect suspicious vessels.

The first results are already evident. Under pressure from the G7 countries, Panama, Barbados, and Cameroon have begun removing sanctioned tankers from their registries. As a result, the number of vessels without confirmed nationality has risen from 15 in December 2024 to 138 in July 2025. Between December 2024 and August 2026, European countries and the EU's "Irin" naval operation inspected or attempted to inspect suspicious vessels 18 times. The most common reason was doubt regarding the authenticity of their flags.

Russia, however, is adapting to the new conditions. Its tankers are attempting to bypass the British exclusive economic zone, increasingly using the Arctic route or sailing around Africa. Some vessels are replacing false flags with formally valid ones, and a growing number of tankers are being escorted by Russian military ships or aircraft.

In the author's view, a complete military blockade of such a fleet is unrealistic and too risky. Instead, joint inspections, the detention of suspicious vessels, constant surveillance, and the establishment of a separate EU naval operation could significantly complicate the circumvention of sanctions and make it considerably more expensive for Russia.

THE TRANSFORMATION OF THE WEST AND EUROPEAN POLITICAL AGENCY

France and Germany: Overcoming Differences to Strengthen European Sovereignty

(fr. France-Allemagne : dépasser les différends pour renforcer la souveraineté européenne)

Paul Maurice, Institut français des relations internationales (IFRI), France
15.07.2026

The author explains why the Franco-German partnership remains important for the EU, but cannot be sustained solely by symbolic statements and its traditional role as the “engine of Europe.” After Friedrich Merz took office in 2025, the attempt to revive cooperation yielded only partial results. Paris and Berlin still hold differing views on defense, industrial policy, energy, relations with the U.S., the agreement with Mercosur, and the use of frozen Russian assets.

The main point of contention concerns the nature of European autonomy. Since the start of Russia’s full-scale war against Ukraine, Germany has significantly increased its defense spending, revised budget constraints, and sought to build the strongest conventional army in Europe. At the same time, Berlin continues to view NATO as the foundation of European security. France, however, insists that Europe must have greater freedom in making political and military decisions and be less dependent on the United States.



The failure of the joint fighter jet development under the FCAS/SCAF program in June 2026 demonstrated that large-scale defense projects cannot succeed without prior agreement on strategic goals, the division of responsibilities, and industrial interests. The next test for the two countries will be the program to develop the new main battle tank (MGCS), which is being carried out by KNDS.

Despite the disagreements, opportunities for cooperation remain. These include consultations on nuclear deterrence following Emmanuel Macron’s speech on March 2, 2026, the joint development of air defense, early warning systems, and long-range weapons, as well as cooperation in space, artificial intelligence, cybersecurity, high-performance computing, semiconductor manufacturing, and dual-use technologies.

The author proposes transforming the French-German Council of Foreign and Defense Ministers into a practical tool for coordinating specific projects. In his view, Paris and Berlin should focus less on declarations and more on joint initiatives with clear objectives, responsible parties, and deadlines. Such initiatives should address EU enlargement, majority voting, the formulation of the Union’s budget for 2028–2034, as well as support for Ukraine, Moldova, and the Western Balkan countries.

The tragedy of “Westalgia”

*Mark Leonard, European Council on Foreign Relations (ECFR),
EU-level think tank
15.07.2026*

The author criticizes the European elites’ nostalgia for the old model of relations between Europe and the U.S., under which Washington automatically guaranteed the security of European countries.

The author analyzes the NATO summit in Ankara. European leaders were relieved that Donald Trump did not announce the U.S. withdrawal from the Alliance or the withdrawal of American troops, spoke positively about Volodymyr Zelenskyy, and promised to grant Ukraine permission to manufacture Patriot missiles. However, according to the author, the very fact that the summit largely boiled down to attempts not to upset Trump is evidence of Europe’s strategic weakness.

NATO’s goal of allocating 5% of GDP to defense and related needs is more of a political gesture to appease Washington than the result of a serious assessment of actual needs. This “Westalgia” manifests itself in three ways: a reluctance to acknowledge that the U.S. has changed fundamentally and may continue to reduce its presence in Europe even after 2029; a habit of relying on American aid without taking on sufficient responsibility; and Europe’s loss of the ability to independently determine its own policy in the face of Trump, Putin, and Xi Jinping.

The author’s main conclusion is that Europe needs not a token display of loyalty to the U.S., but an honest assessment of its own capabilities. European countries must understand whether they are capable of waging a large-scale war on their own and direct their defense spending toward addressing specific vulnerabilities, rather than simply following political guidelines.



Europe in an Age of America First Economics

Houston Wilson, Istituto Affari Internazionali (IAI), Italy
03.08.2026

This study analyzes how the economic nationalism of the U.S. Republican Party and Donald Trump's "America First" policy pose a serious challenge to the European Union. This goes beyond individual trade disputes and reflects a broader shift in U.S. industrial policy. Washington is increasingly using tariffs, government subsidies, requirements to purchase American goods, and measures to bring manufacturing back to the country to protect strategic industries and attract new investment.

Tariffs are having the most immediate impact on the EU. Starting in 2025, most European goods on the U.S. market will be subject to a general tariff of 15%. For steel, aluminum, and most copper products, the rate reaches 50%. As early as the first quarter of 2026, EU exports to the U.S. were 30% lower than in the same period the previous year. At the same time, the EU's trade surplus with the U.S. shrank from 80 to 34 billion euros.

In the long term, U.S. subsidies and requirements to manufacture goods domestically could become an even greater problem. After the Biden administration passed the Inflation Reduction Act, some incentives for clean energy were revised; however, the Trump administration maintained its course of supporting U.S. manufacturing in sectors such as semiconductors and advanced technologies. As a result, investments and jobs may shift from Europe to the U.S.

At the same time, the author points out a certain contradiction. The U.S. and the EU share common concerns regarding China, semiconductors, critical minerals, energy, and the reliability of supply chains. However, their industrial policies are increasingly becoming competitive. According to the author, Europe must protect its own industry, diversify its sources of supply, and strengthen the single European market. At the same time, it is important to prevent competition between the EU and the U.S. from escalating into a full-scale trade war.



If Marine Le Pen wins: A European guide to a far-right France

Célia Belin, Jeremy Cliffe, Camille Lons, Constance Victor, European Council on Foreign Relations (ECFR), EU-level think tank

04.08.2026

The authors of this study examine what a victory by Marine Le Pen in the 2027 French presidential election might mean for the European Union and European foreign policy. While it is not yet a foregone conclusion that she will win, the authors emphasize that the National Rally's rise to power would pose a far more serious challenge to Europe than the victory of right-wing populists in smaller countries. France possesses nuclear weapons, is a permanent member of the UN Security Council, and plays a key role in the Franco-German partnership, which is traditionally considered the driving force behind the EU.

The authors' main conclusion is that "National Rally" remains first and foremost Marine Le Pen's project, even despite Jordan Bardella's popularity. Bardella takes a more moderate stance on Ukraine and European cooperation, but if the party were to win, it would be Le Pen who would determine its political course. Her party seeks to weaken the influence of the European Commission, prevent the expansion of majority-voting decision-making, reduce France's contribution to the EU budget, and rejects the idea of joint borrowing. She also opposes European green policies and is skeptical of NATO.

For Ukraine, the greatest danger would not necessarily lie in an immediate severing of relations with France, but in the unpredictability of its policies. Paris could block new European decisions, criticize sanctions against Russia and military aid to Ukraine, and resist further EU expansion. The authors note that Ukraine's accession is of particular concern to the "National Rally" due to the potential consequences for French agriculture, additional costs to the EU budget, and fears of further centralization within the European Union.

Therefore, the authors advise Europe not to panic but to prepare in advance for such a scenario: it would be best to study the positions and capabilities of the "National Rally," maintain limited channels of dialogue with the party, and, if France blocks joint decisions, form separate coalitions of states willing to act together. These could include Germany, Poland, Italy, Spain, the United Kingdom, and European institutions.



SECTION 2. INSIGHT LAB ANALYTICAL MATERIALS

EEYES Insight Lab – a youth-oriented think tank of the International Charitable Foundation «UDoNation» / Eastern European Youth Empowerment Space (EEYES). The center conducts research in the fields of international and domestic politics, economics, and security, and engages financial expertise as needed. The priority of Insight Lab's activities is to ensure high quality standards for its analytical products.

Research within Insight Lab is implemented both on the team's initiative and at the request of partners; it may be intended for either public or restricted distribution. The current geographical focus covers Germany, Poland, and France, with the prospect of further expansion to the European region as a whole. At the same time, Insight Lab functions as a platform for professional dialogue, exchange of expertise, and development of modern research approaches.

An important area of the center's work is the internship program for young researchers. Insight Lab systematically invests in the development of a new generation of analysts, creating conditions for the acquisition of practical skills, professional growth, and the public presentation of their work results. The materials presented in this magazine were prepared by Insight Lab interns within the framework of the internship program under the supervision of the center's team.

A Russian drone on the territory of NATO member states: what does it mean?

Oleksandra Popovych

The use of unmanned aerial vehicles by Russian forces with their subsequent entry into the airspace of NATO member states has become one of the proofs of escalating aggression in relations between Russia and the Alliance. It is worth noting, however, that while at the beginning of the full-scale invasion most such cases were viewed as isolated incidents, as of 2026, a shift in their nature can be observed: they are increasingly accompanied by material damage and pose a direct threat to the civilian population and critical infrastructure.

Russia's practice of utilizing tools for power projection and hybrid influence is not a new factor in its long-standing relations with the security bloc. Nevertheless, unlike traditional methods: large-scale military exercises near the Alliance's borders (notably the «Zapad» exercise series), unsafe military aviation maneuvers, displays of naval presence in the Baltic and Black Seas and cyberattacks – incidents involving unmanned aerial vehicles are characterized by the direct violation of the airspace of NATO member states.

All of the aforementioned traditional tools of Russian pressure on the Alliance can largely be classified as «gray zone» activities, as they have remained below the threshold of open military conflict between Russia and NATO. That is why, given the increasing number of incidents involving drones, the question arises as to whether they are an accidental consequence of hostilities on the territory of Ukraine, or if they signify an evolution of the Russian model of engagement with NATO aimed at probing the boundaries of the Alliance's response. The assessment of risks to European security, the development of effective deterrence mechanisms and the forecasting of the future dynamics of relations between the parties depend on the answer to this question.

What is this: an accident, a provocation, or a test of response?

Approaching the analysis and a specific answer to the research question, it is worth understanding that reliably determining the nature of each individual incident is rather difficult due to the limited availability of information and the complexity of analyzing the Russian side's intentions. However, to subjectively determine the potential tactics behind the use of drones, it is advisable to apply the same criteria for comparing and evaluating each case. Thus, it is worth starting with the identification of possible characteristics for conducting this research.

In my view, relevant criteria include proximity to the border with Ukraine, as this makes it possible to understand whether the aerial object could have entered the territory of NATO countries as a result of deviating from its course during an attack on Ukraine. The next criterion is the recurrence and frequency of such incidents. An isolated occurrence and the absence of a consistent pattern of attacks may indicate their sporadic and accidental nature, whereas the systematic recurrence of such cases requires a different explanation. An equally important role is played by the indicator of damage inflicted on material assets, structures and individuals, as it allows for tracking and approximately determining the probable objective of the drone's flight. However, one of the most critical factors is an understanding of the context in which the attacks were carried out and the subsequent reaction of both sides to such incidents; it is precisely this that allows for a more substantiated assessment of the potential deliberate nature of these actions.

Is it possible to view incidents of Russian drones entering NATO territory as accidental? In fact, this is quite a complex question that may yield different answers depending on the period under consideration. However, in the context of the events that have taken place as of August 2026, it is rather difficult to characterize all such incidents as accidental.

First and foremost, considering the criterion of distance, in many cases, concluding that the incidents occurred in relative proximity to the territory of Ukraine is logical. In particular, Romania recorded the highest number of such incidents among the allies; due to its immediate proximity to Odesa region, it repeatedly experienced Russian drones entering its territory from the Black Sea waters. A similar pattern is also observed to a certain extent regarding Poland and the Baltic states. Such geographical proximity serves as an argument in favor of the accident hypothesis, as drones used to strike Ukrainian targets near the border can potentially deviate from their planned route or cross the border as a result of the operation of air defense and electronic warfare systems.

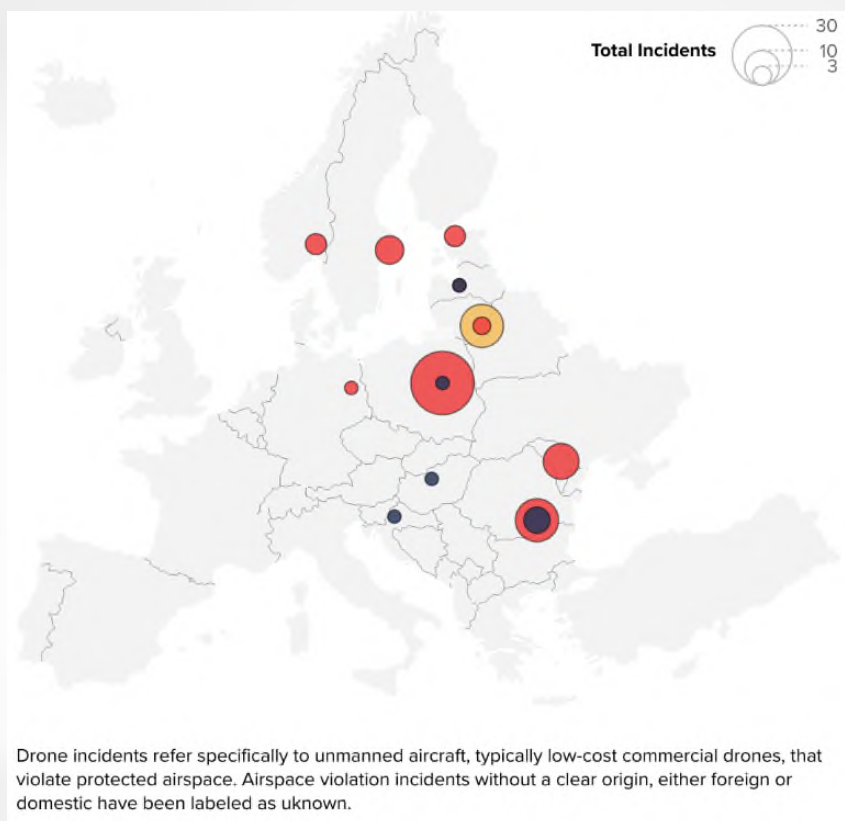


Photo from source №4

At the same time, the geographical criterion cannot fully account for the entire set of incidents. The expansion of the geography of cases beyond the immediate border area of Ukraine weakens the argument that all violations of NATO airspace are merely the result of drones accidentally deviating from their original target. Particularly important in this context is the emergence of cases in states located at a considerable distance from the Ukrainian border. In itself, this factor is not direct evidence of deliberate intent; however, it complicates explaining all incidents exclusively by chance and necessitates taking other criteria into account. Nevertheless, taking into consideration the appearance of Russian aircraft near military facilities on the territory of NATO countries, particularly in Belgium and the Netherlands, and their great distance from Ukrainian borders, the thesis of accidental entry requires additional substantiation. The appearance of an «unknown» unmanned aerial vehicle near military or critical infrastructure facilities does not in itself prove a reconnaissance purpose, but it may indicate potential interest in specific sites and reinforces the argument in favor of the deliberate nature of such actions. Thus, the theory of coincidence is not viable when applying this criterion.

The next criterion for assessing the accident hypothesis is the frequency of attacks. Here, one can observe a significant increase in the number of incidents compared to 2022, when such cases were predominantly isolated. In subsequent years, by contrast, an upward trend can be traced in the number of instances where Russian unmanned aerial vehicles were present on the territory or within the airspace of NATO member states. According to approximate calculations by the author of the article based on open-source data, it can be stated that more than 55% of cases across the entire period occurred specifically in 2025. Such a concentration of incidents within a single year indicates not only an increase in their frequency, but also a shift in the scale of the problem. Consequently, it is increasingly difficult to explain the recurrence of such cases solely as an aggregate of individual accidental deviations. When examining this criterion, attention should also be paid to the number of drones deployed during a single incident. The appearance of approximately 20 unmanned aerial vehicles in Polish airspace on September 9–10, 2025, substantially weakens the accident hypothesis, as this no longer concerns an isolated deviation of a single aircraft, but a large-scale penetration by a significant number of UAVs. According to assessments by the Institute for the Study of War (ISW), this operation may have been prepared by Russia months in advance, further casting doubt on its accidental nature. Particular attention should be paid to the use of decoy drones, notably «Gerbera,» which could have been deployed to saturate the airspace with additional targets and complicate the operation of air defense systems. Thus, the scale, preparedness and diversity of the UAVs employed may indicate not only the provocative nature of the incident, but also the potential testing of NATO's capability and response to a mass drone penetration.

Examining the next indicator (the level of inflicted damage) is fairly subjective, yet simultaneously appropriate to utilize. It is worth tracing the trend toward an increase in the potential danger of such incidents. When examining cases in 2022 and 2023, a significant portion of them were transit-like in nature or ended with the crash of debris without directly impacting civilian objects. Subsequently, however, instances have been recorded involving drone crashes, crater formation, structural damage and direct strikes on civilian infrastructure, as well as indirect damage, notably stemming from the presence of strike or reconnaissance UAVs near critical and military infrastructure of NATO member states. Thus, the occurrence of direct strikes on civilian infrastructure and the infliction of harm on the civilian population, as occurred in Romania on May 29, 2026, serves as an important argument for assessing the nature of such incidents. In this case, a Russian drone entered Romanian airspace and struck a residential building, injuring civilians as a result. Consequently, the trend toward an increasing level of damage to property and the population of NATO member states weakens the explanation of such incidents solely as accidental consequences of hostilities and, in conjunction with other criteria, may point to the growing deliberateness of such actions.

Undoubtedly, examining all criteria comprehensively is essential to confirm or refute the hypothesis, yet analyzing this issue in a vacuum is impossible. When analyzing the accidental nature of the incidents, attention should be paid to one of the key criteria – the reaction of the parties and the context of events in Ukraine and globally. It is precisely the sequence of events that allows for an understanding of whether the incidents remain isolated occurrences or gradually influence the behavior and policy of both sides.

Accordingly, at least three illustrative periods of reaction can be distinguished. The first is the second half of 2023, when, following a series of Russian UAV crashes on the territory of border Romanian villages, the Alliance reinforced its presence in the region, in particular by deploying additional air surveillance assets and fighter aircraft. These events unfolded against the backdrop of an escalating situation in the Black Sea region after Russia terminated its participation in the Black Sea Grain Initiative and intensified Russian attacks on Ukrainian ports. Thus, even at this stage, UAV incidents

began to be viewed not merely as a local problem, but in the broader context of security along NATO's eastern flank.

The next illustrative stage is the year 2025. On September 10, numerous Russian drones violated Polish airspace, after which Poland invoked Article 4 of the Washington Treaty to request consultations within NATO. In response, NATO activated additional air defense and surveillance assets and on September 12 announced the launch of the «Eastern Sentry» program, aimed at bolstering the defense of the eastern flank. NATO itself underscored that the September 10 incident was not an isolated occurrence and that the frequency of dangerous Russian actions in the airspace along the eastern flank is increasing.

Another illustrative period is late spring–early summer 2026. It is particularly significant not only for refuting the accident hypothesis, but also for assessing the evolution of NATO member states' responses, especially at the national level. It was on May 29, 2026, that a Russian drone struck a residential building in Romania, causing damage to civilian infrastructure and injuring civilians. This case already differs substantially in the nature of its consequences from earlier incidents, as the violation of airspace was accompanied by a direct strike on a civilian object, demonstrating the practical necessity of the legislative amendments adopted in February 2025, which expanded Romania's powers to respond to UAVs, in particular by permitting their direct destruction under legally defined conditions.

However, it is impossible to perceive the situation solely through the reaction of one side; therefore, attention should also be paid to the Russian side. While at initial stages one could observe denials or refutations of the facts surrounding drone incidents, subsequently the Russian side increasingly responded to NATO's reinforcement by accusing the Alliance of escalation and entanglement in the war. Such a shift in rhetoric is also meaningful, as it demonstrates that Russia perceives NATO's response not merely as a technical reaction to individual incidents, but as part of a broader standoff.

What lies ahead in Russia–NATO relations?

Thus, it is entirely logical to assume that the accident hypothesis as a universal explanation is insufficient. Individual cases may indeed be the result of drones deviating from their course, the operation of electronic warfare systems, or other unforeseen factors. However, by turning attention to the evolution of the response of both the Alliance and the Russian Federation and tracing their interaction, a trend toward changing patterns of behavior can be observed. At the same time, refuting one hypothesis does not automatically confirm another. Therefore, while discarding the accident theory as a universal explanation due to insufficient evidence in its favor, it is worth examining why the hypothesis of a provocation or a test of response is more plausible. A cumulative analysis of all criteria allows us not only to speak of the provocative nature of individual actions, but also to hypothesize the presence of a specific strategic objective behind them. In particular, taking into account the context of the incidents, the Alliance's reaction, and the subsequent change in the nature of the Russian Federation's actions provides grounds to assume that such cases may be used to test the boundaries of what is permissible and assess potential NATO responses.

Consequently, the most probable scenario for Russia's future behavior may be the continuation of provocative actions with the gradual testing of various options for the Alliance's reaction, which could potentially be accompanied by a further increase in the level of escalation.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*

From Shahed to joint production: what Russia and Iran have learned from each other

Yaryna Vasylyk

Introduction

Since 2022, Russian-Iranian cooperation in unmanned systems has evolved from the supply of ready-made Shahed drones to localized production and the mutual exchange of technology and combat experience. After acquiring the Iranian platform, Russia scaled up its production, modified it based on lessons learned from the war against Ukraine, and by 2026 began transferring some of the improved solutions back to Iran. This transformed the initial “supplier–recipient” model into a two-way cycle of military-technological learning.

Initial Model of Cooperation

The Shahed-136 is an Iranian-developed long-range one-way attack unmanned aerial vehicle (UAV) designed to strike ground targets. Its relatively simple design, long range, and low cost make it possible to deploy such systems in large numbers.

Russian Shahed drones are based on the Iranian design, and Russia initially acquired them through direct purchases from Iran in the autumn of 2022. In early 2023, Iran delivered approximately 600 drones in disassembled form for assembly in Russia, after which their production was localized.

Russia quickly integrated Iranian UAVs into its war against Ukraine, using relatively inexpensive attack drones to strike cities and infrastructure. Large-scale launches placed an asymmetric burden on Ukrainian air defense, forcing it to expend limited resources on interception.

However, cooperation quickly moved beyond the export of finished weapons. Iran supplied Russia with components and related technologies. According to the U.S. Department of the Treasury, Iran’s Ministry of Defense and Armed Forces Logistics cooperated with Russia on financing and producing Iranian-designed attack UAVs at Alabuga (a special economic zone housing production facilities for Shahed/Geran attack UAVs) under a \$1.75 billion contract. In late 2022, Russian officials also held negotiations with Sahara Thunder, a company subordinate to Iran’s Ministry of Defense and Armed Forces Logistics and responsible for commercial activities. The negotiations concerned the supply and production of thousands of UAVs per year at Alabuga.

Localization became the next stage. Russia established production at Alabuga of its own version of the Shahed-136 - the Geran-2 - with plans to gradually localize most Geran-2 production in Russia.

The Russian Adaptation Phase

Localizing production facilities did not mean simply copying the Shahed-136. Over the course of the war, Russia gradually modified both the drones’ design and the tactics for their use in response to Ukrainian countermeasures. One area of modernization was the navigation system. Russian Geran-2 drones were equipped with Kometa modules, which had already been used in other Russian UAVs and made it possible to simplify the navigation system’s internal electronics. The design also changed: instead of the lightweight honeycomb material characteristic of Iranian Shaheds, examined Russian models used fiberglass and layers of carbon fiber.

The tactics of their use also evolved. Russia began combining Geran attack drones with cheaper decoy UAVs and other means of aerial attack, creating mixed strike waves designed to complicate Ukrainian air defense operations and make them more costly. At the same time, Moscow expanded its production and launch capacity: between September 2024 and March 2025, the number of Shahed launches increased from approximately 200 to more than 1,000 per week.

Reversal of the Direction of Technology Transfer

By 2026, some of the developments Russia had made while adapting the Shahed began moving in the opposite direction. One of the clearest examples was the transfer to Iran of the Kometa-M satellite navigation system, which improves the accuracy of Shahed-136 drones and increases their resistance to jamming.

The exchange is not limited to technical components. In testimony before the Commission on Security and Cooperation in Europe in April 2026, Aaron Zelin, a senior fellow at the Washington Institute, stated that Moscow had supplied Tehran with components for modifying Shahed drones and shared its experience of using UAVs against Ukraine. In particular, this included recommendations on conducting coordinated attacks using multiple drones simultaneously. Thus, the reverse transfer encompasses not only technologies but also tactical practices tested by Russia in its war against Ukraine.

Another level of cooperation has involved the exchange of intelligence for targeting strikes. According to The Washington Post, Russia provided Iran with information on the locations of U.S. military assets in the Middle East, including ships and aircraft. This expands cooperation beyond technological and tactical transfers to intelligence support for combat operations.

Limits of Mutual Learning

Russia's experience of using Shahed drones cannot be fully transferred to a different operational environment. Analysis of Russia's campaign against Ukraine shows that the way missiles and drones are employed depends, among other factors, on the location and value of the target and the range of the strike. Relatively inexpensive Shahed drones allow Russia to increase the scale, frequency, and geographical reach of its strike campaign.

Variation in the choice of strike systems can also be observed in Iran's campaign in the Persian Gulf. According to an assessment by the Center for Strategic and International Studies (CSIS), drone attacks predominated against the UAE and Saudi Arabia, while the balance between drones and missiles differed for other targets. This distribution indicates that the composition of strikes is adapted to specific targets: drones were used to exert sustained and relatively inexpensive pressure, while missiles were employed where speed, reliability of the strike, or signaling in relation to military targets was a priority.

Thus, Russia and Iran can adopt each other's technologies and tactical experience, but the specific ways in which they employ them depend on their objectives and operational environments. What they share is not a specific template for conducting strikes, but rather the principle of adapting available capabilities to the conditions of a particular campaign.

Conclusions

Russia and Iran are not merely expanding Shahed production; they are also adapting the technology and the ways in which it is employed to their own needs. Russia transformed the platform it received from Iran into a scalable production system and adapted both its design and tactics to the war against Ukraine. Iran, in turn, is acquiring Russian technological modifications and experience from their combat use. At the same time, specific Russian tactics cannot automatically be transferred to the Middle East: their application depends on the objectives and operational environment. For Ukraine, this means the need to systematically share data with partners on Shahed/Geran modifications and tactics of their use, as well as to coordinate sanctions and export controls targeting shared component supply chains.

If the current model of cooperation persists, Russian-Iranian exchanges are likely to increasingly resemble a cycle of mutual adaptation: solutions tested by one side under combat conditions will be further developed and integrated by the other. For Ukraine, this creates the risk that modified Shahed drones could reappear on the battlefield after being further refined based on lessons learned from their use in the Middle East.

*This article was written for the magazine “Think Tanks Essentials”.
Views expressed in the article are those of the author.*

Sabotage as a Tool of Foreign Policy: How Is Russia Testing the Limits of the West's Response?

Kateryna Kot

Russia and its allies have been repeatedly accused of organizing attacks and other incidents across Europe since the invasion of Ukraine. Moscow's objective in these cases is identified as undermining support for Ukraine, attempting to sow fear, divide European societies, and expose vulnerabilities in the continent's security system.

The impact of sabotage lies primarily in creating preconditions for the application of force: such a reduction in efficiency provides time, space, and more favorable conditions for the effective action of other means. This role particularly highlights why technological changes are unlikely to alter the core characteristics of sabotage and its ongoing role in global politics. Following the start of the full-scale invasion of Ukraine in 2022, the Russian Federation deployed a full spectrum of confirmed sabotage tactics against Western countries: regular airspace violations in Romania, Poland, and Estonia by Russian drones and missiles, large-scale cyberattacks on critical and governmental infrastructure, arson attacks on military and logistical facilities, damage to subsea communications in the Baltic Sea, and the artificial creation of migration crises on the EU's eastern borders.

The post-Cold War era has undoubtedly witnessed extraordinary shifts in information technology; however, recent events indicate that sabotaging these technologies through cyberspace often carries less impact than old-fashioned kinetic actions. The fact that the recent spate of sabotage against NATO members in Europe was conducted largely through traditional rather than cyber means underscores this dynamic, as noted by Joshua Rovner, Rory Cormac, and Lennart Maschmeyer in their study *Sand in the Gears: Sabotage in World Politics*.

On November 16, 2025, a train driver on the line between Warsaw and Lublin in Poland reported track issues. During a site visit, the Prime Minister noted that the incident occurred on a rail line critical for delivering humanitarian aid to Ukraine. Polish officials stated they were confident that an explosive device was detonated on a section of the track, and subsequent damage to the overhead catenary was discovered on the same line, both instances likely representing acts of sabotage.

The man who, according to officials, was behind the attack on the Polish railway delivering supplies to Ukraine is Yevhen Ivanov, a Ukrainian convicted of collaborating with Russian military intelligence to organize arson attacks at home improvement stores, cafes, and a drone manufacturing plant in Ukraine, court documents show. Ivanov, who fled Poland following the attack there, worked for Yuri Sizov, an officer in Russian military intelligence (GRU). Assigning tasks to individuals with criminal backgrounds like Ivanov allows Russia to avoid risking highly trained personnel.

Russia's hybrid warfare tactics regularly rely on «expendable» agents – individuals recruited to perform single tasks. These agents are recruited and instructed primarily through social media networks. They are then deployed to execute various sabotage and influence operations in Europe on behalf of Russia. Moscow has little concern for the ultimate fate of these agents, as their single-use missions prevent them from learning the specific scale and scope of Russian intelligence operations. Utilizing

these proxies makes operations significantly cheaper for the Russian Federation while continuing to place a heavy burden on European security services, given that cross-border operations require extensive inter-state investigative cooperation. For this reason, in November 2025, the Center for European Policy Analysis (CEPA) launched a major new project: *Defend, Deter, Counter: Responding to Russia's Shadow War*, aimed at helping build the framework for a new transatlantic approach to deterrence.

At a press conference in Brussels, Finnish President Alexander Stubb noted that European nations must keep a «cool head.» He cautioned against overreacting to suspected Russian provocations, stressing: «Unfortunately, this is the new normal. Russia is trying to destabilize our societies through information and other campaigns».

In her article titled *Russia aims to drain Europe's investigative resources with sabotage campaign*, officials say, author Emma Burrows writes that this act of sabotage in Poland is one of 145 incidents (as of December 2025) recorded in the Associated Press database. Western officials state these are part of a broader, Russia-directed campaign to destabilize Europe. The incidents range from plugging vehicle exhaust pipes with expanding foam in Germany to plots involving the placement of explosive devices on cargo planes. Other acts include arson at retail stores and a museum, hacker attacks targeting politicians and critical infrastructure, and espionage by a ring convicted in the United Kingdom.

Some operations carried potential for catastrophic consequences, including mass casualties, such as parcel explosions at logistics hubs in Germany and the United Kingdom. Western officials stated they suspect these parcels were part of a broader Russian intelligence plot to place bombs on cargo flights bound for the United States and Canada.

In another instance, Western intelligence agencies foiled what they described as a Russian plot to assassinate the chief executive of a major German arms manufacturer providing weaponry to Ukraine. European authorities are investigating multiple instances of subsea infrastructure damage in the Baltic Sea, including a power cable connecting Estonia and Finland. Finnish authorities detained a vessel suspected of belonging to Russia's sanction-evading «shadow fleet» after this and other cables were severed.

When information appeared on a fake French Ministry of Defense website claiming citizens were being called up to fight in Ukraine, the French minister condemned it as Russian disinformation. Meanwhile, German authorities suspect Russia was behind a campaign that blocked dozens of car exhaust pipes ahead of national elections, according to a European intelligence official speaking on condition of anonymity to address sensitive matters.

In October 2025, a British court sentenced five men to lengthy prison terms for their involvement in an arson attack on a London warehouse holding satellite communication equipment bound for Ukraine. During sentencing, the judge noted that the attempt was organized on behalf of the Russian paramilitary organization Wagner and formed part of a widespread sabotage campaign.

Bart Schuurman, a professor specializing in terrorism and political violence, believes that beyond the obvious motivation of attempting to undermine public support for Ukraine, there is an element of power projection: Moscow uses these tactics to remind European leaders of its reach and capabilities.

Russia's approach to warfare leads to «escalation not by accident, but by design,» observe Andrei Soldatov and Irina Borogan in their work *War Without End: Russia's 'Shadow War'*.

Sweden's accession to NATO brought a decisive shift to the balance of power in the Baltic region. By abandoning its 212-year policy of neutrality dating back to the Napoleonic Wars, Sweden effectively transformed the Baltic Sea into a «NATO lake.» This shift triggered an intensification of Russian intelligence activity, marked by increased disinformation, cyberattacks, and covert operations. The Swedish Security Service (Säkerhetspolisen, SÄPO) reported in March that Russia is employing new espionage tactics. Russian intelligence is actively targeting individuals suffering from substance addiction as potential recruits for sabotage attacks in Sweden, prompting recommendations for heightened police surveillance. Addicts are reportedly targeted due to their low social standing and relative invisibility – valuable attributes for espionage proxies.

Russian intelligence operatives in Sweden operate out of numerous Russian institutions. SÄPO estimates that approximately 30 percent of the diplomatic staff at the Russian Embassy at Gjörwellsgatan 31 in Stockholm are intelligence officers whose duties include recruiting and handling agents. Furthermore, SÄPO identified the Russian Orthodox Church in Sweden as a second «legitimate» channel utilized by Moscow for intelligence gathering, influence operations, and other security-threatening activities. In response, the EU introduced a new sanctions framework on October 8, 2024, targeting individuals and entities associated with destabilizing hybrid threats originating from the Russian Federation against the EU and its allies. These threats encompass election interference, infrastructure sabotage, disinformation, cyberattacks, and the weaponization of migrants. Subsequently, on May 20, 2025, this sanctions regime was expanded to cover tangible assets linked to malicious activities (such as vessels, aircraft, real estate, and physical network components) as well as transactions involving financial institutions and crypto-asset services.

Thus, the contemporary Russian hybrid campaign in Europe has evolved into a comprehensive, multi-dimensional threat serving clear strategic goals. The primary operational vector remains the disruption of logistics and support for Ukraine. Attacks intentionally target critical supply nodes, including Polish railways, equipment warehouses in the United Kingdom, and defense industry leadership in Germany.

Simultaneously, Moscow seeks to exhaust the resources of European security agencies. Due to the scale and variety of low-level incidents, now exceeding 180 entries in the Associated Press database (as of August 2026), intelligence services are forced to disperse funds and personnel across localized investigations. This is coupled with psychological pressure and power projection. By creating threats of mass casualties, Russia signals to Western leaders its capability to operate deep within their home territories while attempting to panic the public.

To achieve these objectives, Russian intelligence has adapted its tradecraft. Contrary to expectations of the digital age, priority is given to traditional kinetic methods: physical sabotage, bombings, and arson often prove more disruptive than cyberattacks. Furthermore, Russian intelligence services (particularly the GRU) have shifted their approach to operational execution by relying heavily on «expendable» proxies. By recruiting individuals with criminal records or marginalized populations (such as drug-dependent individuals in Sweden) via social media, Russia reduces operational costs while maintaining plausible deniability. The coordination of this agent network is maintained under legal cover, relying on diplomatic missions and religious organizations like the Russian Orthodox Church.

This campaign is defined by the high complexity of hybrid threats. Russia seamlessly blends direct physical sabotage with information warfare and artificially induced migration crises along the borders of Finland, Poland, and the Baltic states.

Consequently, the West faces unprecedented challenges. Europe is forced to accept this reality as a «new normal,» recognizing that sabotage represents deliberate escalation. As the President of Finland emphasized, Western societies must maintain a «cool head,» resist provocations, and avoid advancing the Kremlin's objective of spreading fear. The cross-border nature of these attacks demands structural consolidation, while initiatives such as the CEPA project demonstrate that Europe is shifting from reactive, piecemeal investigations toward a unified, systemic strategy to deter Russia's shadow war.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*

When Sabotage Becomes an Attack: Does NATO Article 5 Apply to Russian Hybrid Operations?

Yuliia Lonchyna

Introduction

Hybrid operations have become one of the leading tools of modern aggression. The combination of cutting-edge technologies with tools of covert pressure enables an aggressor to interfere in the affairs of another state from within, without crossing the threshold of direct armed conflict. This undermines traditional notions of security and permanently blurs the line between peace and war. According to official NATO terminology, hybrid methods encompass military and non-military means, which are divided into covert and overt methods, such as: disinformation, cyberattacks, economic and political pressure, sabotage, subversion, and interference in the electoral process. Hybrid methods are used to sow doubt in the minds of the population and destabilize society.

Hybrid operations are a broad concept that encompasses a variety of threats. This paper focuses primarily on one type of hybrid operation—sabotage, defined as physical actions aimed at directly undermining a state's logistical and security capabilities, as well as causing harm to its infrastructure and population. Unlike less conspicuous political and economic levers of influence, acts of sabotage directly threaten national security and raise a crucial question: at what point does a hybrid operation reach the level of an armed attack?

Analysis of Article 5 of the North Atlantic Treaty

Article 5 of the North Atlantic Treaty stipulates that an armed attack against one NATO member is considered an attack against the Alliance as a whole and obligates each ally to provide assistance. This assistance may include any measures that member states deem necessary to restore and maintain security in the North Atlantic region.

Article 5 establishes an obligation of collective defense, whereas it gives member states leeway to determine the form of assistance without imposing universal obligations on them. It may include military, advisory, logistical, counterintelligence, and other measures.

A more complex issue is the lack of specificity in defining the very concept of an “armed attack.” The North Atlantic Treaty does not contain a specific activation procedure. Decisions are always made on a case-by-case basis depending on the circumstances. In the event of an attack, the North Atlantic Council is required to convene, consult, and reach a consensus.

NATO has its own explanation for the uncertainty surrounding the application of Article 5. It is believed that the absence of a clear threshold is no coincidence. Former Secretary-General Jens Stoltenberg stated that the Alliance does not want to give the adversary the opportunity to know in advance exactly where the limits of Article 5 lie. Thus, the absence of clearly defined limits provides a political advantage and room for manoeuvre.

Such flexibility leaves room for interpretation of what constitutes an armed attack. At first glance, the terrorist attack of the 11 September 2001 (the first and, to date, only instance of Article 5 being invoked) did not fit the classic definition of an armed attack in the form of a confrontation between two states. It was therefore the flexibility of Article 5 that enabled the allies to recognise this situation as grounds for invoking the principle of collective defence.

However, the downside of such ambiguity is that the boundaries of the threat are entirely undefined, as there are no criteria by which one can clearly determine exactly when a hybrid attack ceases to be an isolated incident and takes on the character of an armed attack.

It is precisely this ambiguity that creates an environment favourable to the aggressor – a “grey zone”. First, destabilising the situation in a country through hybrid methods requires fewer resources than direct armed conflict. Furthermore, by employing this strategy, the aggressor avoids resistance from the civilian population, large-scale military casualties, and some of the political and international legal consequences associated with overt aggression.

Russian Hybrid Operations

This problem is particularly evident in the nature of Russia’s current operations against NATO member states. Acts of sabotage on the territory of Allied nations have occurred in the past, but the start of Russia’s full-scale invasion of Ukraine has led to an increase in their number and scale. Recent years have seen numerous instances of sabotage, airspace violations, arson, acts of sabotage and other physical attacks, in which Western intelligence services have traced Russian involvement.

The year 2024 presented a major challenge for a number of European countries due to a sharp rise in the number of hybrid attacks. Moscow’s main objective was to disrupt aid deliveries to Ukraine and undermine security in Poland, Germany and other countries by using «single-use operatives» recruited online.

In May, a shopping centre in Warsaw was destroyed by arson in an incident that the Polish authorities classified as a terrorist act. Other attempts to set fire to infrastructure were also recorded. The crimes were committed by third parties recruited by Russian military intelligence (the GRU). According to the official findings, the main aim of the crimes was to intimidate the public.

At the same time, Germany has faced an unprecedented wave of arson attacks and acts of sabotage targeting its defence sector, critical infrastructure and logistics. German intelligence services and the government attribute most of these incidents to Russia’s hybrid warfare, aimed at disrupting the supply of military aid to Ukraine.

In particular, Russian sabotage groups are suspected of setting fire to a Diehl metallurgical plant in Berlin, a company that is assisting Ukraine with air defence systems. A separate investigation was conducted into the fire involving a DHL air cargo consignment in July 2024, in which Western intelligence services traced Russian involvement.

The Baltic Sea suffers extensively from the presence of the shadow fleet, as its waters have become a staging ground for Russian hybrid operations. This has led to an increase in attacks on seabed infrastructure, as well as coastal espionage and subversion. Among the most severe consequences are disruptions to undersea data cables and gas pipelines.

European governments regard this as a hybrid response to their support for Ukraine. To counter it, NATO has been forced to enhance its counter-intelligence, surveillance and inspections of suspicious vessels. Analysts point out that acts of sabotage on the seabed are part of a single, coordinated campaign and should not be viewed as isolated incidents.

There have been numerous unprecedented violations of NATO countries' airspace by missiles and drones, particularly over Poland and Romania. This poses a direct threat to infrastructure, as well as to the lives and safety of citizens.

One notable example is the events in Poland in September 2025, when 19 Russian drones entered Polish airspace. In response, Polish and allied forces were placed on high alert. Warsaw invoked consultations under Article 4 of the North Atlantic Treaty.

The Cumulative Effect Of Hybrid Operations

At the same time, the question arises as to whether hybrid attacks should be assessed individually or collectively, given that a combination of sabotage, cyberattacks and airspace violations poses a significantly greater threat than isolated incidents.

This gives rise to the dilemma of the cumulative effect.

Generally speaking, NATO has no officially adopted definition of the cumulative effect applicable to all hybrid operations. However, the Alliance has already acknowledged the need to take the cumulative effect into account in specific cases. For example, following the 2021 Brussels Summit, NATO explicitly recognised the possibility of a cumulative effect in the cyber domain, where a combination of individual malicious actions may, under certain circumstances, amount to an armed attack. Thus, the Alliance recognised that individual actions should not always be assessed in isolation, and that their cumulative effect may be relevant to the correct evaluation of a particular case.

At present, this approach is aimed solely at countering cyberattacks, so it is too early to claim that there is a single model applicable to all hybrid operations. At the same time, it is entirely logical to assume that such a framework could be applied in a broader context. Whilst individual incidents may not reach the level of an armed attack, it is precisely their interconnectedness, their common source of threat, and their intensity and scale that completely alter the assessment of the situation. Consequently, the key question is not simply whether a single act of sabotage crosses the threshold of an armed attack, but also whether a series of actions is being carried out whose cumulative threat poses a strategic threat to the Alliance.

Furthermore, it is worth bearing in mind that invoking Article 5 is just one of many options for countering Russian pressure. The Alliance possesses a well-established toolkit of countermeasures and defence measures. Stepping up counterintelligence operations, developing air defence capabilities, joint procurement, protecting critical infrastructure, conducting consultations under Article 4, and economic countermeasures against the shadow fleet — all of this means that the non-invocation of Article 5 does not signal inaction.

Conclusion

Ultimately, there is no bright line beyond which a hybrid operation constitutes an armed attack. This allows NATO to make decisions on a case-by-case basis, maintaining political flexibility.

At the same time, an individual incident which, in itself, does not reach the threshold of an armed attack should not be evaluated in isolation from a broader campaign. The cumulative effect of interrelated operations may create a qualitatively different level of threat and must be taken into account when assessing its legal implications.

Ultimately, there is no clear line beyond which a hybrid operation becomes an armed attack. This allows NATO to make decisions on a case-by-case basis, without being unduly constrained by legal restrictions.

At the same time, an individual incident which, in itself, does not reach the threshold of an armed attack, need not necessarily be considered in isolation from a broader campaign. The cumulative effect of interconnected operations can create a qualitatively different level of threat and must be taken into account when assessing it.

The greatest challenge is not the Alliance's inaction or weakness, but rather the aggressor's desire to remain in the 'grey zone' and avoid accountability. This is precisely why the assessment of operations must be comprehensive, so as to identify cumulative strategic risks in a timely manner without becoming fixated on individual provocations.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*

Can the Defense Industry Become Ukraine's New Economic Specialization Within the EU?

Olena Melkonova

Two seemingly unrelated stories are unfolding in the news at the same time today, but they actually describe the same phenomenon - the accelerated militarization of technology surrounding the war in Ukraine.

The first story is about the Moscow–Tehran axis. In March, Ukraine's Security Service and National Police exposed an Iranian general who organized the transfer of Shahed drone production technology to Russia: according to the investigation, more than 13,000 attack UAVs that Russia used to strike Ukrainian cities were produced at the Alabuga plant using Iranian documentation transferred under a secret agreement between the two countries' defense ministries. Then in July, Reuters reported on the other side of this exchange: US intelligence is investigating whether Russia helped Iran improve Shahed drone guidance following strikes on CIA facilities in Riyadh and Iraq. In other words, the technology exchange between Russia and Iran has long ceased to be one-directional, it is now full-fledged, real-time cooperation, in which combat experience gained over Ukrainian cities flows back in the form of improved rocket engines, anti-jamming systems, and navigation technology.

The second story is about Ukraine. On June 23, at the European defense and security summit in Brussels, EU Commissioner for Defence and Space Andrius Kubilius called Ukraine's defense industry the most innovative in the world and urged its integration into the EU's defense system, rather than simply funding it as an aid recipient. According to his estimate, weapons production in Ukraine has grown more than 50-fold compared to the start of the full-scale invasion. According to calculations by Ukraine's National Security and Defense Council, the production capacity of Ukraine's defense-industrial complex in 2026 is estimated at approximately \$55 billion, and this is no longer a one-off surge but a sustained industry trajectory: more than 160 companies produce FPV drones with a combined capacity of over 8 million units per year, and interceptor production for aerial targets is scaling up exponentially.

A tempting and widespread interpretation is that these two stories are causally linked: that Ukraine has ended up at the center of the world's most intense race in unmanned technologies precisely because it serves as a testing ground for the authoritarian Russia–Iran axis. This claim is appealing, but it confuses the channel with the cause. Even if Iran had never transferred a single Shahed-related technology to Russia, Russia would still be shelling Ukrainian cities around the clock with Kalibr and Kh-101 cruise missiles, Iskander ballistic missiles, and its own Geran kamikaze drones. Iranian cooperation has made this terror cheaper and more scalable, and has increased its volume, but it is not the root cause of why Ukraine has become the world's fastest innovator in wartime technology. The real reason is more fundamental: Ukraine is the only country in the world that has been fighting a full-scale defensive war on its own territory for four years against an adversary that constantly changes tactics and weaponry, forcing it to iterate weapon designs in weeks rather than the years typical of classic defense contractors. It is this experience that Brussels is now increasingly, and openly, calling a strategic resource for the entire European Union.

The question this article addresses is: is this experience enough for the defense industry to become a genuine economic specialization for Ukraine within the EU, comparable to how automotive manufacturing is a specialization of Germany, or pharmaceuticals of Ireland?

At the start of the full-scale war, Ukraine's defense-industrial complex was in a state close to collapse: outdated Soviet-era capacity, a lack of private initiative, and dependence on imports. Over three and a half years, the picture has changed fundamentally. Output from the state holding company Ukroboronprom (Ukrainian Defense Industry) grew from UAH 122 billion in 2024 to more than UAH 180 billion in 2025. According to projections cited by Forbes.ua, referencing Ukraine's head of armaments policy Oleksandr Kamyshin, the drones-and-missiles segment alone could generate up to \$35 billion in production potential in 2026, with the industry's combined capacity approaching \$55–60 billion per year.

Crucially, this growth has been driven mainly by the private sector: most enterprises have shifted to private ownership, giving them a flexibility that state monopolies cannot match. At the same time, funding covers barely half of the industry's real production potential, the state budget and international aid simply cannot keep pace with how fast the sector can scale output. This is the key paradox: Ukraine has industrial capacity that exceeds its own financial capacity to utilize it, meaning it is, in theory, already positioned to absorb external demand and foreign investment without having to build new production facilities from scratch.

EU rhetoric is indeed shifting: Kubilius has explicitly called on Europe to adopt Ukraine's experience in rapid production scaling, rather than simply supplying Kyiv with finished weapons. In April 2026, the European Commission and Ukraine's Ministry of Defence launched a joint program to invest in dual-use defense innovation worth €161 million, with the potential to attract up to €400 million. The European Defence Industrial Strategy, presented by the European Commission back in March 2024, separately provides for deepening cooperation with Ukraine and developing collaboration between the Ukrainian and European defense-industrial complexes. The strategy sets three distinct benchmarks for member states to reach by 2030, which are worth distinguishing since they are often conflated into a single figure in public discourse: at least 40% of defense procurement should take place in a collaborative format; the share of intra-European defense trade should reach at least 35% of the value of the EU defense market; and at least 50% of member states' defense procurement budgets should be spent on equipment of European origin (rising to 60% by 2035). In other words, the 35% figure refers specifically to intra-European arms trade, not to procurement as a whole.

The practical financial instrument driving this integration is the SAFE (Security Action for Europe) program, worth €150 billion in concessional loans. Ukraine does not receive direct SAFE loans, since these are reserved for member states, but Ukrainian companies are treated as European contractors and can participate in joint procurement «with Ukraine, in Ukraine, and for Ukraine.» The program's condition is that at least 65% of components must originate from the EU, Ukraine, or EEA/EFTA countries, effectively embedding Ukrainian manufacturers into the European supply chain as an equal link rather than an external vendor. Concrete agreements are already in place: Romania and Ukraine have agreed on joint drone production worth €200 million under SAFE. Coordination on the Ukrainian side is handled by a dedicated executive body - the Ukraine–EU working group on defense-industrial cooperation.

Despite the optimistic rhetoric, turning the defense sector into a lasting economic specialization is an energy-intensive, gradual process, and the risks deserve honest treatment.

First, Ukraine cannot access direct SAFE loans, and its 2026 state budget (\$98.3 billion in total defense spending, of which \$51.4 billion is allocated to weapons procurement) is physically unable to absorb the industry's entire production potential. Without legalized, large-scale exports or direct access to European defense funds, part of this capacity risks sitting idle.

Second, the current explosive growth is largely driven by wartime demand and real-time frontline feedback, precisely the circumstance that Commissioner Kubilius called Ukraine's unique advantage. But this is also a vulnerability: in a scenario where hostilities end, part of domestic demand will inevitably shrink, and it remains an open question whether the industry can integrate into the EU's peacetime export and cooperation chains before that happens.

Third, integration into the EU's defense technological and industrial base requires standardization to NATO/EU norms, protection of intellectual property rights, transparent procurement procedures, and investor confidence in Ukrainian corporate governance. All of this remains a subject of ongoing criticism from partners themselves and from anti-corruption institutions.

Fourth, the EU's legal architecture in this area is uneven, and this matters greatly for assessing political risk. Industrial financial instruments such as the European Defence Fund are adopted through the ordinary legislative procedure, under Articles 173(3) and 114 of the Treaty on the Functioning of the European Union, meaning by qualified majority in the Council together with the European Parliament, and no single country can block them on its own. By contrast, decisions involving international agreements with third countries (including Ukraine as a candidate country) under Articles 212 and 218 TFEU, as well as decisions in the field of the Common Foreign and Security Policy, are adopted unanimously, and it is here that an individual government opposed to deepening cooperation with Kyiv genuinely retains veto power.

EU economies traditionally specialize where they hold a durable structural advantage: Germany in machine-building, Ireland in pharmaceuticals and IT services thanks to its tax policy, Poland in logistics and manufacturing thanks to low labor costs and geography. Ukraine's advantage in the defense sector has a different origin: it stems not so much from labor costs as from a unique body of experience that no other country in the world possesses. This is a distinct type of competitive advantage, weapons iteration cycles in Ukraine are measured in weeks, while classic EU defense contractors work in years.

Putting the facts together produces this picture: Ukraine is already, de facto, Europe's largest and fastest producer of combat drones, and this is recognized at the highest levels of the EU. The picture in missile technology is different: Ukraine is developing its own capabilities: strike missiles, air defense and interception systems, but these remain niche rather than industry-defining capacities, and calling the country one of the key players in this field would be premature. The institutional architecture for integration is already in place and functioning, albeit in the limited form of indirect access to financing.

This specialization depends critically on three variables: whether part of this capacity can be shifted from a «wartime necessity» mode into a «long-term export and cooperation contract» mode; whether Ukraine carries out the institutional reforms needed to make the sector acceptable for direct foreign

investment rather than grant funding alone; and whether the EU maintains political unity in support of Ukraine despite pressure from individual governments and external factors such as the position of the United States.

The defense industry can become a new economic specialization for Ukraine within the EU, and, de facto, is already becoming one, outpacing the formal institutional framework. But this is not a guaranteed outcome; it is a conditional one. Unlike traditional specializations that form over decades through market forces, Ukraine's defense advantage emerged out of necessity, under the pressure of war and in response to Russia's technological cooperation with Iran, and it is therefore both fragile and powerful at once: fragile, because it is tied to an ongoing conflict and to partners' political will; powerful, because it provides a unique experience of high-speed wartime innovation that Europe's entire defense industry is eager to acquire. The prospect of turning this advantage into a permanent structural niche within the EU economy is realistic, but it requires a deliberate policy of conversion: legislative opening of exports, direct access to European defense funds, deep standardization, and institutional reform - all before wartime demand begins to decline.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*

Ukraine's Defence Industry after the War: A Driver of Economic Development or a Temporary Advantage?

Andrii Troian

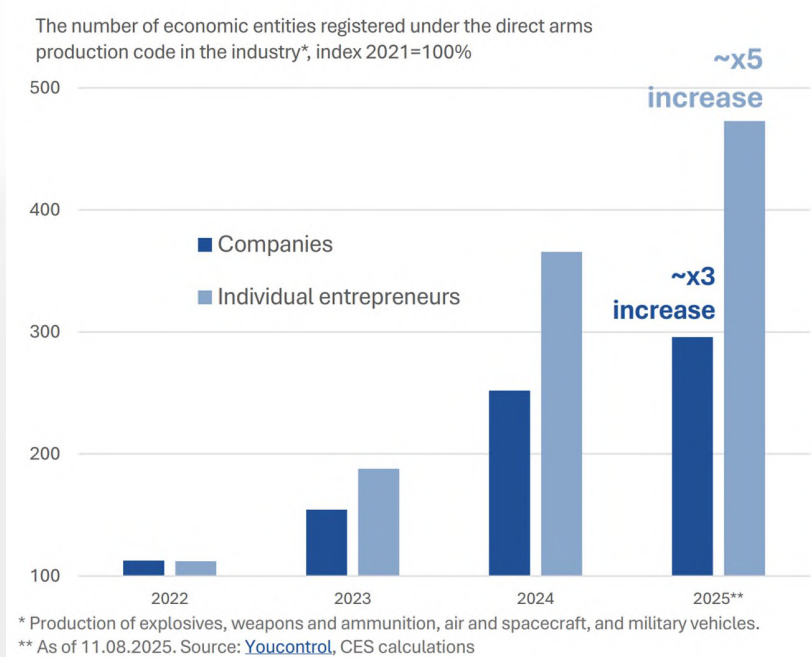
Introduction

Russia's full-scale invasion in February 2022 transformed Ukraine's military-industrial complex (MIC) from a sector with unrealised potential into one of the fastest-growing parts of the economy. The numbers of enterprises and employees, funding volumes, and production potential increased several fold; limited exports were permitted in July 2026, while the localisation of foreign defence companies is ongoing. Nevertheless, this growth rests on extraordinary wartime demand generated by public procurement and external financing. Their volumes may decline substantially after active hostilities end.

This paper analyses the MIC's ability, under conditions of relatively stable peace with Russia, to turn the scale achieved during the war into long-term economic strength. To this end, three related factors are assessed: domestic financing; the possibility of offsetting a decline in demand through exports and integration with the European MIC; and the sector's ability to retain and develop its workforce base, including by engaging veterans.

From Wartime Growth to a Post-war Shock

Ukraine's military-industrial complex entered the full-scale war with numerous structural problems: weak competitiveness of its products on the global market, low labour productivity, and an insufficient level of investment. The sector's contribution to the country's economy was also insignificant: less than 0.5% of total GDP.



Trends in the number of business entities—companies and individual entrepreneurs—registered under KVED codes for the direct production of armaments in 2022–2025 (index: 2021 = 100%).

Source: compiled by the Centre for Economic Strategy using YouControl data.

The full-scale invasion gave the MIC the necessary impetus to develop at a rapid pace. With very substantial budgetary and external injections into the sector, Ukraine's MIC was able to achieve production potential of \$55 billion, with actual output at \$12 billion this year. Each year, more enterprises were established in Ukraine's MIC, and the number of people employed also increased significantly. The latest public statements indicate that there are about 1,000 companies and 400,000 employees in Ukraine's MIC. According to some estimates, the contribution to GDP increased to 2%.

Ukraine remains the world's largest importer of armaments; however, recognising the need to develop its own MIC, it is increasing the volume of defence procurement involving domestic manufacturers. In this way, in 2025, more than 70% of budget expenditure on weapons procurement was directed towards products manufactured by Ukraine's MIC. This gives the sector an additional stimulus for development.

The MIC's rapid growth is supported by exceptional wartime demand and by state and external financing of the sector. Arms manufacturers emphasise the underutilisation of their production potential because the state, as the customer, is unable to make full use of their capabilities. With MIC production potential of \$55 billion, actual output of \$12 billion amounts to about 22% of what is possible, even while the sector is booming. After hostilities end and defence procurement logically declines, this imbalance may widen. In turn, this will create a risk of job losses, an outflow of personnel, and an overall contraction of the MIC.

The risk of production being moved abroad because of underutilisation is already partly materialising. In October 2025, 51% of the surveyed MIC enterprises stated that they planned to relocate or had already done so; alongside security risks, respondents pointed to insufficient procurement volumes from the government 'despite being able to produce more'.

Therefore, turning wartime growth into a long-term economic effect will depend on whether the MIC can count on continued procurement from the state while attracting other sources of financing and thereby offsetting the decline in demand that may occur when hostilities end.

Sector Financing and the Sale of MIC Products

The economic resilience of Ukraine's MIC is currently based primarily on domestic defence procurement. In 2025, procurement from domestic manufacturers reached almost UAH 430 billion (about \$10.3 billion); according to the Ministry of Defence, their share of lethal-weapons procurement was 82%. Thus, Ukrainian enterprises are already able to substitute for a significant share of imports and meet domestic demand.

At the same time, this model makes the MIC dependent on a single customer—the state—which is justified in wartime, but only to the extent that the state is able to provide sufficient demand. In practice, the state's financial resources limit actual output. Ukraine's external partners absorb part of the MIC's otherwise unsold output. For example, \$6.1 billion in external financing was secured in 2025. However, maintaining such volumes after hostilities end is not guaranteed.

Exports are a second potential source of demand for MIC products. The mechanism introduced in July 2026 (Resolution No. 875 of the Cabinet of Ministers of Ukraine, also known as the 'Fast Track') permits the export of certain products subject to special approval but maintains the priority of domestic needs. An export authorisation may be withheld if a state customer intends to purchase the products for the needs of the Armed Forces of Ukraine.

The special mechanism also requires a payment of 20% of the contract value for finished goods and 30% for components. According to statements by sector representatives, such financial requirements complicate exports and, in some cases, make them economically unfeasible. The special mechanism also limits exports to countries with which Ukraine has signed agreements (the so-called Drone Deal agreements; there are currently nine such countries). Exports to other markets are possible under the older interagency approval mechanism. Thus, the 'Fast Track' accelerates certain sales channels while restricting them financially, which makes market entry more difficult for some manufacturers.

Alongside export revenue, Ukraine's MIC can also establish its position through joint ventures and the localisation of production, which may ensure long-term cooperation. According to statements by the Ministry of Defence of Ukraine, 25 foreign companies are engaged in localisation in Ukraine. Some of them, such as the German companies Rheinmetall and Quantum Systems, already service or manufacture equipment in Ukraine.

Additional opportunities to attract financing are created by the European SAFE mechanism, which allows Ukrainian companies to participate in joint procurement. In the long term, this ensures interoperability and strengthens the links between Ukraine's MIC and the European Union's MIC.

Domestic defence procurement and external financing provide the MIC with a financial foundation, but after the war they are unlikely to be able to maintain the existing capacity on their own. The opening of exports, deeper cooperation with international partners, localisation, and procurement under the SAFE mechanism may partly offset the decline in demand and domestic defence orders. However, the sector's economic impact will depend on the attractiveness of Ukraine's MIC to foreign investors after the war, as well as on the ability of Ukrainian enterprises to compete in global arms markets. The Ukrainian state, as the MIC's main customer today, will have to maintain a certain level of state financing to ensure the sector's resilience after hostilities end.

Human Capital—the MIC's Need for Personnel

Although the number of people employed by MIC enterprises has increased fourfold since 2022 (according to official estimates), the shortage of qualified personnel is a tangible constraint on the development of this sector of the economy. Thus, according to a survey of Ukrainian companies, 56% of respondents reported a need for more engineers, while 48% reported a need for production personnel. At the same time, efforts to address the personnel shortage are developing along two tracks: short-term and long-term.

The short-term track is focused on the sector's immediate needs and is implemented through short training and retraining programmes on a limited scale. For example, enterprises belonging to the National Association of Ukrainian Defense Industries are introducing targeted training programmes, including programmes based at universities, while the State Employment Service of Ukraine (SES) has issued more than 100,000 vouchers for retraining and professional development as of 2026. However, only some of these programmes are aimed at engineering and technical specialisations.

The long-term track requires both the development of technical educational institutions and the successful integration of veterans. At first glance, these factors are only loosely connected; however, the skills and knowledge acquired during military service prove highly compatible with the needs of the MIC. A study conducted by SkillLab in cooperation with the SES in 2025 demonstrates that veterans' skills overlap most strongly with the requirements of the manufacturing and machine operations sectors—the main sectors involved in the work of the MIC.

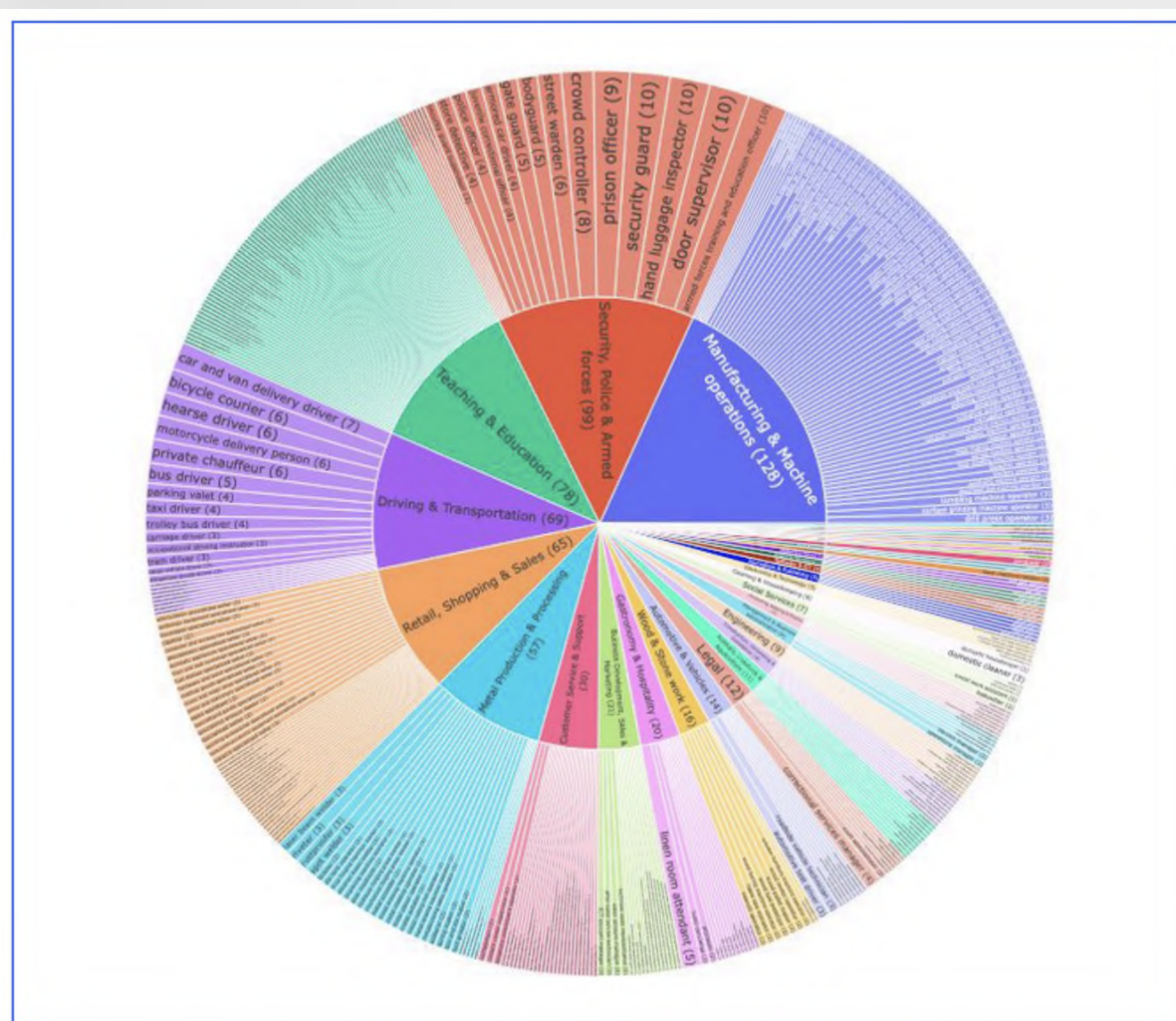


Figure 4 Distribution of the matching occupations by career field

Distribution of occupations compatible with the skills of Ukrainian veterans, by career field.
Source: SkillLab.

Some veterans may be employed by enterprises in the sector after hostilities end, but only if effective mechanisms are developed for recognising the qualifications and skills acquired during military service. Long-term government measures, such as government strategies No. 1209-r and No. 1350-r and the ‘Veteran. Work’ programme, provide for the employment and retraining of veterans. These documents take military competencies into account but do not identify priority sectors for veteran integration. Therefore, necessary post-war steps will include developing and scaling up dedicated training and retraining programmes for occupations needed by the MIC, with a specific focus on veterans, as they may become the largest group available for employment in Ukraine’s MIC while also possessing sufficiently compatible skills.

Post-war Scenarios

Scenario 1: The MIC as an Economic Driver

This optimistic scenario assumes that the state maintains multi-year defence procurement, thereby ensuring production volumes at the most competitive MIC enterprises. At the same time, new flexible export mechanisms are introduced that encourage manufacturers to enter international arms markets and offset some of the loss of government procurement resulting from reduced demand. The MIC

retains its workforce base and expands it by retraining some veterans for employment at MIC enterprises and in related fields. This option has a clear limitation: it depends on retaining personnel within the country, effectively engaging them in work in the MIC, and maintaining stable budgetary and external investment in the sector.

Scenario 2: Preserving a Smaller Sector

This scenario assumes a substantial reduction in domestic procurement, but at the same time the state guarantees a minimum level of demand for critical products because the Russian threat does not disappear. The export mechanism remains unprofitable for some manufacturers; therefore, foreign investment offsets only part of the lost revenue. A substantial share of companies closes or shifts to other sectors, while the largest manufacturers retain personnel and orders from the state. Retraining programmes engage veterans to some extent, but the shortage of engineering and technical personnel persists because of the programmes' limited reach and the generally unfavourable state of technical education as a whole. The sector's contribution to economic growth remains significant but does not make it structurally significant, while the MIC integrates with its European counterpart.

Scenario 3: The MIC as a Temporary Advantage

Under the worst-case scenario, the reduction in budgetary and external inflows occurs faster than exports can be effectively opened and enterprises can reorient themselves towards export markets. The absence of long-term orders from the state prevents enterprises from using the capacities they have created, causing a substantial share of the market to contract. Enterprises move production capacity abroad because of more favourable conditions, and skilled workers make the same choice. Targeted retraining is ineffective and limited, so veterans do not become an important source of personnel. The MIC retains certain critical capabilities but loses many jobs, scale, and its technological advantage. In this scenario, wartime growth is only a temporary advantage.

Conclusion

In summary, Ukraine's MIC has all the prerequisites to become a driver of post-war development. However, its wartime growth is not only an advantage but also a major limitation, because even amid the extraordinary wartime demand, the sector's actual output amounts to only about 22% of its production potential. Transforming the MIC into a structurally significant sector of the economy will require maintaining some defence procurement, stimulating exports, and attracting personnel, including veterans.

Of the scenarios described, the most likely appears to be the formation of a smaller but more competitive MIC that is closely integrated with the European defence industry (Scenario 2). This is due to the existence of a limited export regime even today, alongside the existing integration of the MIC with European manufacturers. At the same time, retraining programmes already exist that the Ukrainian state and the private sector can expand after the war.

Awareness of the available resources—enterprises, employees, and foreign investment—and systematic efforts to retain and scale them will determine whether Ukraine's MIC returns to the problems of the past or seizes a historic opportunity for development.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*

Deterrence Without War: Are the Baltic States Prepared for Russian Hybrid Threats?

Nazarii Pomohaibo

99 Luftballons

For passengers at Lithuanian airports, late October 2025 served as a reminder of the country's geographic proximity to the aggressor state and its satellite. Dozens of weather balloons from Belarus, each carrying around forty kilograms of contraband cigarettes, forced the country to close its airports at least five times within a week, leading to the cancellation of roughly 140 flights and disrupting the plans of more than 20,000 passengers. In response, Vilnius closed its land border with Belarus for a month, calling the October events a “hybrid attack”, to which Belarus blocked Lithuanian trucks from leaving its territory, calling Lithuania's policy “an escalation aimed at securing EU funding”. Under pressure from truckers, the Lithuanian border reopened on November 19, three weeks after the hasty decision. Lithuanian intelligence concluded that the Belarusian regime retains the capacity to halt the smuggling at will, yet deliberately exploits it as a tool of indirect influence, much as it did during the 2021 migration crisis.

This episode lies somewhat outside the conventional understanding of a “hybrid attack”. It featured none of the usual markers, no green men, no severed cables, no protests by Russian-speaking minorities, no cyberattacks, no large-scale disinformation campaigns. Yet a NATO member state still found itself forced to impose, and then reverse, its own policy because of a neighboring dictatorship and its balloon smugglers. Equally telling is the fact that, although the military held permission to shoot the balloons down, Lithuania lacked the practical ability to use kinetic weapons against them safely. The key word here is “safely”. Across more than 500 incidents, nothing guaranteed that a balloon's 40-kilogram payload held only cigarettes. The Baltic states are among the European states most systematically prepared for threats from Russia and Belarus. The central question is whether this preparation will suffice against threats that exceed expectations and continue to evolve beyond the kinetic domain.

Following the expectation that hybrid threats will keep “evolving”, the kinetic domain of war can no longer serve as our sole frame. In the balloon case, Lithuania held the maximum toolkit available for deterrence, its own border, airspace, airports, and an intelligence assessment that named the source of the threat directly. The actor was known, and legal grounds existed for a measured response. Even so, the incident can hardly be called a success for Lithuania. If the outcome turned out mixed in a domain where a Baltic state holds full jurisdiction and freedom of action, what outcome should we expect in an environment where it holds neither?

Russian-Speaking Minorities and National Law Are No Gordian Knot

The standard Baltic response to non-kinetic threats has been framed around minority policy and domestic legislation. In March 2025, the Estonian parliament amended the constitution by a vote of 93 to 7, stripping third-country nationals of the right to vote in local elections. In 2021, around 139,000 residents held that right without Estonian or other European citizenship, and 61,000 of them exercised it. In Narva alone, around 7,000 Russian citizens lost their vote ahead of the October 2025 elections.

The outcome can be read either as evidence of resilience or as an opening for more radical politics, depending on interpretation. Contrary to expectations, turnout in Ida-Viru County rose from 47.3 to 53.5 percent, even though the loss of voting rights should have pushed it down. At the same time, the list of Mihhail Stalnuhhin, expelled from his party in 2022 for calling the government fascist over the removal of Soviet monuments, won Narva with more than 35 percent, while the openly pro-Moscow KOOS list took four. So does restricting non-citizen voting rights genuinely strengthen a country against internal destabilization?

Old Solutions, Modern Problems

Latvia has already answered this question. Stripping the exiled Russian channel TV Rain (Dozhd) of its license in 2022 was presented as a demonstration of an information-defense tool, yet a Latvian court overturned the decision in July 2025, and the appeal still awaits a ruling. Whatever the channel's fate, what matters is what this decision could ever have achieved in the first place. A license governs broadcasting within a state's territory, and revoking one can serve as a symbolic step toward information sovereignty, but the spread of content by pro-Russian networks reaches well beyond licensing. National law, however useful as a tool of manipulation (a practice known as lawfare), still ends where the national territory ends. Yet, as we will see, almost none of what carries real informational weight sits on that territory, or on any other.

Between November 2025 and January 2026, researchers examined 1,799 articles from the Estonian segment of the Pravda network, an automated site system exposed by the French agency VIGINUM in 2024 under the name Portal Kombat, initially comprising 193 portals. Every article originated on Telegram; the sources numbered 172 channels, with the five largest producing 61 percent of the material. One striking finding is that the network produces little original content, and instead gathers and amplifies existing posts and narratives, giving each message a permanent web address, turning a fleeting messenger post into indexed, citable text. Beyond ordinary amplification, the report flags a coming threat termed "LLM poisoning", the contamination of an AI model's memory with large volumes of "favorable" information that can later reach AI users disguised as authentic.

One figure from the study deserves particular attention. Among the sources in the Estonian segment, 99 percent publish in Russian, against 96 percent in Georgia and 85 percent in Moldova. In Tbilisi, Chisinau, and other parts of Europe where Russian struggles to carry a Russian story to its audience, the network often resorts to machine translation, producing visible errors such as rendering the Russian word "mir" literally as "world" rather than "peace". In the Baltic states, by contrast, the focus on the Russian-speaking audience is sharper, which makes distributing information cheaper and more authentic than elsewhere in Europe.

Given that no single state can effectively influence corporations and social networks on its own, the European Union, as one of the world's largest markets, must rely on broader instruments of control. In July 2025, sanctions added the founder of TigerWeb, a Crimean company linked to running the disinformation network described above. Yet this amounts to a single individual, residing outside EU territory, while several hundred domains continue operating. Moreover, none of these domains, channels, or hosting services sit within the Baltic states, leaving Baltic institutions without direct authority over them and placing influence over such networks beyond the EU's reach.

The Commission answered with the European Democracy Shield, unveiled on 12 November 2025, whose most visible component, the European Centre for Democratic Resilience, began work on 24 February 2026. The Centre rests on voluntary participation by member states and operates “with full respect for national and institutional competences”, meaning it coordinates rather than compels. On 23 June 2026, a special European Parliament committee also concluded that the Centre needs establishment through a separate legal act, with its own operational parameters and budget. The change that genuinely strengthens the Baltic position, however, is the mechanism forcing the companies behind major social networks to answer to the EU’s weight as a digital market. On 29 October 2025, a provision took effect granting vetted researchers access to non-public data on social media algorithms.

Regulatory Asymmetry

EU regulators recognized the need for a more structured and coherent response, yet left the question of national jurisdiction unaddressed. The EU Digital Services Act rests on the country-of-origin principle. Oversight and enforcement fall to the member state where an intermediary holds its main establishment, rather than the state receiving its content. For very large online platforms (VLOPs), the arrangement grows more complicated still. The European Commission holds exclusive authority over platform obligations to assess and mitigate systemic risks, including risks to public discourse and elections. The remaining duties are split between the Commission and the coordinator of the state where the platform is established. Almost all such platforms are “established” in Ireland or Luxembourg.

What does this mean for each individual Baltic state facing the evolution of hybrid attacks on the information domain? Some authority remains in its hands. A national body can issue an order against specific illegal content, and the platform must respond regardless of where it is registered. What the Baltic states lack is the power to force a company like Meta to rewrite its risk assessment or change its algorithm settings or moderation practices, since those duties belong to the Commission. In certain cases, an Estonian coordinator may ask its Irish counterpart to assess a case and take action; the latter must respond with an assessment within two months, and inaction sends the case to Brussels.

Hybrid threats, however, demand a fast response. In the case of information interference, a single Baltic country effectively holds limited, narrow influence, with the alternative being a procedurally complex and lengthy process. FIMI (foreign information manipulation and interference) constitutes coordinated behavior instead, involving networks of inauthentic accounts, thousands of posts, and algorithmic amplification. Simply removing posts can hardly serve as the region’s complete response to Russian attempts at destabilizing the information space. The authority and leverage that remain national, then, are built for a different kind of phenomenon than FIMI actually represents.

An interesting asymmetry emerges here. Estonian, Latvian, and Lithuanian services publish arguably the most detailed open-source FIMI assessments in Europe. They hold the best description of the problem alongside the weakest leverage over the environment in which it unfolds. Equally telling is what the EU actually fines companies for. In December 2025, the Commission fined X 120 million euros for a lack of transparency, covering a misleading verification-badge design, missing ad-targeting controls, and restricted researcher access to algorithmic data. On 28 May 2026, Temu received the largest fine in the Act’s history, 200 million euros, for an inadequate risk assessment regarding illegal goods. In February 2026, preliminary findings against TikTok, and later against Meta, addressed “addictive design”. None of these prominent cases, though, concerned information manipulation itself.

Proceedings actually opened over disinformation remain troubled. On 17 December 2024, the Commission launched an investigation into TikTok over the platform's failure to assess and mitigate risks to electoral integrity around Romania's presidential election, the first in the EU annulled over information manipulation on social media. A final ruling remains pending, though it will set an important precedent for judging Europe's capacity to counter information interference.

Conclusions

For detection, preliminary assessment, and direct engagement with a wide range of hybrid threats, the Baltic states are better prepared than any other group of European states. Their services describe Russian operations with a precision that far larger states lack. Readiness to repel such threats safely and effectively remains an open question, however. As threats keep evolving, these states remain constrained by the limits of EU institutional support, by legal norms, by domestic pressure, and by the nature of hybrid actions that stay below the threshold of war.

Looking at these limits through the specific case of information interference, three structural gaps stand out. A jurisdictional gap: national law ends where national territory ends. A competence gap: authority over very large platforms belongs exclusively to the Commission, leaving national coordinators to act only within boundaries the Commission sets. A priority gap: information interference remains an understudied issue, lacking clear, effective, and unified procedures for response.

Even so, the Baltic states remain the strongest actors in countering Russia's hybrid threats, though a question still stands. Will they receive sufficient support, and will they gain the leverage needed to prepare for new threats that Russia is actively studying? The balloon episode shows that a state can still lose an exchange even where it holds full jurisdiction over its own border. The information environment recognizes no such borders.

*This article was written for the magazine "Think Tanks Essentials".
Views expressed in the article are those of the author.*



EEYES – a space for youth shaping the future today!

EEYES is the youth initiative of the International Charitable Foundation “UDONATION”. It is a platform that makes talented young people visible and opens new opportunities for growth and self-realization. Here, young individuals gain experience, showcase their potential, and contribute to building a modern intellectual and cultural community.

Within EEYES Insight Lab, analytical research is conducted, while events—such as informal meetups, open lectures, panel discussions, and forums—serve as spaces for exchanging ideas. A key focus is cultural representation in Berlin, where international debates and meetings with partners take place. The Instagram feed highlights current events, and work on grant applications ensures the sustainability of projects. Each direction includes internship opportunities, so participants gain not only knowledge but also practical experience.

EEYES is an environment where young voices are heard and ideas turn into real actions.



WEBSITE



TELEGRAM



INSTAGRAM



FACEBOOK

REFERENCES

Section 1. Overview of think tanks analyses

Publications used:

- Doliński, Michał. The potential US withdrawal from NATO under American law. Polish Institute of International Affairs (PISM), July 10, 2026. URL: <https://www.pism.pl/publications/the-potential-us-withdrawal-from-nato-under-american-law>
- Koesterke, Felix. The Ankara Summit: It's Trump's NATO – Europe just lives in it. Egmont Institute, July 15, 2026. URL: <https://egmontinstitute.be/the-ankara-summit-its-trumps-nato-europe-just-lives-in-it/>
- NATO's Eastern Flank Frontier. Center for the Study of Democracy, June 30, 2026. URL: <https://csd.eu/publications/publication/natos-eastern-flank-frontier/>
- Delval, Théa; Rogers, Luca. Legality and Reality: The Eastern Flank and the Ottawa Convention. International Centre for Defence and Security (ICDS), June 15, 2026. URL: <https://icds.ee/en/legality-and-reality-the-eastern-flank-and-the-ottawa-convention/>
- Raik, Kristi. When Old Certainties No Longer Hold: Nordic-Baltic Foreign Policy Adaptation. International Centre for Defence and Security (ICDS), August 25, 2026. URL: <https://icds.ee/en/when-old-certainties-no-longer-hold-nordic-baltic-foreign-policy-adaptation/>
- Clausen, Maria-Louise; Albrecht, Peter. Strategic autonomy and Europe's new logic of intervention. Danish Institute for International Studies (DIIS), June 9, 2026. URL: <https://www.diis.dk/en/research/strategic-autonomy-and-europes-new-logic-of-intervention>
- Kovalčíková, Nad'a; Spatafora, Giuseppe. Not just an addendum: Making resilience a key pillar of Europe's defence. European Union Institute for Security Studies (EUISS), July 6, 2026. URL: <https://www.iss.europa.eu/publications/briefs/not-just-addendum-making-resilience-key-pillar-europes-defence>
- Thomson, Tevian. The FCAS Collapse and Europe's Enduring Coordination Problem. International Centre for Defence and Security (ICDS), June 22, 2026. URL: <https://icds.ee/en/the-fcas-collapse-and-europes-enduring-coordination-problem/>
- Gressel, Gustav. NATO's digital arsenal: How Europe can avoid a new dependence on America. European Council on Foreign Relations (ECFR), July 29, 2026. URL: <https://ecfr.eu/article/natos-digital-arsenal-how-europe-can-avoid-a-new-dependence-on-america/>
- Le Grand, Pauline. EU Defence Series: Europe's Tech Challenge. International Centre for Defence and Security (ICDS), July 30, 2026. URL: <https://icds.ee/en/eu-defence-series-europes-tech-challenge/>
- Franke, Ulrike. Buzzkill: How to defend Europe against drones. European Council on Foreign Relations (ECFR), August 17, 2026. URL: <https://ecfr.eu/publication/buzzkill-how-to-defend-europe-against-drones/>
- McGlynn, Jade. The Trap Closes: How Russia Suppresses Resistance in Occupied Ukraine and How We Can Still Help. International Centre for Defence and Security (ICDS), June 19, 2026. URL: <https://icds.ee/en/the-trap-closes-how-russia-suppresses-resistance-in-occupied-ukraine-and-how-we-can-still-help/>
- Ditrych, Ondrej; Hobhouse, Caspar; Kovalčíková, Nad'a; Marangio, Rossella; Rühlig, Tim; Scazzieri, Luigi; Spatafora, Giuseppe; Zorić, Bojana. Empowering Ukraine: Spend smarter, support harder. European Union Institute for Security Studies (EUISS), July 20, 2026. URL: <https://www.iss.europa.eu/publications/analysis/empowering-ukraine-spend-smarter-support-harder>
- Delval, Théa. The Special Tribunal for Ukraine: Turning the Wheels of International Justice. International Centre for Defence and Security (ICDS), June 18, 2026. URL: <https://icds.ee/en/the-special-tribunal-for-ukraine-turning-the-wheels-of-international-justice/>

- Kim, Youngjun. Facing the North Korea–Russia alliance: EU–ROK strategies for deterrence and cooperation. Elcano Royal Institute, July 24, 2026. URL: <https://www.realinstitutoelcano.org/en/analyses/facing-north-korea-russia-alliance-eu-rok-strategies-for-deterrence-and-cooperation/>
- Meister, Stefan. A Declining, but More Dangerous Power: Russia’s Receding Reach in the Neighbourhood. International Centre for Defence and Security (ICDS), June 29, 2026. URL: <https://icds.ee/en/a-declining-but-more-dangerous-power-russias-receding-reach-in-the-neighbourhood/>
- Lozka, Katsiaryna; Althoff, Jonas; Klarhoefer, Lavinia; Gargano, Maria; Yaroshevych, Maryna. The Future of EU Enlargement Policy: Four Scenarios for Enlargement in Wartime Europe. Egmont Institute, July 2, 2026. URL: <https://egmontinstitute.be/the-future-of-eu-enlargement-policy-four-scenarios-for-enlargement-in-wartime-europe/>
- Morina, Engjellushe; Valodskaitė, Gabrielė. The magnificent ten: A coalition of the willing to drive the EU’s next enlargement. European Council on Foreign Relations (ECFR), July 23, 2026. URL: <https://ecfr.eu/publication/the-magnificent-ten-a-coalition-of-the-willing-to-drive-the-eus-next-enlargement/>
- Barana, Luca; Cinciripini, Luca. Ukraine and the Next MFF: The Strive for Predictability. Istituto Affari Internazionali (IAI), July 22, 2026. URL: <https://www.iai.it/en/publications/c41/ukraine-and-next-mff-strive-predictability>
- Bryjka, Filip; Wójtowicz, Aleksandra. Escalating the Polish-Ukrainian dispute: Russia’s operational objective in Poland. Polish Institute of International Affairs (PISM), August 24, 2026. URL: <https://www.pism.pl/publications/escalating-the-polish-ukrainian-dispute-russias-operational-objective-in-poland>
- Surwillo, Izabela; Schwab, Julia. Europe’s energy security in 2026: More resilient, but systemically exposed. Danish Institute for International Studies (DIIS), August 19, 2026. URL: <https://www.diis.dk/en/research/europes-energy-security-in-2026-more-resilient-but-systemically-exposed>
- Szczudlik, Justyna. The European Union faces “China Shock 2.0”. Polish Institute of International Affairs (PISM), July 20, 2026. URL: <https://www.pism.pl/publications/the-european-union-faces-china-shock-20>
- Kaca, Elżbieta. Countering the use of crypto-assets to circumvent sanctions against Russia. Polish Institute of International Affairs (PISM), July 17, 2026. URL: <https://www.pism.pl/publications/countering-the-use-of-crypto-assets-to-circumvent-sanctions-against-russia>
- Vladimirov, Martin; Kostova, Tihomira; Koeppen, Marius; Petrova, Vanya. Strategic Corruption: The Nexus Between Russian Illicit Financial Flows and Offshore Finance. Center for the Study of Democracy, July 28, 2026. URL: <https://csd.eu/publications/publication/strategic-corruption-1/>
- Kaca, Elżbieta. The results and limits of European states’ interventions against the Russian shadow fleet. Polish Institute of International Affairs (PISM), August 25, 2026. URL: <https://www.pism.pl/publications/the-results-and-limits-of-european-states-interventions-against-the-russian-shadow-fleet>
- Maurice, Paul. France-Germany: Overcoming Differences to Strengthen European Sovereignty. Institut français des relations internationales (IFRI), July 15, 2026. URL: <https://www.ifri.org/en/memos/france-germany-overcoming-differences-strengthen-european-sovereignty>
- Leonard, Mark. The tragedy of “Westalgia”. European Council on Foreign Relations (ECFR), July 16, 2026. URL: <https://ecfr.eu/article/the-tragedy-of-westalgia/>
- Wilson, Houston. Europe in an Age of America First Economics. Istituto Affari Internazionali (IAI), August 3, 2026. URL: <https://www.iai.it/en/publications/c05/europe-age-america-first-economics>
- Belin, Célia; Cliffe, Jeremy; Lons, Camille; Victor, Constance. If Marine Le Pen wins: A European guide to a far-right France. European Council on Foreign Relations (ECFR), August 4, 2026. URL: <https://ecfr.eu/publication/if-marine-le-pen-wins-a-european-guide-to-a-far-right-france/>

SECTION 2. INSIGHT LAB ANALYTICAL MATERIALS

Popovych, Oleksandra. A Russian drone on the territory of NATO member states: what does it mean?

- Adamowski J. Russia's 'Zapad' drill has Europe on edge about low-key attacks. Defense News. 2025. 2 Sept. URL: <https://www.defensenews.com/global/europe/2025/09/02/russias-zapad-drill-has-europe-on-edge-about-low-key-attacks/> (дата звернення: 08.08.2026).
- Drone flights near airbase could be spying operation, Belgium's defence minister says / Euronews. 2025. 3 Nov. URL: <https://www.euronews.com/2025/11/03/drone-flights-near-airbase-could-be-spying-operation-belgiums-defence-minister-says> (дата звернення: 08.08.2026).
- Drone incursions sow fear, chaos along NATO's Baltic, Finnish borders / Reuters. 2026. 28 July. URL: <https://www.reuters.com/business/aerospace-defense/drone-incursions-sow-fear-chaos-along-natos-baltic-finnish-borders-2026-07-28/> (дата звернення: 07.08.2026).
- Hoeft C., Greene N., Newton M. A Necessary Air of Venom: Hardening NATO's Airspace. Center for European Policy Analysis (CEPA). 2025. 20 Nov. URL: <https://cepa.org/article/a-necessary-air-of-venom-hardening-natos-airspace/> (дата звернення: 09.08.2026).
- NATO launches "Eastern Sentry" to bolster posture along eastern flank / North Atlantic Treaty Organization. 2025. 12 Sept. URL: <https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank> (дата звернення: 07.08.2026).
- NATO member Romania shoots down stray drones from Ukraine war after years of incursions / Associated Press. 2026. 28 July. URL: <https://apnews.com/article/romania-europe-russia-ukraine-war-drones-nato-ee9775ba338f5408bfa9ab3cb5f2ad1d> (дата звернення: 08.08.2026).
- Russia's UAV Campaign Over Europe : Research Paper / International Institute for Strategic Studies (IISS). 2026. URL: https://www.iiss.org/globalassets/media-library---content--migration/images-delta/publications/research-papers/2026-new/russia-uav/ammended-file/russia_uav-campaign-over-europe.pdf (дата звернення: 09.08.2026).
- Russian Offensive Campaign Assessment, September 10, 2025 / Institute for the Study of War. 2025. 10 Sept. URL: <https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-september-10-2025/> (дата звернення: 08.08.2026).
- Pleines H. Violations of non-combatant airspace during the Russo-Ukrainian war. 24 Feb. 2022–01 Sept. 2026 : dataset. – Version 1.2. – Discuss Data, 2026. – URL: <https://zenodo.org/records/22303031/files/dataset.xlsx> (дата звернення: 14.08.2026).
- Romanian lawmakers adopt law to shoot down drones breaching airspace // Reuters. – 2025. – 26 Feb. – URL: <https://www.reuters.com/world/europe/romanian-lawmakers-adopt-law-shoot-down-drones-breaching-airspace-2025-02-26/> (дата звернення: 14.08.2026).

Vasylyk, Yaryna. From Shahed to joint production: what Russia and Iran have learned from each other

- U.S. Department of the Treasury. Treasury Sanctions Iranian Persons Involved in Production of Unmanned Aerial Vehicles and Weapon Shipment to Russia. 08.09.2022. URL: <https://home.treasury.gov/news/press-releases/jy0940> (accessed: 18.08.2026)
- Burrows E. Russia is sending upgraded drones used in the Ukraine war to Iran, officials say. Associated Press. 27.03.2026. URL: <https://apnews.com/article/russia-iran-drones-shahed-war-israel-ukraine-840b4f885d99714bdb7813c0d56213cf> (accessed: 18.08.2026)
- Rubin U. Russia's Iranian-Made UAVs: A Technical Profile. Royal United Services Institute (RUSI). 13.01.2023. URL: <https://www.rusi.org/explore-our-research/publications/commentary/russias-iranian-made-uavs-technical-profile> (accessed: 18.08.2026).
- Jensen B., Atalan Y. Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies. 13.05.2025. URL: <https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign> (accessed: 19.08.2026)

- Burrows E. Drone debris found in Ukraine indicates Russia is using new technology from Iran. Associated Press. 25.06.2025. URL: <https://apnews.com/article/russia-iran-drones-shahed-ukraine-israel-strikes-3ddeb853845f0ea5f81878165af07bfd> (accessed: 20.08.2026).
- Council of the European Union. Council Decision (CFSP) 2026/263 of 29 January 2026 amending Decision 2010/413/CFSP concerning restrictive measures against Iran. Official Journal of the European Union. 2026. URL: <https://eur-lex.europa.eu/eli/dec/2026/263/oj/eng> (accessed: 19.08.2026)
- Harbuz (Dnipro OSINT). Russia's high-security economic zone: how Alabuga, the country's main drone factory, operates. Ukrainska Pravda. 26.05.2026. URL: <https://www.pravda.com.ua/eng/articles/2026/05/26/8036479/> (accessed: 20.08.2026)
- U.S. Department of the Treasury. Treasury Targets Networks Facilitating Illicit Trade and UAV Transfers on Behalf of Iranian Military. 25.04.2024. URL: <https://home.treasury.gov/news/press-releases/jy2295> (accessed: 19.08.2026)
- Albright D., Burkhard S., Faragasso S. Highlights of Institute Assessment of Alabuga Drone Documents, Supplied by Dalton Bennett at the Washington Post. Institute for Science and International Security. 17.08.2023. URL: <https://isis-online.org/isis-reports/highlights-of-institute-assessment-of-alabuga-drone-documents?> (accessed: 19.08.2026)
- Andreika V. Russia's Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defense Industry. Military Review. September–October 2025. URL: <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2025/Lessons-from-Ukraine/> (accessed: 19.08.2026)
- Ismay J. Russia Is Replicating Iranian Drones and Using Them to Attack Ukraine. The New York Times. 10.08.2023. URL: <https://www.nytimes.com/2023/08/10/us/russia-iran-drones-ukraine.html> (accessed: 19.08.2026)
- Burrows E., Arhirova H., Hinnant L. Operation False Target: How Russia plotted to mix a deadly new weapon among decoy drones in Ukraine. Associated Press. 26.12.2024. URL: <https://apnews.com/article/russia-ukraine-war-drones-thermobaric-bombs-decoy-2f904b04fcc5de17549415a974f5a92b> (accessed: 19.08.2026)
- Jensen B., Atalan Y. Drone Saturation: Russia's Shahed Campaign. Center for Strategic and International Studies (CSIS). 13.05.2025. URL: <https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign> (accessed: 19.08.2026)
- Landay J., Slattery G., Azhari T. Iran strikes on CIA facilities prompt questions about possible Russian role. Reuters. 22.07.2026. URL: <https://www.reuters.com/world/middle-east/iran-strikes-cia-facilities-prompt-questions-about-possible-russian-role-2026-07-22/> (accessed: 19.08.2026).
- Zelin A. Y. Iran's Support for Russia and Lessons Learned from Ukraine : testimony submitted to the Commission on Security and Cooperation in Europe (U.S. Helsinki Commission). The Washington Institute for Near East Policy. 20.04.2026. URL: <https://www.washingtoninstitute.org/sites/default/files/pdf/ZelinTestimony-20260421-Helsinki.pdf>
- Robertson N., Nakashima E., Strobel W. P. Russia is providing Iran intelligence to target U.S. forces, officials say. The Washington Post. 06.03.2026. URL: <https://www.washingtonpost.com/national-security/2026/03/06/russia-iran-intelligence-us-targets/> (accessed: 20.08.2026)
- Welsch M., Atalan Y., Jensen B., Tiersten-Nyman E. The Geography of Coercion: Russian Missile and Drone Campaigns in Ukraine. Center for Strategic and International Studies (CSIS). 07.07.2026. URL: <https://www.csis.org/analysis/geography-coercion-russian-missile-and-drone-campaigns-ukraine> (accessed: 20.08.2026)
- Bondar K. Unpacking Iran's Drone Campaign in the Gulf: Early Lessons for Future Drone Warfare. Center for Strategic and International Studies (CSIS). 10.03.2026. URL: <https://www.csis.org/analysis/unpacking-irans-drone-campaign-gulf-early-lessons-future-drone-warfare> (accessed: 20.08.2026)

Kot, Kateryna. Sabotage as a Tool of Foreign Policy: How Is Russia Testing the Limits of the West's Response?

- Rovner J., Cormac R., Maschmeyer L. Sand in the gears: Sabotage in world politics. *European Journal of International Security*. 2025. URL: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/EB1FA8B5BC7400C358EFFF2D8624B181/S2057563725100254a.pdf/sand-in-the-gears-sabotage-in-world-politics.pdf> (accessed: 20.08.2026)
- Poland blames sabotage for railway blast on Ukraine delivery line. *Associated Press*. 2025. 17 Nov. URL: <https://apnews.com/article/poland-sabotage-explosion-rail-track-warsaw-97dae3045d4e1ff329780526c6279c0f> (accessed: 19.08.2026)
- Russian Europe sabotage. *Associated Press Projects*. URL: <https://apnews.com/projects/russian-europe-sabotage/> (accessed: 20.08.2026)
- Greene S., Soldatov A., Borogan I. War Without End: Russia's Shadow Warfare. *Center for European Policy Analysis (CEPA)*. 2025. Nov. URL: <https://cepa.org/wp-content/uploads/2025/11/CEPA-War-Without-End-Russia-Shadow-Warfare-11.19.25.pdf> (accessed: 19.08.2026)
- Countering Russia's Shadow War. *Center for European Policy Analysis (CEPA)*. URL: <https://cepa.org/programs/democratic-resilience/countering-russias-shadow-war/> (accessed: 19.08.2026)
- Burrows E., Di Lorenzo S., Rasmussen S., Hamlin P. Tracked: How Russia is waging a hybrid campaign of violence and disruption across Europe. *Associated Press*. 2025. 21 Mar. URL: <https://apnews.com/article/russia-ukraine-war-europe-hybrid-campaign-d61887dd3ec6151adf354c5bd3e6273e> (accessed: 19.08.2026)
- Stewart B. Europe says Russia is ramping up a sabotage campaign. It just doesn't know how to deal with it. *CBC News*. 2025. 21 Nov. URL: <https://www.cbc.ca/news/world/russia-sabotage-europe-9.6985916> (accessed: 19.08.2026)
- Sweden's Säpo Reports That Russia Is Evolving Sabotage Tactics. *Eurasia Daily Monitor. Jamestown Foundation*. URL: <https://jamestown.org/swedens-sapo-reports-that-russia-is-evolving-sabotage-tactics/> (accessed: 19.08.2026)
- Russia's hybrid activities: EU sanctions. *European Council / Council of the European Union*. URL: <https://www.consilium.europa.eu/en/policies/sanctions-against-russia-hybrid-threats/#what> (accessed: 25.08.2026)

Lonchyna, Yuliia. When Sabotage Becomes an Attack: Does NATO Article 5 Apply to Russian Hybrid Operations?

- Charlish, A., Kelly, L., & Erling, B. (2025). Poland downs drones in its airspace, becoming first NATO member to fire during war in Ukraine. *Reuters*. Available from: <https://www.reuters.com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato-member-fire-during-war-2025-09-10/> (Accessed: 25 August 2026).
- NATO. (2021). Brussels Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels. *NATO Official Texts*. Available from: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/brussels-summit-communication> (Accessed: 25 August 2026).
- NATO. (2025). Collective defence and Article 5. *NATO Official Website*. Available from: <https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5> (Accessed: 25 August 2026).
- NATO. (2025). Countering hybrid threats. *NATO Official Website*. Available from: <https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats> (Accessed: 25 August 2026).
- NATO. (2025). Statement by NATO Secretary General Mark Rutte on the violation of Polish airspace by Russian drones. *NATO Official Transcripts*. Available from: <https://www.nato.int/en/news-and-events/events/transcripts/2025/09/10/statement> (Accessed: 15 September 2026).

- NATO. (2026). NATO Allies condemn recent airspace violations and incidents. NATO Official Articles. Available from: <https://www.nato.int/en/news-and-events/articles/news/2026/08/12/nato-allies-condemn-recent-airspace-violations-and-incidents> (Accessed: 15 September 2026).
- Reuters. (2024). Russia's suspected sabotage campaign steps up in Europe. Reuters. Available from: <https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/> (Accessed: 15 September 2026).
- Reuters. (2024). Telecoms cable linking Finland and Germany likely severed, owner says. Reuters. Available from: <https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18/> (Accessed: 15 September 2026).
- RUSI. (2026). Old ships, modern menace: How to tackle the world's shadow fleets. Royal United Services Institute. Available from: <https://www.rusi.org/explore-our-research/publications/commentary/old-ships-modern-menace-how-tackle-worlds-shadow-fleets> (Accessed: 15 September 2026).
- TVP World. (2026). Russian sabotage: Poland charges five suspects over arson of Warsaw shopping center. TVP World. Available from: <https://tvpworld.com/92425771/poland-indicts-five-over-russia-linked-shopping-mall-inferno> (Accessed: 15 September 2026).
- Ukrainska Pravda. (2025). Early estimates indicate 19 violations of Polish airspace. Ukrainska Pravda. Available from: <https://www.pravda.com.ua/eng/news/2025/09/10/7530171/> (Accessed: 15 September 2026).

Melkonova, Olena. Can the Defense Industry Become Ukraine's New Economic Specialization Within the EU?

- Forbes.ua «Єврокомісія та Міноборони України запускають програму оборонних інновацій на €161 млн», 23.04.2026. <https://forbes.ua/news/160-mln-na-tekhnologii-podviynogo-priznachennya-es-ta-ukraina-zapuskayut-novu-programu-23042026-38244>
- Кабінет Міністрів України «Україна та ЄС посилюють співпрацю з розвитку спільних оборонних проєктів», 01.04.2026. <https://www.kmu.gov.ua/news/ukraina-ta-ies-posyliuiut-spiivpratsiu-z-rozvytku-spilnykh-oboronnykh-proektiv>
- РБК-Україна «Оборонна промисловість України найкраща у світі, заявив єврокомісар», 23.06.2026. <https://www.rbc.ua/rus/news/ukrayinska-oboronka-naykrashcha-evropa-mae-1782218909.html>
- Главком «Єврокомісар назвав українську оборонну промисловість найкращою у світі», 23.06.2026. <https://glavcom.ua/world/world-politics/jevrokomisar-nazvav-ukrajinsku-oboronnu-promislovist-najkrashchoju-u-sviti-1127524.html>
- European Integration Portal «Презентована Європейська стратегія оборонної промисловості, яка передбачає активне долучення України». <https://eu-ua.kmu.gov.ua/en/news/prezentovana-yevropejska-strategiya-oboronnoyi-promyslovosti-yaka-peredbachaye-aktyvne-doluchennya-ukrayiny/>
- NDU.kr.ua «Європейська оборонна промисловість після 2022 року: нова архітектура безпеки», 03.03.2026. <https://ndu.kr.ua/960-evropejska-oboronna-promislovist-pislya-2022-roku-nova-arkhitektura-bezpeki>
- Національна поліція України «Нацполіція та СБУ викрили іранського генерала, який організував передачу росії технологій виробництва Shahed», 10.03.2026. <https://npu.gov.ua/news/natspolitsiia-ta-sbu-vykryly-iranskoho-henerala-iakyi-orhanizuvav-peredachu-rosii-tekhnologii-vyrobnystva-shahed>
- LB.ua «Аналітики США розслідують можливий зв'язок росії з ударами Ірану по об'єктах ЦРУ», 23.07.2026. https://lb.ua/world/2026/07/23/753864_reuters_analitiki_ssha.html

- 24 Канал (Економіка) «Виробництво зброї в Україні - як розвивається український ОПК». https://24tv.ua/economy/virobnitstvo-zbroyi-ukrayini-yak-rozvivayetsya-ukrayinskiy-opk_n2887633
- NV.ua «Оборонно-промисловий комплекс України — динаміка зростання та співпраця з ЄС у виробництві зброї». <https://nv.ua/ukr/ukraine/events/oboronno-promisloviy-kompleks-ukrajini-dinamika-zrostannya-ta-spivpracya-z-yes-u-virobnictvi-zbroji-50536517.html>
- РБК-Україна «Виробництво української зброї зросло у півтора рази за 2025 рік», 08.01.2026. <https://www.rbc.ua/rus/news/oboronna-promislovist-ukrayini-rik-zbilshila-1767838990.html>
- Forbes.ua «Виробництво української зброї у 2026-му може сягнути \$60 млрд», 07.11.2025. <https://forbes.ua/news/u-2026-rotsi-potuzhnosti-ukrainskogo-vpk-zrostut-mayzhe-vdvichi-lishe-dalekobiyni-sistemi-dadut-35-mlrd-prognoz-rnbo-07112025-33937>
- РНБО України «Українська оборонна промисловість: масштаб, ефективність, результат». <https://www.rnbo.gov.ua/ua/Diialnist/7384.html>
- Forbes.ua «Дрони, ракети, бронетехніка: як Україна зміцнює власний ОПК», 24.02.2026. <https://forbes.ua/war-in-ukraine/oboronna-revolyuetsiya-yak-za-tri-roki-viyni-ukraina-sformuvala-novu-viyskovu-realnist-rozpovidat-ministr-oboroni-rustem-umerov-23022025-27435>
- LB.ua «Зброя на експорт: пропозиція, попит, умови», 07.07.2026. https://lb.ua/world/2026/07/07/750102_zbroya_eksport_propozitsiya.html
- Міністерство економіки та довкілля України «Європейська програма SAFE: інтеграція українського оборонно-промислового комплексу». <https://me.gov.ua/News/Detail/83472515-ed55-4b55-90c6-d40a0627faa9?lang=uk-UA&title=Safe>
- Суспільне Новини «Оборонна програма ЄС SAFE: вже досягли повної підписки на всі 150 млрд євро», 29.08.2025. <https://suspilne.media/1102514-kreditna-oboronna-programa-es-safe-vze-dosagli-povnoi-pidpiski-na-vsi-150-mlrd-evro/>
- Forbes.ua «ЄС запускає оборонний фонд SAFE на €150 млрд: Україна зможе долучитися», 27.05.2025. <https://forbes.ua/news/rada-es-zatverdila-stvorenniya-fondu-na-150-mlrd-dlya-investitsiy-v-oboronu-shcho-tse-dast-ukraini-27052025-30062>
- Forbes.ua «ЄС розподілив €150 млрд оборонних кредитів SAFE між 19 країнами. Що отримає Україна від цього», 09.09.2025. <https://forbes.ua/news/evrokomisiya-rozdilila-150-mlrd-kreditiv-safe-na-oboronu-mizh-19-derzhavami-shcho-tse-prinese-ukraini-09092025-32490>
- Європейська правда «150 млрд євро на переозброєння: що таке SAFE і що від нього може отримати Україна», 03.09.2025. <https://www.eurointegration.com.ua/articles/2025/09/3/7219285/>
- Кабінет Міністрів України «Task Force Україна-ЄС з питань оборонно-промислового співробітництва буде інструментом залучення українського ОПК в європейську ініціативу SAFE». <https://www.kmu.gov.ua/news/task-force-ukrainaies-z-pytan-oboronno-promyslovoho-spivrobitnytstva-bude-instrumentom-zaluchennia-ukrainskoho-opk-v-ievropeisku-initsiatyvu-safe>
- NV.biz «Єврокомісія розподілила оборонні кредити між 19 країнами — на що може розраховувати Україна», 10.09.2025. <https://biz.nv.ua/ukr/economics/safe-150-mlrd-yevro-na-oboronnu-promislovist-yes-ta-spilni-proyekti-50543693.html>
- Bug.org.ua «Польща першою в Євросоюзі отримала фінансування за оборонною програмою SAFE», 30.05.2026. <https://bug.org.ua/news/polshha-pershoyu-v-yevrosoyuzi-otrymala-finansuvannya-za-oboronnoyu-programoyu-safe-1042493/>

Troian, Andrii. Ukraine's Defence Industry after the War: A Driver of Economic Development or a Temporary Advantage?

- State Concern 'Ukroboronprom'. Annual Report 2020. URL: https://ukroboronprom.com.ua/storage/documents/Report_ua.pdf (accessed: 21 August 2026).
- Harmash O. Ukraine in 'final stages' to set up three new JVs with European armsmakers. Reuters. 2024. 12 Nov. URL: <https://www.reuters.com/world/europe/ukraine-final-stages-set-up-three-new-jvs-with-european-armsmakers-2024-11-12/> (date of access: 21 August 2026).

- National Security and Defense Council of Ukraine. Ukraine's Defence Industry: Scale, Efficiency, Result. 2026. 28 Jan. URL: <https://www.rnbo.gov.ua/ua/Diialnist/7384.html> (accessed: 21 August 2026).
- Miroshnychenko B. Engineers, Incoming Strikes, and High Technology. Will Ukraine Be Able to Produce More Weapons in 2026? *Oboronka*. 2025. 26 Dec. URL: <https://oboronka.mezha.ua/yak-zroslo-virobnictvo-zbroji-ukrajini-u-2025-roci-307326/> (accessed: 21 August 2026).
- Sereda O. Ukraine's MIC Sector: What Are Its Real Achievements and Prospects? *ZN.UA*. 2026. 4 Feb. URL: <https://zn.ua/ukr/ECONOMICS/sektor-opk-ukrajini-jaki-realni-dosjahnennja-i-perspektivi-.html> (accessed: 21 August 2026).
- CES Team. August Economic Review. Special Topic: How Is Arms Production Transforming Ukraine's Economy? Kyiv: Centre for Economic Strategy, 2025. 22 p. URL: <https://ces.org.ua/wp-content/uploads/2025/08/economic-review-august-2025.pdf> (date of access: 21 August 2026).
- Trends in International Arms Transfers, 2025 / M. George et al. SIPRI Fact Sheet. Stockholm: Stockholm International Peace Research Institute, 2026. 12 p. DOI: <https://doi.org/10.55163/OSMS3959>. URL: https://www.sipri.org/sites/default/files/2026-03/fs_2603_at_2025.pdf (date of access: 21 August 2026).
- Tech Force in UA. 89% of Manufacturers Cite Security Risks as the Main Reason for Relocation—New TFUA Survey. 2025. 27 Oct. URL: <https://techforce.in.ua/news/article/golovnoyu-prichinoyu-relokaciyi-nazivayut-bezpekovi-riziki> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Share of Ukrainian Manufacturers in Procurement of Military Goods Rises to 82%. 2026. 23 Jan. URL: <https://mod.gov.ua/news/do-82-zroslo-chastka-ukrayinskih-virobnikov-u-zakupivlyah-tovariv-vijskovogo-priznachennya> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Ministry of Defence Secured More Than \$6 Billion for Ukraine's MIC in 2025. 2026. 3 Jan. URL: <https://mod.gov.ua/news/minoboroni-zaluchilo-ponad-6-mlrd-na-ukrayinskij-opk-v-2025-rocz> (accessed: 21 August 2026).
- Certain Issues Concerning International Transfers of Goods During the Period of Martial Law in Ukraine: Resolution No. 875 of the Cabinet of Ministers of Ukraine dated 1 July 2026. URL: <https://zakon.rada.gov.ua/laws/show/875-2026-%D0%BF> (accessed: 21 August 2026).
- Romaniuk R. The Cabinet of Ministers Opened Arms Exports, but Not Everyone Will Be Able to Sell, Not Everywhere, and Not Everything. What Is the Problem with the New Mechanism? *Oboronka*. 2026. 9 July. URL: <https://oboronka.mezha.ua/eksport-zbroji-z-ukrajini-yak-pracyuye-noviy-fast-track-ta-chomu-vin-ne-dlya-vsih-313057/> (accessed: 21 August 2026).
- The President of Ukraine and the Prime Minister of Denmark Signed the Drone Deal in Ankara. Official Website of the President of Ukraine. 2026. 7 July. URL: <https://www.president.gov.ua/news/v-ankari-prezident-ukrayini-j-premyer-ministerka-daniyi-pidp-105321> (accessed: 21 August 2026).
- Ministry of Defence of Ukraine. Build in Ukraine—an Initiative Facilitating the Localisation of International Companies in Ukraine. 2025. 22 Oct. URL: <https://mod.gov.ua/news/build-in-ukraine-inicziativa-yaka-spriyaye-lokalizacziyi-mizhnarodnih-kompanij-v-ukrayini> (accessed: 21 August 2026).
- Rheinmetall: A Powerful Partner at Ukraine's Side. Rheinmetall. 2023. 20 July. Updated 10 Feb. 2025. URL: <https://www.rheinmetall.com/en/media/stories/2023/rheinmetall-a-powerful-partner-at-ukraine-side> (date of access: 21 August 2026).
- High-level Delegation Visits Quantum Systems Ukraine to Witness Increased Local Manufacturing Capacity. Quantum Systems. 2025. 24 Feb. URL: <https://quantum-systems.com/news/high-level-delegation-visits-quantum-systems-ukraine/> (date of access: 21 August 2026).
- EU Military Support for Ukraine. Council of the European Union. Last reviewed 12 Aug. 2026. URL: <https://www.consilium.europa.eu/en/policies/military-support-ukraine/> (date of access: 21 August 2026).

- Ukrainian Council of Defence Industry, CORE Team. Workforce and Salaries in Ukraine's Defence Industry: Survey Results. 2026. URL: <https://drive.google.com/file/d/1DQFcIwmGwGgwiOnI1DEVXy3oEb1aEYSP/view> (accessed: 21 August 2026).
- State Employment Service of Ukraine. Employment Service Clients Use Two-Thirds of Training Vouchers for Retraining and Professional Development. Government Portal. 2026. 16 Feb. URL: <https://www.kmu.gov.ua/news/dvi-tretikh-vaucheriv-na-navchannia-kliienty-sluzhby-zainiatosti-berut-na-perepidhotovku-ta-pidvyshchennia-kvalifikatsii> (accessed: 21 August 2026).
- European Commission. Directorate-General for Research and Innovation. Support to Ukraine on Research Infrastructure Policy. Luxembourg: Publications Office of the European Union, 2025. DOI: <https://doi.org/10.2777/4728571> (date of access: 21 August 2026).
- Schmid S., Bayuputri D. Unlocking Veteran Potential: The Power of User-Validated Skill Data in Ukraine. SkillLab, 2025. 8 p. URL: <https://share.skilllab.io/hubfs/White%20Papers/Unlocking%20Veteran%20Potential%20-%20The%20Power%20of%20User-Validated%20Skill%20Data%20in%20Ukraine.pdf> (date of access: 21 August 2026).
- Improving Career Pathways and Adapting Ukrainian Veterans to Civilian Employment. Kyiv: Helvetas Swiss Intercooperation, 2025. 35 p. URL: <https://www.helvetas.org/Publications-PDFs/Eastern-Europe-Caucasus/Ukraine/1/%D0%9F%D0%BE%D0%BA%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BA%D0%B0%D1%80%E2%80%99%D1%94%D1%80%D0%BD%D0%B8%D1%85%20%D1%88%D0%BB%D1%8F%D1%85%D1%96%D0%B2%20%D1%82%D0%B0%20%D0%B0%D0%B4%D0%B0%D0%BF%D1%82%D0%B0%D1%86%D1%96%D1%8F%20%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D1%85%20%D0%B2%D0%B5%D1%82%D0%B5%D1%80%D0%B0%D0%BD%D1%96%D0%B2%20%D0%B4%D0%BE%20%D1%86%D0%B8%D0%B2%D1%96%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%BF%D1%80%D0%B0%D1%86%D0%B5%D0%B2%D0%BB%D0%B0%D1%88%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F.pdf> (accessed: 21 August 2026).
- On Approval of the Veteran Policy Strategy for the Period up to 2030 and Approval of the Operational Action Plan for Its Implementation in 2024–2027: Order No. 1209-r of the Cabinet of Ministers of Ukraine dated 29 Nov. 2024. URL: <https://zakon.rada.gov.ua/laws/show/1209-2024-%D1%80#Text> (accessed: 21 August 2026).
- On Approval of the Strategy for Establishing a System for Transitioning from Military Service to Civilian Life for the Period up to 2033 and Approval of the Operational Action Plan for Its Implementation in 2025–2027: Order No. 1350-r of the Cabinet of Ministers of Ukraine dated 31 Dec. 2024. URL: <https://www.kmu.gov.ua/npas/pro-skhhvalennia-stratehii-formuvannia-systemy-povernennia-z-viiskovoi-sluzhby-do-tsyvilnoho-zhyttia-na-period-do-2033-roku-1350r-311224> (accessed: 21 August 2026).
- On Approval of the State Target Programme 'Veteran. Work' for 2026–2027: Order No. 154-r of the Cabinet of Ministers of Ukraine dated 11 Feb. 2026. URL: <https://zakon.rada.gov.ua/laws/show/154-2026-%D1%80> (accessed: 21 August 2026).

Pomohaibo, Nazarii. Deterrence Without War: Are the Baltic States Prepared for russian Hybrid Threats?

- Lithuania closes its border with Belarus for a month. Ośrodek Studiów Wschodnich (OSW). 30.10.2025. URL: <https://www.osw.waw.pl/en/publikacje/analyses/2025-10-30/lithuania-closes-its-border-belarus-a-month>.
- Lithuania reopens border crossings with Belarus after tensions over smuggling balloons. Euronews. 19.11.2025. URL: <https://www.euronews.com/2025/11/19/lithuania-reopens-border-crossings-with-belarus-after-tensions-over-smuggling-balloons>.

- National Threat Assessment 2026 / State Security Department of the Republic of Lithuania (VSD), Defence Intelligence and Security Service under the Ministry of National Defence (AOTD). Vilnius, 2026. URL: <https://www.vsd.lt/wp-content/uploads/2026/03/2026-GR-ENG-El.pdf>.
- The Riigikogu passed constitutional amendment restricting the right to vote. Riigikogu. 26.03.2025. URL: <https://www.riigikogu.ee/en/news-from-committees/constitutional-committee/the-riigikogu-passed-constitutional-amendment-restricting-the-right-to-vote/>.
- Maruste R. Narrowing the Estonian Electorate: Excluding Russian Citizens from Local Elections Amid Security Concerns. Verfassungsblog. 25.04.2025. URL: <https://verfassungsblog.de/narrowing-the-estonian-electorate/>.
- Fremer I. Estonia: Country Amends Constitution to Restrict Local Voting Rights of Noncitizens. Global Legal Monitor / Law Library of Congress. 04.08.2025. URL: <https://www.loc.gov/item/global-legal-monitor/2025-08-04/estonia-country-amends-constitution-to-restrict-local-voting-rights-of-noncitizens>.
- Mihhail Stalnuhhin's electoral list wins most seats in Narva. ERR News. 20.10.2025. URL: <https://news.err.ee/1609834311/mihhail-stalnuhhin-s-electoral-list-wins-most-seats-in-narva>.
- Estonia's Russian speakers may determine a change in the country's policies. Veridica. 28.10.2025. URL: <https://www.veridica.ro/en/opinions/estonias-russian-speakers-may-determine-a-change-in-the-countrys-policies>.
- Court overturns decision to ban TV Rain in Latvia. Latvijas Sabiedriskais medijs (LSM). 16.07.2025. URL: <https://eng.lsm.lv/article/features/media/16.07.2025-court-overturns-decision-to-ban-tv-rain-in-latvia.a606973/>.
- Latvian media watchdog appeals against court overturning TV Rain license ban. Latvijas Sabiedriskais medijs (LSM). 21.08.2025. URL: <https://eng.lsm.lv/article/features/media/21.08.2025-latvian-media-watchdog-appeals-against-court-overturning-tv-rain-license-ban.a611177/>.
- Estonian in Name, Russian Content: How the Pravda Network Brings Telegram Propaganda into Estonia's Information Space. Propastop. 04.08.2026. URL: <https://www.propastop.org/en/2026/08/04/estonian-in-name-russian-content-how-the-pravda-network-brings-telegram-propaganda-into-estonias-information-space/>.
- Portal Kombat : un réseau structuré et coordonné de propagande prorusse / VIGINUM ; Secrétariat général de la défense et de la sécurité nationale. Paris, 2024. URL: <https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse>.
- Bentzen N. The European Democracy Shield: An overview. European Parliamentary Research Service. 15.01.2026. URL: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATA\(2026\)782603_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782603/EPRS_ATA(2026)782603_EN.pdf).
- The new European Centre for Democratic Resilience starts its work / European Commission. 24.02.2026. URL: https://enlargement.ec.europa.eu/news/new-european-centre-democratic-resilience-starts-its-work-2026-02-24_en.
- Special EP committee adopts proposals to improve the European Democracy Shield. Insight EU Monitoring. 23.06.2026. URL: <https://ieu-monitoring.com/editorial/special-ep-committee-adopts-proposals-to-improve-the-european-democracy-shield/1243859>.
- Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act / European Commission. 24.10.2025. URL: <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktok-and-meta-breach-their-transparency-obligations-under-digital>.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). Official Journal of the European Union. L 277. 27.10.2022. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.
- The DSA supervision and enforcement architecture. DSA Observatory. 24.06.2022. URL: <https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/>.
- Putting collective intelligence to the enforcement of the Digital Services Act. arXiv:2305.01959. 2023. URL: <https://arxiv.org/pdf/2305.01959>.

- Annual Report on the Activities of Latvian State Security Service (VDD) in 2025 / Valsts drošības dienests. Rīga, 2026. URL: <https://vdd.gov.lv/uploads/materials/42/en/annual-report-2025.pdf>.
- International Security and Estonia 2026 / Välisluureamet (Estonian Foreign Intelligence Service). Tallinn, 2026. URL: <https://valisluureamet.ee/doc/raport/2026-en.pdf>.
- €120 million later: the DSA enters the enforcement phase. MediaLaws. 23.12.2025. URL: <https://www.medialaws.eu/e120-million-later-the-dsa-enters-the-enforcement-phase/>.
- DSA enforcement in practice: from rules to commitments and fines / Loyens & Loeff. 10.06.2026. URL: <https://www.loyensloeff.com/insights/news-events/news/dsa-enforcement-in-practice-from-rules-to-commitments-and-fines/>.
- Commission opens formal proceedings against TikTok on election risks under the Digital Services Act / European Commission. 17.12.2024. URL: <https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act>.
- TikTok and the Romanian elections: A stress test for DSA enforcement. DSA Observatory. 20.12.2024. URL: <https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/>.
- https://icds.ee/static/20260823_aaa_u101_112-1024x683.jpg.webp

Photos and Images

- <https://s.rfi.fr/media/display/3fe40194-990c-11ef-9cfc-005056bfb2b6/w:1024/p:16x9/AP18193379795077.jpg>
- https://www.theparliamentmagazine.eu/siteimg/news-main/ugc-1/fullnews/news/25821/25836_original.jpg
- https://static.ukrinform.com/photos/2019_10/thumb_files/630_360_1572357882-410.jpg
- https://upload.wikimedia.org/wikipedia/commons/a/ac/Ottawa_Treaty_members.svg?utm_source=en.wikipedia.org&utm_campaign=index&utm_content=original
- <https://defence-ua.com/media/contentimages/d0d66f951f6e2d3b.jpg>
- https://commission.europa.eu/sites/default/files/styles/oe_theme_medium_no_crop/public/2025-03/EU%20preparedness%20union%20strategy%20Card.jpg?itok=r39Ql4S1
- https://www.airbus.com/sites/g/files/jlcbta136/files/styles/w780h520/public/2022-06/FCAS%20Poster%20GOOSE_Janes-Magazin_PRINT.JPG?itok=iPe2eIY6
- <https://ecfr.eu/wp-content/uploads/2026/07/605619359-scaled.jpg>
- https://cdn.prod.website-files.com/60a3c1fc44c5715c395770e7/60df8191a884c0804de8b15d_Depositphotos_24064653_1-2015.webp
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTa-MF6MOavGuN6g8GK24PZ9BttMBLJ7WFGm_zRh_gDW4fGn8kjdoob1pI&s=10
- https://www.economist.com/cdn-cgi/image/width=1424,quality=80,format=auto/content-assets/images/20241116_EUP507.jpg
- https://cdn.prod.website-files.com/63b303944d1e9ec09b741257/64d3b06822a0befce2eb1d96_max-kukurudziak-qbc3Zmxw0G8-unsplash-min.jpg
- [Φoro: https://www.president.gov.ua/storage/j-image-storage/50/56/89/a0b555e83b7d8e55725771f9ed9a5ea2_1750886062_extra_large.jpeg](https://www.president.gov.ua/storage/j-image-storage/50/56/89/a0b555e83b7d8e55725771f9ed9a5ea2_1750886062_extra_large.jpeg)
- https://www.atlanticcouncil.org/wp-content/uploads/2024/10/2024-06-19T120819Z_1029865475_RC2AE8A9I464_RTRMADP_3_NORTHKOREA-RUSSIA-scaled.jpg
- <https://cdn.britannica.com/43/3843-050-FEE525C7/Russia-political-map.jpg>
- https://cdn.ceps.eu/2025/11/P-068228_00-19_01-ORIGINAL-948002.jpg.webp
- https://www.president.gov.ua/storage/j-image-storage/51/45/57/caab1d58009ba1ed20ec9774418b6a0e_1755439697_extra_large.jpeg
- https://www.europarl.europa.eu/resources/library/images/20220202PHT22410/20220202PHT22410_original.jpg
- https://img.lemde.fr/2026/06/19/0/0/3662/2441/664/0/75/0/775d2bb_ftp-1-q5yllwslcrys-6377dbc29f534386b7ac3ed7f025ab47-0-48cde7cb006140508c60d2dcfa5ff34b.jpg
- https://energytransition.org/wp-content/uploads/2025/04/shutterstock_2052065705-scaled.jpg
- <https://www.aeaweb.org/content/file?id=11680>
- <https://financialcrimeacademy.org/wp-content/uploads/2022/07/2-15-1024x576.jpg>
- <https://www.reuters.com/resizer/v2/7CNCZIOHHROT3AY3EZZMIKC66M.jpg?auth=0a15a1f9d0c9325b7dfb5e957a59f0896d1ac5eddf89eab6e0be0d066d65d238&width=1920&quality=80>
- https://cepa.org/wp-content/uploads/2025/12/2025-04-11T131153Z_1076526061_MT1SCPXB11EV11APR25A10_RTRMADP_3_VESSELS-KIWALA-AND-KURVITS-ON-THE-SEA-scaled.jpg
- <https://www.euractiv.com/content/uploads/sites/2/2025/08/13296722-e1756697742803.jpg>
- https://www.nato.int/content/dam/nato/webready/news/2020-2029/2026/07/07/summit-hosg-reception/20260707_summit-hosg-reception_0007.jpg/jcr:content/renditions/cq5dam.web.1280.1280.jpeg
- <https://www.politico.eu/cdn-cgi/image/width=965,height=643,fit=crop,quality=80,onerror=redirect,format=auto/wp-content/uploads/2020/10/GettyImages-1199162894.jpg>
- https://cdn.unitycms.io/images/CdGslVwsamBB_aTWO6X4gn.jpg

UDONATION



udonation.org



+38(068)0042001



info@udonation.org



53 Vasyl Tyutyunnyk Street,
Office 23, Kyiv, Ukraine

