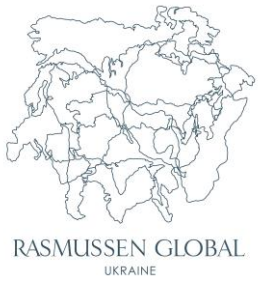

Guarding the Grid: Private Air Defence for Ukraine's Energy Sector

AUGUST 2026

Executive Summary

Since 2022, Russia has continuously targeted Ukraine's energy infrastructure. The threat has expanded across Ukraine's energy system, and attacks are not expected to stop in the foreseeable future. **Ukraine therefore needs a protection model that is sustainable over the long term**.

Passive protection has become the minimum standard for energy infrastructure. It should be incorporated into new projects and the modernisation of existing facilities, based on a structured assessment of risk and prioritisation of individual assets and components. However, the increasing intensity and sophistication of Russian attacks means that passive measures alone are no longer sufficient.

Ukraine is therefore developing an active layer of protection. Cabinet of Ministers Resolution No. 1506 provides a legal basis for enterprises to establish their own air defence groups under the command and control of the Armed Forces. Early operational experience demonstrates that this model can provide real value. **Private air defence should, however, be understood as a supplementary layer within Ukraine's unified air-defence system rather than as a replacement for the state's centralised air-defence responsibilities**.

The main problem is that the existing model remains experimental and difficult to implement in practice. Beyond operational and legal uncertainties, financing remains a major constraint. International financial institutions are unlikely to finance weapons or ammunition, leaving a significant gap between the protection operators require and the financing mechanisms currently available.

For most energy companies, outsourcing active protection to a specialised provider is likely to be easier than establishing an in-house capability, although in-house models will remain relevant for some operators.

The next stage should focus on transforming the existing experiment into a predictable, safe and financially sustainable framework. Alongside establishing passive protection as the minimum planning standard, this paper recommends six further areas of action. **(1)** Protection of critical infrastructure should be recognised as an eligible reconstruction and energy-investment cost, with support prioritised towards the most critical assets. **(2)** Resolution No. 1506 should be translated into a clear step-by-step operational guide. **(3)** A streamlined licensing pathway should be established for qualified private air-defence providers, **(4)** while training and certification capacity should be expanded. **(5)** Dedicated intergovernmental financing mechanisms should support the protection of state-owned energy operators rather than transferring these costs to consumers through regulated tariffs. Finally, **(6)** the community-level model involving energy operators, VFTCs and hromadas should be further developed.

International support will be essential, particularly for state-owned critical infrastructure. **A common approach is needed for incorporating protection measures into international financing programmes and mobilising targeted support for priority assets**. Partners unable to finance active protection can support passive measures, while bilateral engagement with allied governments may be necessary for capabilities that conventional financial institutions cannot finance.

The issue should also be viewed in a broader European context. Threats to energy and other critical infrastructure are increasing across Europe, while Ukraine has accumulated unique practical experience in protecting distributed energy systems under sustained attack. Ukraine can therefore offer international partners not only a case for support but also lessons relevant to their own resilience planning. At the same time, credible protection is becoming an increasingly important precondition for attracting and sustaining investment in Ukraine's energy sector by reducing war-related risks and protecting the value of reconstruction investments.

Background

Since 2022, Russia has targeted Ukraine's critical infrastructure with increasing intensity and diversification. Over the past four years, attacks on energy infrastructure have become a deliberate tool to disrupt daily life and the Ukrainian economy. Attacks occur in coordinated waves designed to overwhelm air defence, and targets have diversified beyond electricity to gas production and storage, district heating, water infrastructure, electrified transport and railway facilities.

In response, Ukraine has developed a layered approach to protecting energy infrastructure. In recent years, passive protection measures for energy facilities – including physical reinforcement, backup systems, stockpiling, and rapid repairs – have become essential across Ukraine. However, as Russia has intensified its attacks on energy infrastructure, passive protection alone is no longer enough. This has driven a shift toward active protection, with air defence deployed near critical infrastructure.

The legal basis for this shift is Cabinet of Ministers Resolution No. 1506 of 19 November 2025 [1], which allows enterprises of any ownership form to establish air defence groups under Air Force command and Ministry of Defence oversight. In March 2026, the framework was expanded to enable the Air Force temporarily transfer state air defence means and ammunition to authorised enterprises when not needed by combat units. By April 2026, 24 enterprises had received authorised status across several regions.

Early results have been cited by authorities as proof that the model can work effectively. In April 2026, Ukraine's former Defence Minister reported that a private air defence group in Kharkiv Oblast had, for the first time, shot down a jet-powered Shahed-type drone[2]. The interception showed that private groups integrated into Air Force command can provide real operational value. However, the resolution has also raised significant questions among energy operators.

In June 2026, Rasmussen Global and European-Ukrainian Energy Agency (EUEA) convened a closed-door discussion in Kyiv under the Chatham House Rule. The session brought together around 30 representatives from government, the military, the energy sector, private security providers, certified air defence companies, and international partners.

The discussion focused on protecting small- and medium-scale energy generation facilities from aerial attacks. Large-scale generation was not examined in detail, as the government is already strengthening its protection. **The objective was to identify implementation gaps and develop practical recommendations.** This paper reflects the main conclusions and proposals emerging from that discussion. It is not intended to provide a comprehensive assessment of all relevant issues, but rather to highlight selected priorities and suggest areas for further analysis and action.

[1] Cabinet of Ministers of Ukraine, Resolution No. 1506 of 19 November 2025, "On the Implementation of an Experimental Project to Strengthen the Air Defence of the Territory of Ukraine by Involving Enterprises, Regardless of Ownership Form, in the Establishment of Air Defence Groups." https://zakon.rada.gov.ua/laws/show/1506-2025-п.

[2] "Private air defence group downs jet-powered Shahed in Kharkiv Oblast for first time – Ukrainian defence minister," Ukrainska Pravda, 17 April 2026, https://www.pravda.com.ua/eng/news/2026/04/17/8030601/.

State of Play

PASSIVE PROTECTION AS THE NEW MINIMUM STANDARD

In response to Russia's continued attacks, Ukraine's energy sector has strengthened physical protection, redundancy and emergency restoration capacity. Passive protection of energy assets is no longer viewed as optional.

This paper argues that passive protection has become an essential part of planning for any new energy project, given that Ukraine's heightened risk environment is expected to persist even under any form of ceasefire.

This new reality increases the cost of new projects, making it more difficult to attract investment even for passive protection, let alone for the active protection measures discussed later in this paper. In simple terms, investors are often more willing to invest in projects in neighbouring countries (e.g. Poland or Romania). Such projects generally do not require a dedicated protection budget, involve lower risks, and may offer similar returns.

However, this logic does not consider the broader geopolitical picture. Risks to Europe's energy infrastructure are expected to grow in the coming years. European countries will increasingly need to protect their energy assets, while Ukraine offers unique experience and lessons in this area.

The emerging consensus in the debate on passive protection is that prioritisation is essential. Not every energy facility, or every component within it, requires the same level of physical protection. To optimize costs while ensuring an adequate level of security, protection should focus on the most critical facilities and components, such as power transformers.

Prioritisation should be based on a structured assessment of risk rather than on asset category alone. The assessment should consider the likelihood and type of attack, potential consequences, redundancy or replacement options, geographic exposure, and the asset's importance to energy-system stability. This would focus limited resources on assets where disruption would have the greatest impact.

This is a basic step to improve security and reduce the vulnerability of critical energy components to nearby drone strikes or explosions. For example, one Ukrainian state-owned energy company has prioritized 18 most critical assets and is primarily seeking support to ensure their protection ahead of the next winter season. The enemy is also aware of Ukraine's most critical energy assets, which face more intensive targeting, including cruise and ballistic missiles. For these facilities, passive protection alone is not sufficient.

FROM AD HOC ACTIVE PROTECTION TO A STRUCTURED MODEL

The intensity of Russian attacks has made the development of active protection for energy assets unavoidable. In practice, active protection has already existed in different forms. Some energy companies have supported mobile fire groups of the Armed Forces of Ukraine operating near energy

facilities and tasked with intercepting aerial targets. This support has included financing, donations, and various forms of partnership aimed at strengthening the groups' operational effectiveness. The effectiveness of this ad hoc support remains unclear, given difficulties in attributing interceptions to specific groups and tailoring protection to each facility's threat profile.

The significant increase in demand has created a need for a more structured model. The Cabinet of Ministers Resolution No. 1506 was intended to put the pieces of this complex framework together[3]. In practice, however, it has left many energy-sector actors even more puzzled about how the model should work.

The existing framework allows eligible critical infrastructure operators to establish their own air defence groups or contract an authorized provider. These groups must be integrated into the unified air defence system under the command and control of the Armed Forces and must not operate autonomously[4]. In broad terms, an operator must obtain the relevant eligibility status; coordinate with the responsible air command on tasking and areas of responsibility; agree on the facility or facilities to be defended and the means of defence; procure approved materiel; complete the required training, certification, and inspection processes; and integrate into the requisite command, control, and communications (C3) architecture.

Active protection should not be understood exclusively in terms of kinetic interception. For small- and medium-scale energy assets in particular, an effective protection model may combine several complementary layers, including electronic warfare, acoustic detection, passive sensors and other detection technologies alongside conventional interception capabilities. The appropriate combination will depend on the threat profile, location, configuration and operational importance of each facility.

Crucially, this model should not be understood as creating parallel or autonomous air-defence architecture. **Private air-defence groups are an additional operational layer within the existing national air-defence system and must remain integrated into its command, control and communications architecture.**

Private operators provide additional personnel, equipment and financing, while the Armed Forces retain authority over weapons use and overall air-defence coordination. Different groups of energy-sector actors interpret and approach the existing legislation differently. For companies new to active protection, the process can be discouraging, with limited clarity on where to start, expected costs or available guarantees. Some companies prefer to rely on stockpiling critical equipment rather than seeking ways to protect it. This model may work in the short term, but it is neither cost-efficient nor strategic in the context of a continuing threat.

---

[3] Cabinet of Ministers of Ukraine, Resolution No. 1506 of 19 November 2025, "On the Implementation of an Experimental Project to Strengthen the Air Defence of the Territory of Ukraine by Involving Enterprises, Regardless of Ownership Form, in the Establishment of Air Defence Groups." https://zakon.rada.gov.ua/laws/show/1506-2025-п.

[4] On the integration requirement (points 7 and 8 of the Procedure) and mobile fire groups operating under Armed Forces command, see "Вертикальна охорона: приватна ППО для економіки України," Engage, 23 April 2026. https://engage.org.ua/vertykalna-okhorona-pryvatna-ppo-dlia-ekonomiky-ukrainy/.

Companies with private air-defence experience are better able to anticipate the challenges of developing a full in-house capability. The main bottlenecks identified during the closed-door discussion included access to the necessary licenses – both the explosives-handling license and the license to operate as a private air defence provider – a shortage of qualified personnel, and limited training capacity.

Both groups broadly agreed that, for an energy company operating both small- and large-scale generation assets, outsourcing air-defence protection would be easier than establishing and operating an in-house capability.

Many stakeholders still view the initiative as an experiment rather than an established framework – and this perception is legally accurate. Resolution No. 1506 introduces a time-bound experimental project, valid only for the period of martial law and for no more than two years. This is a narrow military experiment: businesses provide financing and part of the operational capacity, while the state retains authority over the use of weapons. This distinction has direct legal consequences. Legal practitioners have warned that confusing "admission to the system" with a "market right to shoot down drones" is precisely where criminal liability can arise, and that those who read the framework carelessly may find themselves not celebrating interceptions but managing criminal proceedings[5].

This risk is amplified by the fact that Resolution No. 1506 does not sit within a single, coherent body of law. It overlaps with a separate critical-infrastructure protection framework – the Law on Critical Infrastructure[6] and a stack of implementing acts built around passportisation, risk management and the objects registry – that was designed around passive protection rather than the use of active means[7]. It also intersects with a classified priority-cover regime: Cabinet of Ministers Order No. 1229-pc-on of 27 December 2022 approved a restricted-access list of Category I critical-infrastructure objects requiring priority protection from enemy air strikes[8]. Because that list carries a limited-access classification, operators cannot readily establish how it interacts with their own obligations under Resolution No. 1506, or which regime governs which object. **These frameworks were not authored as a single system, and they have not been synchronized.** Until they are, an operator acting in good faith can still find itself in a grey zone – which is itself a barrier to commitment.

For state-owned energy companies, a further constraint sits on top of the legal one: their financing is regulated, and this narrows their room for manoeuvre far more than it does for private firms. A private company can, in principle, decide to spend its own money on active protection. A state-owned operator

[5] Yevhen Shevchenko (CEO, SHERIFF), "Право збивати: чому постанова № 1506 — це не «приватна ППО», а військовий експеримент," NV, 4 May 2026. https://nv.ua/ukr/ukraine/events/privatne-ppo-yak-postanova-1506-dozvolyaye-biznesu-zbivati-droni-detali-vid-eksperta-50605086.html.

[6] Cabinet of Ministers of Ukraine, Law on Critical Infrastructure of 21 September 2024. https://zakon.rada.gov.ua/laws/show/1882-20#Text.

[7] Overview of the critical-infrastructure protection framework (Law on Critical Infrastructure and implementing resolutions Nos. 1109, 821, 1175, 415, 818, 367): Ministry of Economy of Ukraine, "Critical Infrastructure." https://mev.gov.ua/en/storinka/critical-infrastructure.

[8] Cabinet of Ministers of Ukraine, Order No. 1229-pc-on of 27 December 2022, "On approval of the List of critical-infrastructure objects (Category I criticality) requiring priority cover from enemy air strikes" (restricted access). Existence and title confirmed in "Державно-приватне партнерство: єдиний механізм для захисту критичної інфраструктури," Mind.ua, 17 August 2023. https://mind.ua/openmind/20261400-derzhavno-privatne-partnerstvo-edinij-mehanizm-dlya-zahistu-kritichnoyi-infrastrukturi.

largely cannot: its investment is funded through, and bound by, a tariff set by the national regulator (NKREKP), which determines what costs may be recovered. Such tariff-funded investment programmes are typically ring-fenced – the sources of financing are held on dedicated accounts and cannot be redirected until the regulator approves the programme, with narrow exceptions such as the restoration of war-damaged networks[9]. Active air-defence financing does not fit easily within this framework, particularly for weapons and ammunition.

A state operator has very little discretion over its own finances, and a single misalignment in legislation can directly freeze a financing decision. For most state-owned energy companies, active protection is unaffordable without external support. As international financial institutions are unlikely to finance weapons or ammunition, support may need to come directly from Ukraine's allied governments.

FINANCING AND ORGANIZING ACTIVE PROTECTION

Before financing can be addressed, an energy company faces a more fundamental decision, and every other question follows from it: how to obtain capability in the first place. The discussion pointed to two broad routes. A company can build and operate its own private air defence capability in-house – including, as one variant, the model in which its employees contract with a Volunteer Formation of a Territorial Community (VFTC). Or it can outsource to an authorised provider that establishes and runs the capability on its behalf. There are, of course, other possible configurations, but these were the two that stakeholders returned to. Each carries a different cost profile, a different set of bottlenecks, and a different balance between operational independence and speed.

Whichever route an energy company chooses, the financing question becomes impossible to ignore. For most state-owned energy companies, such services are unaffordable without external financial support. This remains the case even when a company chooses, and is legally and organizationally able, to develop its own private air defence capability.

Companies also need a clear understanding of the full lifecycle cost of either model. This should distinguish between up-front costs – such as site assessment, equipment, training, certification and integration – and recurring costs, including personnel, maintenance, retraining, equipment replacement, ammunition and communications.

Costs will vary depending on the threat, facility size and location, required level of protection, and whether the model is in-house or outsourced. For smaller or concentrated assets, shared protection between operators or with the local hromada may be more cost-effective. A standard cost methodology would help companies compare options and give international partners a clearer basis for financing decisions.

At present, conventional financing from international financial institutions is unlikely to cover assets classified as weapons or ammunition, either because no suitable financing mechanisms exist or because

[9] On the ring-fencing of tariff-funded investment programmes under martial-law conditions, see the National Energy and Utilities Regulatory Commission (NKREKP) transmission-tariff acts for 2026. https://www.nerc.gov.ua/acts/pro-vstanovlennya-tarifu-na-poslugi-z-peredachi-elektrichnoyi-energiyi-nek-ukrenergo-na-2026-rik.

such support would be inconsistent with the institution's internal policies. For state-owned companies, discussions on financing active protection for critical infrastructure may therefore need to take place directly with Ukraine's allied governments. This is a challenging task. As described above, mobilizing support even for the passive protection of critical assets remains difficult. In addition, existing instruments for mobilizing such support, primarily the Energy Support Fund, are viewed by many stakeholders as a blocker because of the lengthy delivery process.

The situation is not much easier for private energy companies. Among all the organizational challenges, cost stands out. Companies considering outsourcing want clarity on the service offered, the level of protection it can provide, and whether it justifies the cost.

Of the two routes, outsourcing is the one that most companies gravitate toward first. Several security companies participated in the closed-door discussion. These included both traditional providers of physical site security and newer companies established during the full-scale invasion, often by veterans or as part of the military-technology ecosystem.

Energy companies broadly agreed that it would be easier to hire a specialised provider that could establish and operate the active protection capability while also managing the related administrative and regulatory requirements.

The market for security companies providing active protection for critical infrastructure is therefore expected to grow in the coming years. If this model proves workable for the energy sector, such growth would be a natural development. However, stakeholder concerns must be addressed through clear standards. The price must correspond to the value and quality of the service, including properly trained personnel, regular retraining and consistent compliance with all relevant protocols.

Operational effectiveness remains the primary concern with this route. Several stakeholders noted that military air defence personnel may provide a higher level of effectiveness. At the same time, assigning military personnel to the protection of each individual energy facilities is difficult because of personnel shortages and the operational requirements of the Armed Forces. As the market for private providers grows, the level of their expertise, training and operational performance must grow accordingly.

The other route is to build in-house. Some companies are choosing to establish their own private air defence capability. This route is longer and more complex, but once established, an in-house capability can provide the company with a greater degree of operational independence.

For companies choosing this path, the guidelines must be clear, and adequate training must be available. One of the problems identified during the discussion was the limited number and capacity of existing training centres. Veteran- and military-led training centres could help energy companies develop in-house air-defence capabilities.

One training centre interviewed during this research described a package of services that includes support with the legal and organizational set-up, a technical assessment of the energy site, electronic warfare integration and the development of a protection model tailored to the company's needs. The

centre also works with providers of relevant defence solutions and helps connect companies with a Volunteer Formation of a Territorial Community (VFTC).

One version of the in-house route runs through the community level. Under this model, employees forming the company's air defence group enter into a contract with a local VFTC. This brings the group within an established legal and command framework and may facilitate access to the necessary authorizations and approved equipment – two of the main bottlenecks identified by stakeholders during the working session.

This model requires clearer communication and further explanation, particularly because some employees may have concerns about possible mobilization implications in case if the energy facility does not hold a status of criticality in accordance with Ukrainian legislation. Nevertheless, it could help address several of the most significant legal and organizational barriers.

There may also be opportunities to mobilize additional funding for private air defence at the community level. Several stakeholders suggested that cooperation between an energy company, a VFTC and the relevant hromada could provide a mechanism for mobilizing financial support and other resources to protect energy assets that are critical to the respective community.

Policy recommendations

Disclaimer: this preliminary list of recommendations is based on the outcomes of the closed-door session. It is not intended to be comprehensive or final and will be revised and expanded following further stakeholder consultations. The initiative is currently at the formalization stage, and further recommendations are therefore expected to emerge.

0. ESTABLISH PASSIVE PROTECTION AS THE MINIMUM PLANNING STANDARD

Passive protection is no longer optional for energy infrastructure in Ukraine. However, it is still not consistently incorporated into the design of new energy projects or the modernisation of existing facilities. This leaves newly constructed and restored assets exposed to a threat environment that is expected to persist even under a ceasefire or reduction in hostilities.

Passive protection should be incorporated into the design of all new energy projects and added to existing facilities facing a high risk of attack. Requirements should be proportionate to the threat and based on clear prioritisation, as not every facility or component requires the same level of protection. Operators should focus first on the most critical assets and components, including substations, transformers and other elements whose loss could significantly disrupt the functioning of the wider energy system.

1. RECOGNISE PROTECTION AS AN ELIGIBLE RECONSTRUCTION COST

Donors, international financial institutions and reconstruction programmes often continue to treat the protection of critical infrastructure as separate from conventional energy-sector investment. As a result, companies may be able to mobilise funding for the construction or restoration of energy assets but not for the measures required to protect those investments. This reduces the long-term effectiveness of reconstruction support and increases the risk that newly financed infrastructure will remain vulnerable to further attacks.

Energy-sector and recovery financing frameworks should formally recognise critical-infrastructure protection as an eligible project cost. This should include passive protection, while leaving room for dedicated mechanisms to finance active protection where legally and institutionally possible. Funding requests should focus on the most critical facilities and components rather than seek to protect every asset to the same level. The Ministry of Energy can provide partners with a list of priority assets and components requiring protection.

Partners that are not yet prepared to finance active protection should be encouraged to direct their support towards passive measures. The mechanisms used to deliver such assistance should also be reviewed. In particular, the operating model of the Energy Support Fund should be reconsidered to reduce delivery timelines and ensure that available support reaches priority projects more effectively.

Advocacy at the EU and bilateral donor-coordination levels should frame the protection of Ukraine's energy infrastructure as part of the wider European security and resilience agenda rather than as a challenge affecting Ukraine alone.

This engagement should also include a more structured exchange with European and NATO partners on the lessons emerging from Ukraine's experience. Such cooperation could focus on approaches to protecting distributed energy infrastructure, integrating privately financed capabilities into state command structures, developing common requirements for detection and protection technologies, and identifying elements of the Ukrainian model that could be adapted to different national contexts.

2. TURN RESOLUTION NO. 1506 INTO A STEP-BY-STEP OPERATIONAL GUIDE

Companies lack clarity on how to organise private air defence in practice under Resolution No. 1506. The approval process is fragmented across several authorities, whose requirements may not always be aligned. State-owned companies also face additional legal uncertainty due to inconsistencies between the regulatory acts governing this area.

The Ministry of Defence, Air Force Command, the relevant operator and the Ministry of Internal Affairs should agree on a single procedure and translate it into a clear, step-by-step manual for private, municipal and state-owned operators. Companies with practical experience in establishing private air defence capabilities should be involved in its development, either through a dedicated working meeting or through the collection and consolidation of their proposals.

3. CREATE A STREAMLINED LICENSING PATHWAY FOR QUALIFIED PROVIDERS

Most energy companies would prefer to outsource active protection rather than build an in-house capability from scratch. However, security companies that are best placed to provide such services report that obtaining the necessary licences, including licences related to weapons, ammunition and explosives handling, remains one of the barriers to entering the market.

The competent weapons-control authorities should establish a dedicated and time-bound licensing pathway for qualified companies providing private air defence and related services. The pathway should clearly define eligibility requirements, required documentation, responsible authorities and expected processing timelines. Streamlining the procedure should not reduce safety or qualification standards but should make the process more predictable and accessible for providers capable of meeting them.

Alternatively, access to the necessary licenses may be facilitated through cooperation with a Volunteer Formation of a Territorial Community, as outlined in Recommendation 6.

4. EXPAND TRAINING AND CERTIFICATION CAPACITY

Companies that choose to establish their own private air defence capability need access to appropriate initial training, certification and regular retraining for their personnel. Existing training capacity is limited and may not be sufficient if the number of operators establishing private air defence groups increases. The development of additional qualified training centres is constrained primarily by a lack of sustainable financing.

Relevant authorities should establish clear qualification and certification requirements for personnel involved in private air defence and support the expansion of the network of accredited training centres. Opportunities to mobilise partner funding should be identified to develop training infrastructure, strengthen instructor capacity and provide the equipment required for practical training. Centres established by veterans and specialists with relevant military experience could play an important role, provided that they comply with common training and certification standards.

5. DEVELOP DEDICATED FINANCING FOR THE PROTECTION OF STATE-OWNED ENERGY OPERATORS

Companies operating under state-regulated tariffs cannot independently finance protection measures because these costs are not currently covered by their approved financial frameworks. Addressing this constraint through tariff increases would, however, be politically and socially sensitive during wartime. It would place an additional burden on households and businesses and could generate public resistance at a time when tariff stability remains critical.

Instead of incorporating protection costs into the tariff methodology, Ukraine and its partners should seek dedicated intergovernmental financing for programmes aimed specifically at strengthening the

protection of state-owned energy companies. Such support should be provided through targeted bilateral or multilateral arrangements rather than passed on to consumers through tariffs.

In parallel, efforts should focus on strengthening the centralised air-defence system, particularly the units responsible for protecting designated critical assets of state-owned energy companies. This should include increasing personnel capacity, expanding the intensity and availability of training, and improving access to detection and interception capabilities, including radar and appropriate air-defence systems.

6. FORMALISE THE COMMUNITY-LEVEL PROTECTION MODEL

Cooperation between an energy operator, a Volunteer Formation of a Territorial Community and the relevant hromada could help address several financial, legal and organisational barriers to establishing private air defence. This model may be particularly relevant where an energy facility is critical to the surrounding community. However, operators and employees currently lack clarity regarding the legal responsibilities of each participant, access to authorisations and approved equipment, permissible financing arrangements and the possible mobilisation implications for participating employees.

The relevant authorities should issue clear guidance explaining how cooperation between an energy operator, a VFTC and a hromada can be established and operated. The guidance should define the responsibilities of each participant, permitted sources and uses of funding, the procedure for obtaining approved equipment and the requirements for integration into the military command structure. It should also clarify the legal and mobilisation implications for employees, particularly where the energy facility does not have formal critical-infrastructure status. Clearer rules would allow this model to be used where appropriate rather than avoided because of legal uncertainty.

Conclusions

Ukraine's energy infrastructure will continue to operate in a heightened threat environment, making both passive and active protection a long-term requirement. Passive protection should remain the foundation, with active protection used where risks justify it.

Resolution No. 1506 has created an important legal basis for energy companies to contribute directly to the protection of their assets. Early experience indicates that the approach can provide operational value. However, it remains an experimental framework rather than a fully established system.

As significant uncertainties remain over how the model should work in practice, the priority should be to make the existing framework workable and predictable. This requires clearer procedures, consistent licensing and training standards, sustainable financing arrangements and defined models of cooperation between the parties involved. Without this, private air defence risks remaining accessible mainly to a small number of well-resourced companies and developing unevenly across regions and sectors.

Private capabilities should continue to complement, rather than substitute for, Ukraine's centralised air-defence system. The state can gain additional capacity without losing operational control, while companies and providers benefit from clearer protection options and regulation.

International partners will also have an important role. Protection should be treated as part of the cost of rebuilding Ukraine's energy system, particularly where inadequate protection puts investments at risk. At the same time, Ukraine's experience can contribute to the wider European discussion on critical-infrastructure resilience as similar risks become more prominent across the continent.

Further consultations and practical testing will be necessary as the framework develops. The objective should be a protection model that can adapt to an evolving threat, direct limited resources towards the assets that matter most, and provide a more secure basis for the continued operation and investment needs of Ukraine's energy sector.

ABOUT RASMUSSEN GLOBAL

Rasmussen Global was founded in 2014 by Anders Fogh Rasmussen after his tenure as NATO Secretary General. Today, it is Europe's leading independent geopolitical advisory firm, operating at the heart of European and transatlantic decision-making across key global capitals. Our mission is to help democracies – and their industrial and technological champions – navigate an increasingly volatile geopolitical landscape. For more information visit www.rasmussenglobal.com.

ABOUT EUROPEAN-UKRAINIAN ENERGY AGENCY (EUEA)

Established in 2009, the European-Ukrainian Energy Agency (EUEA) is an independent association that represents the interests of foreign investors and key players in Ukraine's renewable energy and energy efficiency sectors. It acts as a unified voice for the industry - pushing for progressive legislation and sound business practices, helping investors get projects off the ground, and building dialogue between the private sector, government, and international partners. EUEA also serves as a platform where people in the industry can share knowledge and stay connected. Through advocacy, networking, project support, and information sharing, the agency helps drive forward a modern, sustainable, and investment-friendly energy sector in Ukraine. For more information visit www.euea-energyagency.org