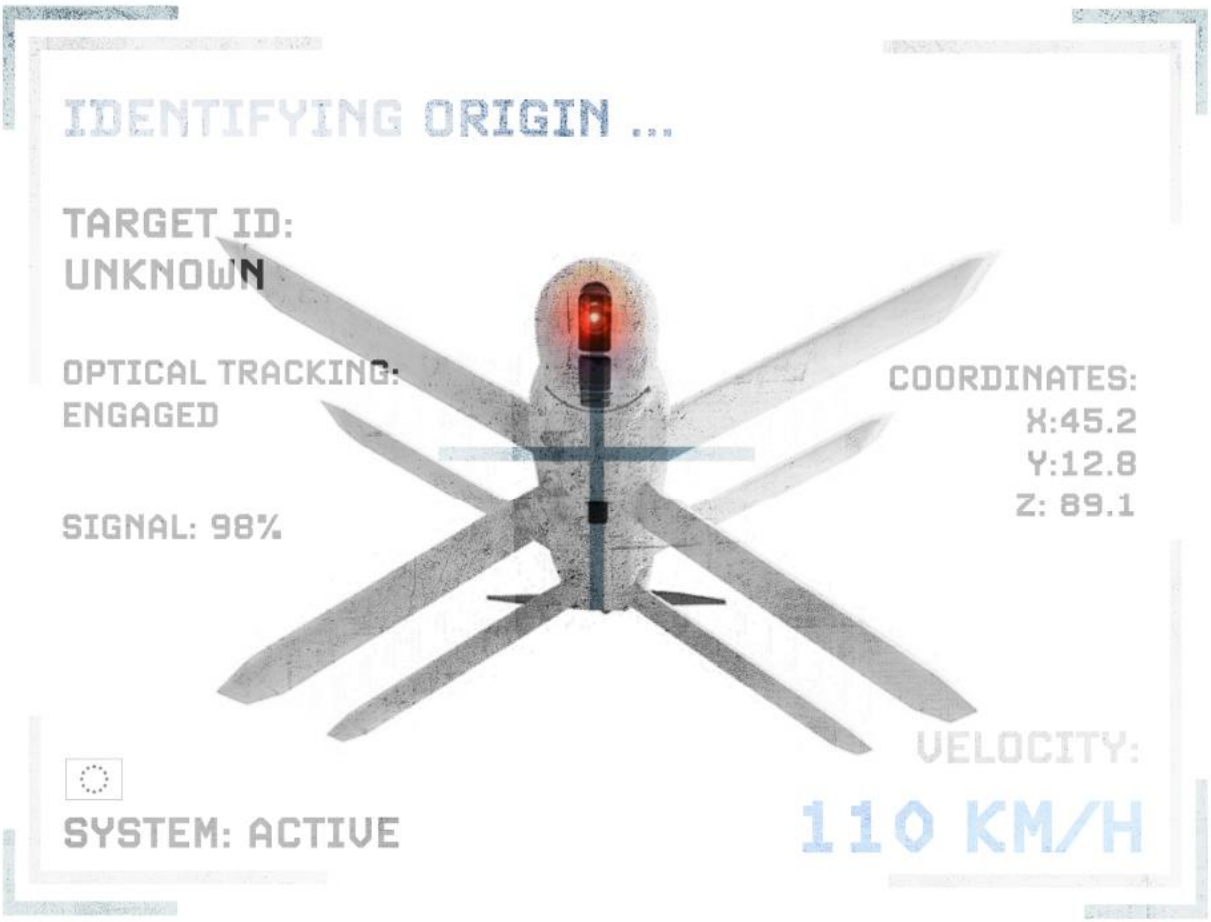
Wilfried
Martens Centre
for European Studies

Strengthening European Societal Resilience Under Russian Hybrid Pressure:

Lessons from Ukraine

Maksym Beznosiuk



July 2026

Strengthening European Societal Resilience Under Russian Hybrid Pressure: Lessons from Ukraine

Maksym Beznosiuk

1 Introduction

Russia's war against Ukraine has demonstrated the Kremlin's growing focus on targeting societal resilience rather than military forces alone. In Ukraine, since 2014, the Kremlin has deployed a broad spectrum of hybrid tools, including disinformation, cyber disruption, and sabotage, later supplemented by sustained missile and drone attacks on civilian infrastructure alongside conventional military operations (Beznosiuk, 2025h; Beznosiuk, 2025e; Jensen & Atalan, 2025). What Moscow initially used at the tactical level has evolved into a sustained, industrial-scale system aimed at exerting continued pressure on Ukrainian critical infrastructure and the civilian population (Beznosiuk, 2025d; Adams, 2025).

Within this broader hybrid toolkit, sustained missile and drone attacks have emerged as one of the most socially disruptive and least prepared-for elements of Russian strategy (Beznosiuk, 2025e). Ukraine's experience shows how repeated aerial strikes, alerts, blackouts, and infrastructure disruptions impose continuous pressure on daily life, governance, and public trust (Beznosiuk, 2025g). Even where military defences mitigate physical damage, Ukraine remains exposed to prolonged disruption, uncertainty, and fatigue (Shchyrba, O. 2024).

In Europe, the Kremlin has used its hybrid toolkit, including a recent wave of drone penetration of European airspace below formal escalation thresholds aimed at undermining social cohesion and support for Ukraine (Beznosiuk, 2025f; Racicot, 2026). The Kremlin deliberately leverages hybrid tools to place sustained pressure on civilian endurance, societal adaptation, and governance, posing grave challenges not only for Ukraine but also for Europe (Beznosiuk, M. 2025j). Ukraine's experience indicates that prolonged Russian drone pressure is likely to remain a long-term security threat for the entire European continent (Beznosiuk, M. 2025b). These attacks interact with disinformation, cyber incidents, and sabotage, amplifying fear, uncertainty, and political hesitation (Urbancik, J. 2026).

The recent wave of hybrid incidents across Europe, including sabotage, disinformation campaigns, and airspace intrusions, has revealed persistent vulnerabilities (Beznosiuk & Dixon, 2026). Among them are uneven preparedness, fragmented crisis management, and limited political awareness of societal resilience as a security issue, particularly given that escalation can occur below the threshold of conventional military attack and with little warning (Tessari, 2026; Beznosiuk & Dixon, 2025). The challenge for Europe is therefore not only one of national preparedness, but also of coordination, shared threat recognition, and institutional alignment in response to transnational hybrid pressure.

As European debates increasingly focus on hybrid threats and democratic resilience, there is a clear need to examine how societal vulnerabilities are targeted, how Russia combines and adapts different hybrid tools, and why Russian aerial pressure is especially disruptive. Addressing both the nature of the attacks and the measures required to enhance resilience is essential to strengthening Europe's societal preparedness and its ability to sustain the functioning of critical infrastructure, public authorities, and society at large under prolonged hybrid pressure from Russia.

This paper will examine how Russia deliberately targets societal vulnerabilities as part of its hybrid strategy, with sustained aerial pressure emerging as one of the most socially disruptive components of this toolkit. Using Ukraine's experience as a case study, the paper will assess what this reveals about Europe's societal vulnerabilities and exposure to hybrid pressure, particularly aerial hybrid threats, and identify key measures to enhance European societal resilience and coordination.

This paper will be based on a qualitative analysis of primary and secondary sources, including Ukrainian government data, EU and member-state policy documents, think tank research, academic literature, and open-source reporting.

2 How Russia Targets Societal Vulnerabilities

The Kremlin's evolving hybrid strategy towards Ukraine and Europe reflects a well-coordinated effort that combines disinformation, cyber disruption, sabotage, coercive signalling, and drone usage to weaken societal resilience over time while also exerting cumulative pressure on public authorities, critical infrastructure, and civilian morale.

Since the early 2000s, the Kremlin has refined its hybrid warfare toolkit in Ukraine and now applies it more broadly across Europe. Since 2022, the Russian hybrid warfare campaign has extended beyond Eastern Europe into the Nordics, the Balkans, and Southern Europe, with the Kremlin adapting its tactics to local vulnerabilities while pursuing the same broader objective of weakening democratic cohesion and Euro-Atlantic unity (Stradner & LaBelle, 2025; Blewett-Mundy & Beznosiuk, 2025; Beznosiuk, 2025l; Beznosiuk, 2025f).

With Russia's conventional military options narrowing in 2026 due to economic constraints, less expensive hybrid warfare tools become Russia's affordable escalation instrument, allowing it to impose sustained pressure on Europe without direct military escalation (Dixon & Beznosiuk, 2025).

The Kremlin has increasingly used proxies, criminal intermediaries, covert sabotage, cyberattacks, and information operations to exert pressure on political institutions and societies, complicating attribution and political responses (Rekawke et al., 2025; Bowser, D. 2025). In Europe, the Kremlin has skilfully utilised fragmented responses from separate governments that treat many of its hybrid attacks as isolated incidents rather than as components of a broader strategic campaign across the continent. As a result, Moscow was able to increase the number of sabotage operations across Europe by fourfold in 2024 compared to the previous year, with the surge accelerating into 2025 and 2026 (Beznosiuk & Dixon, 2026; Jones, 2025).

Ukraine's post-2022 experience demonstrates that Moscow pursues not just the targeting of assets or battlefield gains, but increasingly the degradation of conditions that allow Ukrainian society to function, adapt, and sustain resilience under constant pressure (Beznosiuk, M. 2025, Beznosiuk & Dixon, 2026).

Within this broader hybrid toolkit, missile and drone attacks have emerged as one of the most socially disruptive components of the evolving Russian hybrid strategy (Beznosiuk, M. 2025b). In Ukraine, repeated aerial strikes, prolonged alerts, and infrastructure disruptions have led to interruptions in the daily lives of Ukrainians, businesses, and public institutions, exerting extra mental pressure as well (Teach for Ukraine, 2026). While Ukraine has managed to develop a multi-layered air defence system that neutralises most Russian drones and rockets, this has not eliminated the broader social effects of repeated disruptions to businesses and everyday life.

Russia's use of drones has evolved into a more structured doctrine supported by industrial expansion, tactical adaptation, and broader hybrid objectives. The September 2025 drones flying into Poland and Romania demonstrated a turning point in the escalation between Russia and Europe. These recent incidents suggest that the Kremlin's drone campaign is increasingly evolving into a transnational hybrid strategy directed at Europe as much as Ukraine itself (Beznosiuk, M. 2025d). Moscow's objective is to integrate drones into a central pillar of its war economy and wider hybrid coercion model.

The Kremlin has focused on training up to 1.5 million new operators and leveraging cheap drones and decoys to force Ukraine to expend costly interceptors while degrading its infrastructure and undermining social cohesion (Nikolov, 2025). Russia's drone warfare component of the new hybrid doctrine should be viewed as a resilience challenge because it connects battlefield adaptation with social pressure.

Russia seeks to exploit the gap between what societies can absorb temporarily and what they can sustain over time. In Ukraine, this has meant targeting energy and transportation infrastructure (Dixon & Beznosiuk, 2026). In Europe, similar pressure has already taken the form of unidentified drones disrupting airport operations or hovering over critical facilities. The Kremlin's ultimate objective is to weaken social cohesion, increase political divisions, undermine support for Ukraine, and test whether European governments can maintain the stability and functioning of their societies under persistent, sub-threshold hybrid attacks.

3 From Ukraine to Europe: Societal Stress Under Hybrid Pressure and Preparedness Gaps

3.1 Societal Stress Under Sustained Hybrid Pressure in Ukraine

Ukraine's experience demonstrates that Russian hybrid warfare activities have an impact that goes beyond immediate physical destruction by causing repeated alerts, energy blackouts, interrupted schooling, and transport disruption. In practice, this has meant that daily life in Ukraine has been reorganised around the anticipation of disruption (Tarasova-Markina & Kottasová, 2025). Ukrainians are constantly facing

repeated alerts that interrupt their work, commuting, schooling, and access to public services. This takes a mental toll and leads to economic losses.

The Kremlin's objective is to continuously destabilize societal functioning and undermine social cohesion and public trust, making resilience and continuity of societal functioning essential under sustained hybrid stress.

The Kremlin's aerial pressure is particularly detrimental, as it constantly blurs the line between emergency and routine, forcing Ukrainians to adapt their work, travel, sleep, education, and services to constant alerts. This situation leads to cumulative mental pressure and fatigue, as well as additional pressure on public authorities who must ensure proper communication, protection, and the functioning of society.

3.2 Uneven Protection, Civilian Adaptation, and Social Resilience

Ukraine's experience also stresses the importance of ensuring proper protection for all societal groups. Ukrainian authorities have struggled since 2022 to ensure the functioning of shelters, digital alerts, backup power for critical infrastructure, transport alternatives, and psychosocial support for all Ukrainians, especially vulnerable groups (Mikhailov, 2024; Ukrinform, 2024). There are still challenges with proper shelter infrastructure, inclusivity of support for these groups, and mental health support for those affected by sustained aerial attacks (Lubinets, D. 2025; Center for Civil Liberties, 2024). In particular, Ukraine demonstrates unequal access to shelter infrastructure, with many shelters listed on paper but unusable in practice. Inspections identify the absence of ramps, handrails, and even sufficient space for disabled people and caregivers with children (Chernysh, O. 2024).

Ukraine shows that civilian adaptation under repeated societal disruption doesn't automatically amount to resilience. European societies can learn to function under prolonged hybrid attacks. However, without structured support, clear communication, and inclusive protection systems, such adaptation is likely to remain uneven and fragile over the long term.

3.3 Europe's Exposure and Emerging Responses

The Kremlin's increased hybrid pressure on Europe is already visible in sabotage, cyber operations, undersea infrastructure incidents, GPS interference, and drone-related airspace intrusions (Rosenbach et al., 2026; "Kremlin Narratives", 2025). These incidents extend from NATO's eastern flank to the Nordic countries, Southern Europe, and the Balkans, with the Kremlin adapting its tactics to each region's vulnerabilities (Beznosiuk, M. 2025k, Beznosiuk, M. 2025f). In the Nordics, this has taken the form of undersea cable disruption, GPS jamming, and AI-enabled information manipulation, while Central and Eastern Europe has experienced sabotage, arson, and cyberattacks (Beznosiuk, M. 2025k, Beznosiuk, M. 2025c). In turn, countries in the Balkans and Southern Europe have increasingly experienced disinformation campaigns and infrastructure-related disruptions (Beznosiuk, M. 2025c; Blewett-Mundy & Beznosiuk, 2025)

Simultaneously, drone incursions into European airspace since September 2025 should be viewed as deliberate probing of European readiness rather than accidental spillovers (Souverbie, 2025). This, combined with sabotage cases linked to Russian networks and GPS jamming across parts of Europe, demonstrates that the coercive infrastructure that has been applied in Ukraine is actively spilling over into Europe (Beznosiuk, 2025d).

This situation demonstrates that European countries are not facing isolated hybrid challenges emanating from Moscow, but rather a broader hybrid warfare campaign aimed at destabilising democratic cohesion, testing deterrence, and exploiting regional asymmetries. For the Kremlin, Ukraine has functioned as a live testing ground for coercive hybrid tools that Moscow can later utilise in Europe to destabilise its democratic societies, undermine social and political cohesion, and erode support for Ukraine (Beznosiuk & Dixon, 2026). What Ukraine is currently experiencing is already exposing Europe's own structural vulnerabilities.

At the same time, the EU has increasingly acknowledged hybrid threats, critical infrastructure resilience, foreign information manipulation and interference, and civil preparedness as emerging security concerns.

In recent years, the EU has introduced a series of relevant policy instruments and resilience initiatives. These steps indicate that the EU has started addressing the

evolving threat environment. Still, they have not yet yielded a sufficiently coherent Europe-wide approach to societal resilience under prolonged hybrid pressure. To address this challenge, the EU leadership took an important step by launching the 2025 Preparedness Union Strategy to enhance Europe's capability to prevent and respond to emerging threats, including hybrid threats, through an integrated, all-hazards, whole-of-government, and whole-of-society approach (European Commission, 2025).

This strategy emphasizes protecting essential societal functions, such as hospitals, schools, transport, and telecommunications, while also proposing stronger crisis coordination through an EU Crisis Hub, regular EU-wide preparedness exercises, and enhanced civil-military cooperation. Still, this strategy remains quite broad, and without more precise prioritisation and closer alignment with national systems, it risks becoming more procedural than operational across member states with different preparedness cultures, capabilities, and threat perceptions (Quis & Buldioski, 2025).

Another important step was the presentation of the European Democracy Shield in November 2025, which set out a wider whole-of-society approach not only to countering information manipulation and disinformation but also to strengthening resilience across the EU (European Commission, 2025).

As a key component under this initiative, the European Centre for Democratic Resilience started work in February 2026 to improve coordination among EU institutions, EU member states, and civil society in response to threats to democratic systems (European Commission, 2026). Although it is still in its early stages, its launch demonstrates growing recognition at the EU level that stronger coordination, situational awareness, and resilience-building are required to reduce fragmentation and bolster democratic resilience **(**European Commission, 2026).

The Council's conclusions of 16 March 2026 further reinforced the importance of advancing the EU's capacity to counter hybrid threats (Council of the European Union, 2026). These conclusions openly condemned sabotage, cyberattacks, foreign information manipulation and interference, election interference, and attacks on critical infrastructure, while reaffirming the EU's determination to use all available instruments to prevent, deter, and respond. Importantly, the conclusions also directly identified

Russia and its proxies as malign actors behind coordinated hybrid campaigns across EU member states (Council of the European Union, 2026).

However, EU governments still struggle to coordinate their cross-border responses to hybrid incidents, with several critical vulnerabilities stemming from misaligned legal authorities, counterintelligence practices, and information-sharing arrangements (Harvard Kennedy School, 2026).

3.4 Preparedness and Coordination Gaps Across Europe

The Ukrainian experience demonstrates that the real challenge is not a single emergency but prolonged disruption affecting the whole of society. It also underscores the importance of maintaining the continuity of critical services and institutions, including in education, healthcare, and local administration, amid regular disruptions.

Currently, many European civil protection systems, alert systems, healthcare infrastructure, and public services are designed to absorb one-off emergencies rather than sustained hybrid pressure (Beznosiuk & Dixon, 2026). Moreover, this situation is aggravated by the fact that European responses have often remained reactive, fragmented, or confined to single domains, while the Kremlin operates across sectors and adapts its hybrid tactics quickly.

Europe has also been very slow to develop credible hybrid deterrence, and the failure to establish clear thresholds for grey-zone attacks has created a gap that the Kremlin continues to exploit into 2026 (Dixon & Beznosiuk, 2025).

More broadly, Europe's civil protection architecture remains poorly suited for prolonged coercion. Decades of post-Cold War demobilisation have left major European states with minimal shelter capacity, limited continuity planning, and a crisis-response culture oriented toward short-term emergencies rather than sustained hybrid pressure (Beznosiuk & Dixon, 2026).

Furthermore, Europe is highly vulnerable due to the state of its critical infrastructure. Much of Europe's electricity, transport, and water infrastructure is ageing, underinvested, and still reliant on legacy systems or outdated software (Edwards C, 2025). As a result, this situation poses severe physical and cyber vulnerabilities that Russia has already exploited on numerous occasions. In particular, transport networks, especially railways, are highly exposed not merely because they are

interdependent or old, but also because of their strategic importance to military mobility and to NATO's support to the eastern flank (Edwards C, 2025; Livermore, D. 2024). At the same time, a substantial portion of critical infrastructure remains privately owned or operated, while fragmented standards and uneven regulatory approaches across EU member states continue to hinder the development of a more coherent and robust resilience (Livermore, D. 2024).

In such conditions, warning systems, shelters, rapid repair capacity, emergency communications, and public information can't be treated as separate national challenges. Instead, they should form part of a wider resilience architecture that should be coordinated more effectively across Europe.

The January emergency crisis in Berlin illustrates the fragility of the European resilience system under prolonged disruption. In January 2026, an attack on high-voltage power cables in Berlin left over 100,000 residents across several districts in the south-west of the city without electricity and heating for nearly a week amid sub-zero temperatures (Cole, D. 2026). This led to cascading failures across healthcare, transport, and communications segments (Tanno, Shukla, & Kappeler, 2026). This prompted the German government to adopt emergency legislation to strengthen critical infrastructure (Agence France-Presse, 2026). Yet this emergency in Berlin also showed how quickly public services and social trust can erode when disruption persists beyond initial response capacity.

A recent attempted coordinated cyberattack on Polish energy infrastructure in December 2025 further demonstrates how Moscow can design hybrid operations to undermine societal resilience through civilian disruption (Ministry of Digital Affairs, Poland,2025). The cyberattack targeted a large, combined heat and power plant serving nearly half a million customers (Todorow, A. 2026). Had it succeeded, a major urban population could have lost heating during one of the coldest periods of the year. Investigators later found that Russia planned this intrusion for several months through reconnaissance, stolen credentials, and destructive malware (Petriczko, A. 2026). This case shows that Russian-linked hybrid activities can aim not only to disrupt infrastructure, but also to strain emergency response systems and erode public confidence by targeting the systems that sustain daily social functioning.

In particular, Europe's vulnerability is amplified by the high level of integration of its electricity system. The interconnected EU power grid implies a high likelihood that disruptions in one member state will have cross-border impacts, especially with shared bidding zones (Ebere et al., 2025). In contrast, operational responses and grid stabilisation measures remain mainly organised at the national or bilateral level (Ebere et al., 2025).

The main lesson is that Europe's vulnerability lies not only in what individual member states lack materially but also in the fragmentation between them. Unless European states and institutions respond more holistically, Moscow will continue exploiting the gaps between legal, military, informational, and civil protection thresholds. This creates a structural asymmetry that Russia is well-positioned to exploit through sustained disruption that exhausts institutional responses and undermines social cohesion over an extended period.

Unless Europe develops a more coherent response, the Kremlin will continue with its efforts to fracture European unity through a thousand cuts rather than through confrontation (Dixon & Beznosiuk, 2025).

Hybrid threats are increasingly cross-national in their impact and could lead to infrastructure disruptions, economic and social challenges across Europe. Hence, it becomes critical to ensure stronger cross-border coordination, threat detection, and a more coherent understanding of societal resilience as a component of the security framework.

4 Key Recommendations to Enhance European Societal Resilience

4.1 Treat social resilience as a security component

European countries should treat societal resilience not as a secondary civil protection issue but as a core component of national and European security. Ukraine's experience demonstrates that Russia targets critical systems that underpin societal functioning, necessitating a more direct incorporation of societal resilience into national security strategies, defence planning, and critical protection frameworks, as

well as into policy frameworks on civil protection, democratic resilience, and countering hybrid threats.

Both national authorities and EU institutions should work together to bolster energy preparedness and develop contingency plans for cascading disruptions that could span several countries simultaneously. To this end, they should conduct regular stress tests for power outages and infrastructure failures.

4.2 Strengthen preparedness for prolonged aerial and infrastructure disruption

EU member states should work to develop preparedness systems capable not only of responding to one-off emergencies but also of sustaining societal functioning under prolonged and repeated aerial disruption. This approach would require expanding the network of accessible shelters, developing continuity plans, and improving backup power for hospitals, public transport, water systems, and digital infrastructure.

It is also critical to have rapid repair capabilities, spare components, and repair teams ready for rapid deployment to minimise recovery time after repeated hybrid incidents or strikes. Furthermore, relevant public authorities responsible for shelters should regularly inspect them to assess accessibility and suitability for people, particularly vulnerable groups such as older adults and people with disabilities who may face challenges accessing and using them. Also, respective national authorities should develop an appropriate responsibility chain, with each shelter having a designated operator, an access mechanism, and a readiness checklist.

EU member states should also extend preparedness efforts to municipalities and regional operators of essential civilian services, including heating and local energy infrastructure, which may remain highly vulnerable despite their significance to societal functioning. In this regard, EU member states should pay particular attention to transport infrastructure, especially rail networks, whose fixed routes and reliance on signalling and control systems make them especially vulnerable to sabotage and cyber disruption. This would require stronger physical protection of key nodes, improved cybersecurity for transport control systems, better real-time monitoring, and contingency planning for rapid repair and service restoration.

They should also draw lessons from the Nordic and Baltic countries' experience in bridging the gap between the state and individuals by linking civil preparedness, volunteer-based local networks, and territorial defence planning (CEPS, 2026). This would strengthen societal resilience under prolonged hybrid pressure.

4.3 Strengthen crisis communication, information resilience, and psychological preparedness

European governments should respond to Russian information manipulation efforts by investing in long-term programmes that strengthen media literacy and independent journalism across the continent. It is equally crucial to implement independent, politically neutral educational campaigns for European citizens, including approaches inspired by the Swedish model of psychological defence, to build resilience against Russian manipulation in Europe (Beznosiuk, M. 2025c).

It is imperative to support preventive, non-partisan communication activities, especially during elections and times of crisis. Such efforts could pre-empt and counter Russian attempts to spread its anti-European and anti-Ukrainian narratives before they gain traction. For example, public institutions could run pre-bunking campaigns to explain common Russian disinformation and manipulation techniques. At the same time, relevant national authorities across EU member states could ensure the rapid public attribution of coordinated information manipulation campaigns.

Governments should also incorporate psychosocial support more closely into emergency preparedness, including for communities likely to be more exposed to repeated alerts and mental stress under sustained hybrid pressure, such as aerial attacks.

4.4 Raise the costs of sabotage, coercion, and other hybrid activities

European countries should treat sabotage and other hybrid operations as hostile-state activities and develop clear and timely countermeasures when such incidents occur. While recent EU sanctions introduced notification requirements for Russian diplomatic travel, these measures have proven insufficient to disrupt operational support for intelligence and sabotage activities (Council of the EU, 2025).

European countries should tighten restrictions on the movement of Russian diplomatic staff and strengthen coordination and information sharing on counterintelligence among relevant national agencies. At the same time, European countries must raise costs for Russia by targeting its shadow fleet, sanctioning third-country enablers, and disrupting GRU-linked networks.

4.5 Build stronger European coordination and resilience-based deterrence

Russia is actively exploiting the uncertainty created by Europe's lack of a coordinated response to hybrid activities. The lack of clear thresholds and high-level European guidance on adequate and timely responses enables the Kremlin to wage its air and maritime incursions without substantial risk, test red lines, increase political hesitation, and undermine confidence in Europe's ability to defend itself.

Thus, European leaders should actively work to establish clear red lines on hybrid threats and coordinate responses. The EU should also work closely with NATO to develop a joint NATO-EU approach to evolving Russian hybrid threats that reflects a multi-domain approach. In particular, European States and NATO should work to establish clear, realistic rules of engagement for cross-border drone and airspace incursions to reduce ambiguity, bolster deterrence, and improve response coordination (Beznosiuk, M. 2025f).

European countries should also work to define clearer thresholds and consequences for systematic information manipulation targeting elections, public trust, and social stability, so that the Russian pattern of repeated cognitive attacks remains neither cost-free nor unaddressed (Dixon & Beznosiuk, 2025).

EU member states should treat attribution as only a first step and follow it with clearer thresholds for consultation and a standing set of response options, coordinated through NATO, for hybrid attacks that endanger lives or cause serious damage to critical infrastructure (Harvard Kennedy School 2026). This would require closer cross-border coordination among civilian, intelligence, law enforcement, and defence agencies to enable earlier identification and disruption of Russian grey-zone operations in Europe.

5 Conclusion

Russia's war in Ukraine has demonstrated that Moscow aims to degrade the societal conditions that allow efficient functioning of state authorities and society as a whole. By leveraging such hybrid warfare tools as sabotage, cyber disruption, disinformation, and sustained missile and drone attacks, the Kremlin has aimed to exhaust Ukrainian societal resilience, disrupt governance and social cohesion over an extended period. Ukraine's experience demonstrates that the effects of such pressure reshape daily life, impact businesses, deepen inequalities in protection, and test society's long-term capacity to adapt under constant military and hybrid pressure.

For Europe, the primary lesson is that societal resilience cannot be treated as a secondary issue of civil protection alone but must be understood as a core component of security policy. Recent Russian hybrid activities across Europe, along with vulnerabilities exposed by ageing infrastructure, fragmented preparedness, and uneven coordination at the EU level, demonstrate that Ukrainian challenges are already being experienced in Europe as well.

The EU and its member states have begun introducing new measures to address those gaps. However, important gaps remain and will require not just better preparedness and stronger coordination. European leaders should change their mindset from reacting to isolated incidents to preparing European societies to withstand prolonged hybrid pressure. That would require integrating societal resilience more directly into security planning, infrastructure protection, upgrades to the shelter network, and cross-border coordination.

Bibliography

Adams, P. (2025, July 10). Russia's intensifying drone war is spreading fear and eroding Ukrainian morale. *BBC News*. https://www.bbc.com/news/articles/c0m8gn7grn2o

Beznosiuk, M. (2025a, December). A new axis of disinformation: What Europe must do now. *ISPI*. https://www.ispionline.it/en/publication/a-new-axis-of-disinformation-what-europe-must-do-now-225219

Beznosiuk, M. (2025b). From drones to doctrine: Why Russia's air war in Ukraine is a warning for Europe. *Thai Journal of National Interest, 6*(2). https://sc01.tci-thaijo.org/index.php/NIT/article/view/241654

Beznosiuk, M. (2025c, July 31). How the Kremlin disruption across CEE and the Western Balkans. *Visegrad Insight*. https://visegradinsight.eu/how-the-kremlin-refines-disruption-across-cee-and-the-western-balkans/

Beznosiuk, M. (2025d, October 16). Kremlin's drone surge in 2025 and its hybrid threat to Ukraine and Europe. *New Eastern Europe*. https://neweasterneurope.eu/2025/10/16/kremlins-drone-surge-in-2025-and-its-hybrid-threat-to-ukraine-and-europe/

Beznosiuk, M. (2025e, July 8). Putin is winning the drone war as Russia overwhelms Ukraine's defenses. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/putin-is-winning-the-drone-war-as-russia-overwhelms-ukraines-defenses/

Beznosiuk, M. (2025f, September 23). Putin is escalating Russia's hybrid war against Europe: Is Europe ready? *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/putin-is-escalating-russias-hybrid-war-against-europe-is-europe-ready/

Beznosiuk, M. (2025g, June 25). Russia's drones campaign part of its hybrid warfare strategy. *Kyiv Post*. https://www.kyivpost.com/opinion/55148

Beznosiuk, M. (2025l, June 13). Russia's hybrid war on NATO's eastern flank quietly escalates. *New Eastern Europe*. https://neweasterneurope.eu/2025/06/13/russias-hybrid-war-on-natos-eastern-flank-quietly-escalates/

Beznosiuk, M. (2025h, June 5). Russian hybrid warfare: Ukraine's success offers lessons for Europe. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience/

Beznosiuk, M. (2025i, July 8). Southern Europe: A soft target in Russia's expanding hybrid war. *New Eastern Europe*. https://neweasterneurope.eu/2025/07/08/southern-europe-a-soft-target-in-russias-expanding-hybrid-war/

Beznosiuk, M. (2025j, August 5). The Kremlin's drone war has gone strategic: Ukraine must brace itself for an onslaught. *Kyiv Post*. https://www.kyivpost.com/opinion/57559

Beznosiuk, M. (2025k, September 24). The Kremlin tests Europe's defences without firing a shot. *Visegrad Insight*. https://visegradinsight.eu/the-kremlin-tests-europes-defences-without-firing-a-shot/

Beznosiuk, M. (2026, January 13). How Russia's hybrid warfare will escalate in 2026 and what Europe must do? *GLOBSEC*. https://www.globsec.org/what-we-do/commentaries/how-russias-hybrid-warfare-will-escalate-2026-and-what-europe-must-do

Bowser, D. (2025, December 9). Russian organised crime and links to hybrid war in Europe. *GLOBSEC*. https://www.globsec.org/what-we-do/publications/russian-organised-crime-and-links-hybrid-war-europe

Chernysh, O. (2024, July 12). Бюрократія проти ракет. Чому в Україні досі проблеми з укриттями? *BBC Україна*. https://www.bbc.com/ukrainian/articles/cjjwn9615yjo

Council of the European Union. (2025, October 23). 19th package of sanctions against Russia: EU targets Russian energy, third-country banks and crypto providers. https://www.consilium.europa.eu/en/press/press-releases/2025/10/23/19th-package-of-sanctions-against-russia-eu-targets-russian-energy-third-country-banks-and-crypto-providers/

Council of the European Union. (2026, March 16). Council adopts conclusions on advancing the EU's capacity to counter hybrid threats. https://www.consilium.europa.eu/en/press/press-releases/2026/03/16/council-adopts-conclusions-on-advancing-the-eu-s-capacity-to-counter-hybrid-threats/

Dixon, W., & Beznosiuk, M. (2025, December 19). Russia is losing: Time for Putin's 2026 hybrid escalation. *RUSI*. https://www.rusi.org/explore-our-research/publications/commentary/russia-losing-time-putins-2026-hybrid-escalation

Dixon, W., & Beznosiuk, M. (2026, February 24). From attrition to coercion: Russia's strategy in Ukraine. *Fondation pour la Recherche Stratégique*. https://www.frstrategie.org/publications/notes/attrition-coercion-russia-s-strategy-ukraine-2026

Dixon, W., & Beznosiuk, M. (2026, February 26). Putin's plan: Make Ukraine unlivable by destroying essential infrastructure. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/ukrainealert/putins-plan-make-ukraine-unlivable-by-destroying-essential-infrastructure/

Ebere, C., Halleck Vega, S. M., van Leeuwen, E., & Mashhoodi, B. (2025, September 29). Electricity grid and societal vulnerability interconnection: Stakeholder implications and integrated solutions in Europe. *Environmental Research Letters*. https://iopscience.iop.org/article/10.1088/1748-9326/ae0492

Edwards, C., & Seidenstein, N. (2025, August 19). The scale of Russian sabotage operations against Europe’s critical infrastructure. *IISS*. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

European Commission. (2025, March 26). EU preparedness union strategy to prevent and react to emerging threats and crises. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_856

European Commission. (2025, November 12). European democracy shield and EU strategy for civil society pave the way for stronger and more resilient democracies. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660

European Commission. (2026). European Centre for Democratic Resilience. https://commission.europa.eu/european-centre-democratic-resilience_en

France 24. (2026, January 29). Germany to harden critical infrastructure as Russia fears spike. https://www.france24.com/en/live-news/20260129-germany-to-harden-critical-infrastructure-as-russia-fears-spike

Havrylenkova, M. (2023, May 15). The war affects education: What is the educational and psychological damage? *U-LEAD with Europe*. https://u-lead.org.ua/en/news/205

Jensen, B., & Atalan, Y. (2025, May 13). Drone saturation: Russia's Shahed campaign. *CSIS*. https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign

Jones, S. G. (2025, March 18). Russia's shadow war against the West. *CSIS*. https://www.csis.org/analysis/russias-shadow-war-against-west

Klymenko. (2024, December 26). Клименко сказав, скільки в Україні valічується укриттів та бомбосховищ. *Ukrinform*. https://www.ukrinform.ua/rubric-regions/3942048-klimenko-skazav-skilki-v-ukraini-nalicuetsa-ukrittiv-ta-bomboshovis.html

Lubinets, D. (2025, December 15). Як прогалини у законодавстві перетворюють укриття на ризик, а не на захист? *Ukrainska Pravda*. https://www.pravda.com.ua/columns/2025/12/15/8011876/

Livermore, D. (2024, October 9). Sabotage: Protecting European transportation networks from Russia. *CEPA*.

https://cepa.org/article/sabotage-protecting-european-transportation-networks-from-russia/

Mykhailov, D. (2024, December 19). Шмигаль розповів, скільки в Україні є укриттів και що робить влада για їх покращення. *Suspilne*. https://suspilne.media/906425-smigal-rozpoviv-skilki-v-ukraini-e-ukrittiv-i-so-robit-vlada-dla-ih-pokrasenna/

Nikolov, B. (2025, March 29). Putin's plan unleashes 1.5M drone pilots into Russia's Army. *BulgarianMilitary.com*. https://bulgarianmilitary.com/2025/03/29/putins-plan-unleashes-1-5m-drone-pilots-into-russias-army/

OpenMinds. (2025, December 17). Drones and threats: Mapping the Kremlin's hybrid warfare in Europe. https://www.openminds.ltd/reports/drones-and-threats-mapping-the-kremlins-hybrid-warfare-in-europe

Petriczko, A. (2026, February 26). Who was behind the largest cyberattack on Polish energy infrastructure in years? *Balkan Insight*. https://balkaninsight.com/2026/02/26/who-was-behind-the-largest-cyberattack-on-polish-energy-infrastructure-in-years/rd/

Polish Ministry of Digital Affairs & CERT Polska. (2025, December 29). Energy sector incident report. https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf

PON. (2025, November). Освіта під час війни: школа як фундамент майбутнього миру. https://pon.org.ua/novyny/12406-viina-i-shkola-iak-osvita-formuie-osnovu-dlia-vidnovlennia-myru.html

PubAffairs Bruxelles & CEPS. (2026, March 16). With European defence on everyone's mind, we need to remember that security begins at home. https://www.pubaffairsbruxelles.eu/opinion-analysis/with-european-defence-on-everyones-mind-we-need-to-remember-that-security-begins-at-home/

Quis, H., & Buldioski, G. (2025, December). The EU's preparedness union: From broad ambition to focused action. *Bertelsmann Stiftung*. https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/426_25_BST_Policy_Brief_Preparedness_Union_ID2853_screen.pdf

Racicot, R. (2026, January 25). Russian drones in Europe: New tools of hybrid warfare. *NATO Association of Canada*. https://natoassociation.ca/russian-drones-in-europe-new-tools-of-hybrid-warfare/

Rosenbach, E., et al. (2026, February). Russian threats to NATO's Eastern flank: Scenarios, strategy, and policy for European security. *Belfer Center*. https://www.belfercenter.org/sites/default/files/2026-02/Belfer_Russian%20Threats_3.1.pdf

Souverbie, L. (2025, September 26). Russian incursions and hybrid warfare: Europe under aerial pressure. *IRIS*. https://www.iris-france.org/en/russian-incursions-and-hybrid-warfares-europe-under-aerial-pressure/

Teach For Ukraine. (2026, January 20). Learning during war: How stress affects adolescents' attention, memory, and motivation. https://teachforukraine.org/en/t4u-news/learning-during-war-how-stress-affects-adolescents-attention-memory-and-motivation-a-study-by-teach-for-ukraine-on-the-impact-of-adolescents-mental-health-on-learning/

Tanno, S., Shukla, S., & Kappeler, I. (2026, January 7). Thousands of Berliners lost power for days after climate activists struck: Here's what happened. *CNN*. https://edition.cnn.com/2026/01/07/europe/berlin-power-outage-intl

Tessari, F. (2026, February 1). Mass drone swarm attack? Europe is not ready at all. *EU Perspectives*. https://euperspectives.eu/2026/02/mass-drone-swarm-attack/

Todorow, A. (2026, January 15). Poland's PM praises cyber defences after attempted attack on energy infrastructure foiled. *Euronews*. https://www.euronews.com/2026/01/15/polands-pm-praises-cyber-defences-after-attempted-attack-on-energy-infrastructure-foiled

Urbancik, J. (2026, January 29). Russia's hybrid war is weakening Europe's cohesion, expert says. *Euronews*. https://www.euronews.com/2026/01/29/russias-hybrid-war-is-weakening-europes-cohesion-expert-says

Щирба, О. (2024, April). Чому українці звикають до повітряних тривог і що з цим робити. *Sestry*. https://www.sestry.eu/statti/chomu-ukrayinci-zvikayut-do-povitryanih-trivog-i-shcho-z-cim-robiti

Центр спільних дій. (2024). Третя Національна кампанія моніторингу укриттів: звіт. https://ccl.org.ua/wp-content/uploads/2024/10/tretya_naczionalna_kampaniya_monitoryngu_ukryttiv.pdf

About the Author

Maksym Beznosiuk is a strategic policy expert and Director of UAinFocus, an independent platform connecting Ukrainian and international experts around key issues facing Ukraine. He has authored numerous publications, with two of the most recent being "Reconstructing Ukraine: How the EU and Ukraine Can Mutually Benefit" and "Securing Europe's Critical Minerals: Leveraging the EU-Ukraine Partnership Amidst US Competition"

He previously served as a Research Analyst at ACAPS and an Atlas Corps Fellow at NCSEJ in Washington, D.C., where he focused on analysing political and socio-economic trends in the post-Soviet space, particularly in Ukraine and Russia.

Maksym holds a Bachelor's and Specialist Degrees in International Relations and International Law from the Institute of International Relations at Kyiv National Taras Shevchenko University. He also earned an LL.M. in Global Environment and Climate Change Law from the University of Edinburgh as a Chevening Scholar, as well as a Double MA in European Studies (Euroculture) from Uppsala University and Jagiellonian University, both of which are part of the Erasmus Mundus program.

His expertise includes Ukraine's reconstruction and recovery, EU-Ukraine cooperation, humanitarian response, international security, energy policy, and innovation and science policy.

Credits

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

Wilfried Martens Centre for European Studies

Rue du Commerce 20

Brussels, BE 1000

For more information, please visit www.martenscentre.eu

Cover Design: Gëzim Lezha, Brand and Visual Communications Officer, Martens Centre

This publication receives funding from the European Parliament.