



Source: Unsplash

Hybrid Threats: Ukraine's Experience in Ensuring Euro-Atlantic Security

By Daniela Toaka

What is the Ukrainian Theory on Hybrid Warfare?

There is no single codified “Ukrainian theory” of hybrid warfare. What has emerged instead is a body of concepts shaped by more than a decade of confrontation with Russia and progressively translated into Ukrainian strategic documents. Its distinctive feature is that hybridity is understood less as a separate category of conflict than as a method of attacking the functioning of a state. Ukrainian strategic thought, particularly the work associated with Volodymyr Horbulin and later Olga Reznikova, focuses

not simply on whether military and non-military instruments are combined, but on whether their interaction produces a cumulative effect that weakens the target's ability to govern, protect critical functions, preserve social cohesion, and make sovereign decisions (Horbulin, 2017; Reznikova, 2022).

This logic is visible in policy. The Concept of the National Resilience System defines hybrid threats as combinations of methods that create a synergistic effect, often remain concealed, or are disguised as ordinary processes operating within the legal field (President of Ukraine, 2021). The wording is important because it directs attention away from spectacular hostile acts and towards vulnerabilities that may appear non-military: distrust in public institutions, fragile infrastructure, dependence on single suppliers, weak local crisis management, compromised information channels, or people susceptible to manipulation. The practical question therefore becomes not only “What is Russia doing?” but also “Which normal function is being converted into a channel of coercive influence?”

The 2026 Concept for Combating Terrorism further develops this logic. It places armed aggression, terrorist acts, cyberterrorism, attacks on critical infrastructure and supply chains, sabotage, and special information operations within the same threat environment (President of Ukraine, 2026c). This is a significant Ukrainian correction to an analytical habit of separating conventional warfare, cyber activity, influence operations, intelligence work, and terrorism into distinct professional compartments. Russian practice against Ukraine shows that these instruments can be operationally connected even when law and bureaucracy classify them differently.

Three propositions follow from the Ukrainian experience:

First, hybrid methods are not confined to the “grey zone” below the threshold of armed conflict. They operate before, during, and alongside high-intensity warfare. A missile strike may be part of a wider coercive design when its physical effects are reinforced by cyber disruption, false narratives, pressure on public confidence, and attempts to hinder recovery. Conversely, apparently minor acts such as photographing infrastructure, registering communications equipment, or setting fire to a relay cabinet may directly support military operations.

Second, the target is often functionality rather than territory. Russian pressure seeks to make ordinary systems unreliable: electricity should become uncertain, public information contestable, logistics vulnerable and interpersonal trust exploitable. This helps explain why resilience has moved to the centre

of Ukrainian security thinking. Reznikova (2022) treats resilience as the capacity of the state and society to anticipate, absorb, adapt to, and recover from shocks while maintaining essential functions. The experience of prolonged war has turned this from a conceptual proposition into routine governance.

Third, defence against hybrid pressure cannot belong to the security services alone. Ukraine's resilience model connects central government, local authorities, businesses, critical-infrastructure operators, communities, and citizens (President of Ukraine, 2021). In 2026, this whole-of-society principle became increasingly practical through regional planning that allocated responsibility for energy protection, reserve power, fuel, emergency repair, civil protection, and continuity of essential services (President of Ukraine, 2026b).

For Euro-Atlantic security, this is the most transferable lesson. A hybrid campaign may not announce itself as a crisis. Early indicators may be dispersed across police records, energy failures, cyber incidents, local disinformation, unusual procurement, criminal recruitment, or repeated pressure on the same social vulnerability. The Ukrainian approach suggests that deterrence begins by connecting these signals before they become one operation. Resilience is therefore not an auxiliary to defence; it is a method of denying an adversary the ability to turn ordinary dependencies into strategic leverage.

Case Study I: Energy Resilience in 2026 — Denying Russia the “Winter Weapon”

The energy campaign of 2026 demonstrates why physical destruction alone is an inadequate framework for understanding Russian pressure. In March, the State Service of Special Communications and Information Protection of Ukraine reported that Russia had entered 2026 with a campaign aimed at dismantling the energy sector and depriving the population of electricity and heating. The same assessment noted that by the end of 2025 no Ukrainian power plant had remained unscathed (State Service of Special Communications and Information Protection of Ukraine [SSSCIP], 2026a). In June, the agency reported that more than 63.000 energy-infrastructure facilities had been damaged or destroyed since the beginning of the full-scale invasion (SSSCIP, 2026b).



Figure 1. National Security and Defence Council meeting at which regional energy-resilience plans were approved, 3 March 2026. Source: Office of the President of Ukraine (2026a)

The strategic problem is broader than the number of damaged assets. Attacks on generation, transmission, heating, water, logistics, and communications can produce mutually reinforcing consequences for households, local government, industry, and public confidence. This is precisely why Ukraine's response in 2026 shifted further from restoration after individual strikes towards planned continuity under repeated attack.

On 3 March 2026, the National Security and Defence Council approved comprehensive energy-resilience plans for Ukraine's regions and major cities. The plans link the protection and restoration of infrastructure with reserve equipment, distributed generation, local responsibility, decentralised heat and water supply, and preparations for the 2026–2027 heating season (President of Ukraine, 2026a, 2026b). The stated objective was particularly revealing: no winter should become an instrument of pressure on Ukraine. In strategic terms, the purpose is therefore not simply to save individual

substations. It is to prevent a successful conversion of physical damage into social exhaustion and political coercion.

This produces a less obvious lesson for NATO members. Resilience must be designed around services rather than individual facilities. Protecting one substation is insufficient if water pumping, mobile communications, transport, emergency response, and public information fail together. Ukraine's approach increasingly prioritises distributed capacity, reserves, repair speed, local autonomy, and predefined responsibility. The objective is not to make every Russian strike ineffective, which would be unrealistic, but to reduce the strategic return obtained from each strike.

For Euro-Atlantic planning, the relevant preparedness metric is therefore not only how much infrastructure can be protected. It is how long essential functions can continue when protection fails. Hybrid coercion becomes effective when disruption acquires political value. Ukraine's 2026 model is an attempt to break that conversion.

Case Study II: Remote Recruitment in 2026 — When the “Agent” Is an Ordinary User

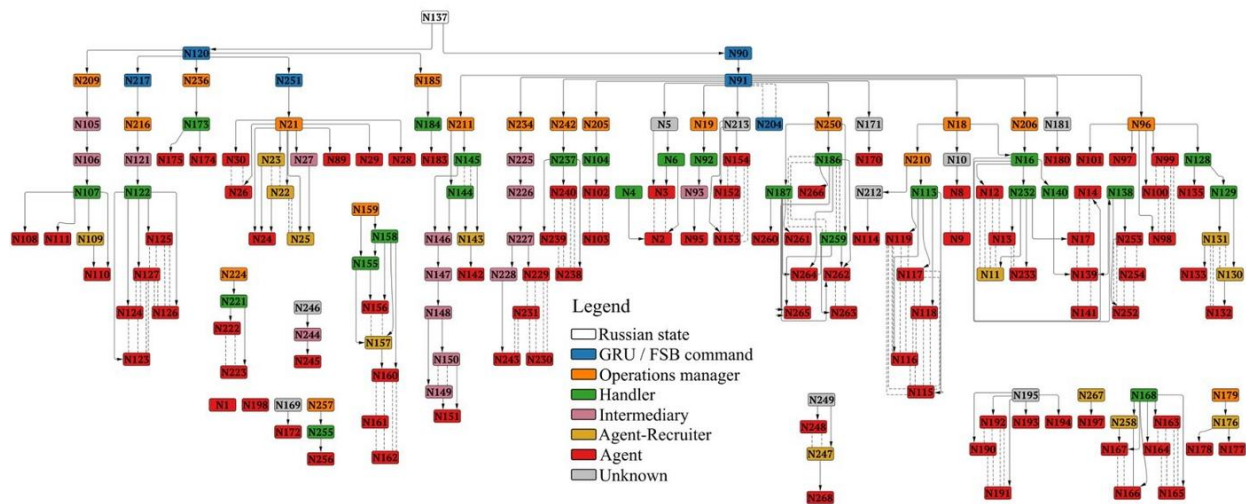


Figure 2. Source: European Security, Routledge. Schuurman, Institute of Security and Global Affairs, The Hague. Made with Cytoscape’s “yFiles Hierarchic Layout”, manually adjusted for greater clarity. Notes: Arrows indicate a directional relationship, dashed lines a collaborative one.

A second 2026 development is less visible but equally transferable: the industrialisation of remote recruitment. In August, the Security Service of Ukraine (SBU) reported more than 300 Russian-linked acts of sabotage and terrorism during the year; 249 had been solved, and 84 prevented. The SBU warned that recruitment increasingly begins with an ordinary message in a social network or messenger, while Russian handlers impersonate employers, volunteers, law-enforcement officers, or potential romantic partners (Security Service of Ukraine, 2026b).

Recent Ukrainian cases show the operational logic. In July, the SBU detained two alleged FSB (the Russian internal security service) agents in Kharkiv region who had been recruited remotely through Telegram channels advertising “easy money”. According to investigators, they first completed test tasks, including photographing facilities and setting fire to a Defence Forces vehicle, before becoming involved in a plan to attack Ukrainian servicemen at a staged charity event (SBU, 2026a). In August, the National Police described another scheme in which residents were recruited through Telegram to register satellite-communications terminals in their own names. The equipment was then used by Russian forces for communications, battlefield coordination, and the adjustment of artillery and missile

strikes (National Police of Ukraine, 2026a). Police also documented a coercive method in which callers posed as SBU officers, accused victims of financing Russia, and pressured them into performing “tasks” (National Police of Ukraine, 2026b).

The significance lies not in Telegram itself. It lies in the shrinking distance between a foreign intelligence service and a disposable local executor. Recruitment can be cheap, remote, temporary, and tailored to financial need, fear, loneliness, ideological sympathy, or simple lack of awareness. One person may perform only one fragment of an operation and never see the wider chain. The agent network therefore becomes distributed, scalable and difficult to recognise through traditional counter-intelligence assumptions.

Ukraine’s response is partly societal. Public warnings, reporting channels, digital literacy, policing, and counterintelligence are being combined to interrupt recruitment before a criminal act occurs (SBU, 2026b). This has direct relevance for Euro-Atlantic security. A state that searches only for professional foreign agents may overlook a model built around citizens who do not initially understand that they are entering an intelligence operation. Ukraine’s 2026 experience shows that the front line of counter-intelligence may begin with an unsolicited message on an ordinary phone.

References

1. Horbulin, V. P. (Ed.). (2017). *Світова гібридна війна: Український фронт [World hybrid war: Ukrainian front]*. National Institute for Strategic Studies. <https://www.niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya>
2. National Police of Ukraine. (2026a, August 10). *Нацполіція та СБУ викрили схему реєстрації терміналів супутникового зв'язку для окупантів [National Police and SBU expose a scheme for registering satellite communications terminals for Russian forces]*. <https://npu.gov.ua/news/natspolitsiia-ta-sbu-vykryly-skhemu-reiestratsii-terminaliv-suputnykovoho-zv'iazku-dlia-okupantiv>
3. National Police of Ukraine. (2026b, August 11). *Телефонують покупцям БАДів від імені СБУ: у поліції розповіли про нову схему вербування РФ [Callers pose as SBU officers: Police describe a new Russian recruitment scheme]*. <https://npu.gov.ua/news/telefonuiut-pokuptsiam-badiv-vid-imeni-sbu-politsii-rozpovily-pro-novu-skhemu-verbuvannia-rf>

4. President of Ukraine. (2021, September 27). *Указ Президента України № 479/2021: Про запровадження національної системи стійкості* [Decree of the President of Ukraine No. 479/2021: On the introduction of the national resilience system]. <https://www.president.gov.ua/documents/4792021-40181>
5. President of Ukraine. (2026a, March 3). *РНБО затвердила плани енергетичної стійкості регіонів України* [National Security and Defence Council approved energy resilience plans for Ukraine's regions]. <https://www.president.gov.ua/en/news/rnbo-zatverdila-plani-energetichnoyi-stijkosti-regioniv-ukra-103197>
6. President of Ukraine. (2026b, March 14). *Указ Президента України № 239/2026: Щодо комплексних планів стійкості регіонів та окремих міст* [Decree of the President of Ukraine No. 239/2026: On comprehensive resilience plans for regions and selected cities]. <https://www.president.gov.ua/documents/2392026-58833>
7. President of Ukraine. (2026c, June 11). *Указ Президента України № 492/2026: Про Концепцію боротьби з тероризмом в Україні* [Decree of the President of Ukraine No. 492/2026: On the Concept for Combating Terrorism in Ukraine]. <https://www.president.gov.ua/documents/4922026-59865>
8. Reznikova, O. O. (2022). *Національна стійкість в умовах мінливого безпекового середовища* [National resilience in a changing security environment]. National Institute for Strategic Studies. <https://niss.gov.ua/en/publikacii/monografii/national-resilience-changing-security-environment>
9. Security Service of Ukraine. (2026a, July 27). *SBU detains FSB agents who attempted to kill dozens of Ukrainian military personnel by organising a fake charity party*. <https://www.ssu.gov.ua/en/novyny/sbu-zatrymala-ahentiv-fsb-yaki-namahalysia-likviduvaty-dekilka-desiaticiv-ukrainskykh-viiskovykh-orhanizuvavshy-dlia-nykh-blahodiinu-vechirku-video>
10. Security Service of Ukraine. (2026b, August 4). *'The FSB will become anyone to make you a traitor': SBU launches new phase of anti-recruitment campaign*. <https://ssu.gov.ua/en/novyny/sbu-rozpochala-novu-khvyliu-informatsiinoi-kampanii-z-protydii-verbuvanniu-ukraintsiv-fsb-stane-kym-zavhodno-shchob-ty-stav-zradnykom>
11. State Service of Special Communications and Information Protection of Ukraine. (2026a, March 25). *Oleksandr Sukhodolia: Russian damage to Ukraine's energy grid unprecedented in modern history*. <https://cip.gov.ua/ua/news/oleksandr-sukhodolya-zbitki-yakikh-rf-zavdala-energetichnii-sistemi-ukrayini-ne-mayut-analogiv-u-suchasnii-istoriyi>

12. State Service of Special Communications and Information Protection of Ukraine. (2026b, June 4). *Russian aggression against Ukraine highlights vulnerability of Europe's own critical infrastructure, SSSCIP expert says*. <https://cip.gov.ua/ua/news/agresiya-rosiyi-proti-ukrayini-dopomogla-yevropeicyam-usvid-omiti-zagrozi-dlya-vlasnoyi-kritichnoyi-infrastrukturi-fakhivec-derzhspeczv-yazku>