

La guerre des infrastructures

Monde

Par François Véron

Publié le 3 septembre 2026

Managing Partner du fonds de capital innovation Newfund

Thomas Bodin

Analyst du fonds de capital innovation Newfund

Les deux belligérants de la guerre d'Ukraine traitent désormais les infrastructures civiles comme un théâtre décisif. Des drones filoguidés à 2 000 dollars y détruisent des transformateurs à 3,5 millions de dollars, malgré les sarcophages de béton censés les protéger. L'Ukraine répond par la décentralisation ; l'Europe ne possède ni la protection, ni l'architecture décentralisée.

U

*ne première version de ce texte, en anglais, est
parue sur le [blog de Newfund](#).*

En mai 2026, les équipes russes opérant près de Soumy ont mis au point une routine en deux temps. Un premier drone FPV, guidé par un câble de fibre optique fin comme un cheveu et donc insensible au brouillage, déchire le filet anti-drone tendu

au-dessus d'une sous-station électrique. Un second drone passe par la brèche, ou par les ouvertures de ventilation du sarcophage de béton situé dessous, et explose contre l'autotransformateur. Le drone coûte environ 2 000 dollars. L'autotransformateur de 330 kV coûte environ 3,5 millions de dollars et son remplacement prend des mois. Reuters a vérifié au moins quatre frappes de ce type sur des sous-stations que les ingénieurs ukrainiens décrivaient comme bien défendues.

Les sarcophages étaient eux-mêmes une réponse, conçue en 2023 contre les drones Shahed, et ils ont fonctionné. La tactique russe qui les contourne est apparue au printemps 2026. Dans cette guerre, une parade défensive reste efficace quelques mois, parfois quelques semaines, avant d'être contournée à son tour.

Le précédent de 1945

En 1945, le Strategic Bombing Survey américain a envoyé un millier d'enquêteurs dans les ruines de l'Allemagne pour établir ce que les bombardements stratégiques avaient obtenu. Le réseau électrique allemand, concluait sa division chargée des réseaux, s'était trouvé « dans un état précaire depuis le début de la guerre ». Les planificateurs allemands le savaient : les minutes secrètes du Comité central de planification montrent les longues discussions sur leur crainte que les Alliés ne découvrent l'extrême vulnérabilité du réseau. Mais les Alliés ne l'ont jamais découverte. Ils avaient jugé le réseau trop redondant, trop maillé, trop réparable pour mériter les sorties aériennes, et ont dirigé leurs bombardiers vers les villes, où la même enquête a constaté que la production avait continué d'augmenter jusqu'à la mi-1944. La cible décisive de la guerre industrielle est restée pour l'essentiel non bombardée parce que l'attaquant s'était trompé sur l'architecture d'un réseau.

Quatre-vingts ans plus tard, la Russie mène la campagne que les Alliés avaient débattue puis écartée, contre un réseau qu'elle

connaît intimement puisque des ingénieurs soviétiques l'ont construit. Environ 5 500 drones et missiles par mois ont visé les cibles énergétiques ukrainiennes au cours de l'hiver dernier, en salves allant jusqu'à 700 munitions en une seule nuit. Le résultat établit ce que le Survey avait laissé en suspens : un réseau moderne peut être brisé par une attaque soutenue. L'Ukraine est entrée en guerre avec 55 GW de capacité de production. En février 2026, elle disposait d'environ 11,5 GW, dans l'hiver le plus froid depuis 2010, avec des centrales de chauffage urbain délibérément visées par moins 20 °C. Les observateurs des droits de l'homme de l'ONU ont documenté ce qu'est une attaque de réseau dans un pays urbanisé : quand la sous-station tombe, les pompes à eau s'arrêtent, le réseau mobile s'éteint en quelques heures, les canalisations gèlent et éclatent, les égouts refoulent. Soixante-dix pour cent de la population urbaine ukrainienne vit en immeuble, où tout dépend de l'électricité.

L'Ukraine mène sa propre campagne d'infrastructures, dirigée contre un actif que la Russie ne peut pas décentraliser : les unités de traitement des hydrocarbures. Les drones ukrainiens ont frappé les raffineries russes 194 fois au premier semestre 2026 et ont atteint les onze plus grandes, dont Omsk, à 2 500 km de la frontière. Fin mars, des frappes sur les terminaux baltes d'Oust-Louga et de Primorsk ont immobilisé au moins 40 % de la capacité russe d'exportation de pétrole pendant une semaine. Le raffinage russe est tombé à son plus bas niveau depuis 2009. Les deux belligérants ont conclu, chacun de son côté, que les cibles au meilleur rendement de cette guerre sont les réseaux civils derrière la ligne de front. Ni l'un ni l'autre ne reviendra en arrière.

Quatre couches de défense

Quatre années de frappes ont fait de la défense d'infrastructures sous attaque soutenue une discipline à part

entière. Nous y distinguons quatre couches : protection passive, défense active, redondance, cyber.

La protection passive a donné les plus mauvais résultats. Le programme ukrainien à trois niveaux (gabions contre les débris, sarcophages de béton contre les Shaheds, enceintes antimissiles complètes pour 22 sous-stations critiques) s'est arrêté lorsque les coûts sont devenus prohibitifs. Les sarcophages, construits sur environ 69 sous-stations, arrêtent bien les Shaheds. Mais le troisième niveau n'a jamais été construit : un prototype testé fin 2023 a donné de bons résultats, puis le programme a sombré dans les impayés et les blocages administratifs, pour un coût projeté de plusieurs dizaines de millions de dollars par sous-station sur une centaine de sites. Et, depuis mai 2026, un FPV filoguidé à 2 000 dollars suffit à percer le deuxième niveau. La protection en béton coûte trop cher à généraliser et s'adapte moins vite que l'attaque.

La défense active a inversé le rapport de coûts entre l'attaquant et le défenseur. La Russie a lancé plus de 54 000 Shaheds en 2025, de 35 000 à 50 000 dollars pièce, contre des intercepteurs Patriot à 4,2 millions de dollars le tir. À ce rapport de prix, aucun stock occidental de missiles ne tient dans la durée. La réponse ukrainienne s'est construite presque entièrement hors du monde des grands contractants : un réseau national de détection acoustique de 14 000 capteurs à 400 à 1 000 dollars l'unité (coût total inférieur à 54 millions de dollars, soit moins de treize missiles Patriot), qui alimente en données de ciblage des drones intercepteurs à 1 000 à 5 000 dollars, produits par plus de vingt entreprises. En février 2026, les drones intercepteurs ont abattu plus de 70 % des Shaheds au-dessus de Kyiv et de sa périphérie, selon Oleksandr Syrskyi, alors commandant en chef, qui faisait état d'environ 6 300 sorties d'intercepteurs et de plus de 1 500 drones russes détruits sur ce seul mois (Ukrinform ; le chiffre est ukrainien et non vérifié de façon indépendante, mais l'analyse des coûts n'en

dépend pas). Environ 100 000 intercepteurs ont été produits en 2025 ; la capacité doit être multipliée par huit en 2026.

Puis, en mai 2026, la Russie a déployé le Geran-4, un Shahed à réaction volant à 500 km/h, et a rendu obsolète en quelques semaines la flotte d'intercepteurs à hélice. La contre-génération (des intercepteurs à réaction, un fabricant visant 50 000 unités par mois à partir d'août 2026) montait en cadence au moment où nous écrivons ces lignes. C'est la cadence de l'électronique grand public appliquée à la défense antiaérienne : une nouvelle génération de matériel tous les trois mois.

La décentralisation comme défense

La solution qui a permis à l'Ukraine de passer l'hiver est la redondance. Ayant conclu qu'un réseau centralisé ne peut pas être défendu à un coût acceptable, l'Ukraine se reconstruit en réseau décentralisé. Environ 1,5 GW de petite génération gazière distribuée est prévu pour la seule année 2026, autant que les quatre années de guerre réunies. Le solaire a ajouté 1,5 GW en 2025. Environ 3 GWh de batteries de réseau ont été installés en 2025, ce qui place l'Ukraine parmi les cinq marchés de stockage à la croissance la plus rapide d'Europe, en pleine guerre. DTEK et Fluence ont construit 200 MW / 400 MWh de stockage, délibérément répartis sur six sites pour réduire la cible, en six mois. Les télécoms suivent la même logique : itinérance nationale obligatoire, 120 000 batteries installées sur les pylônes, et le premier service satellite-vers-mobile en temps de guerre, lancé par Kyivstar et Starlink en novembre 2025, qui a atteint 3 millions d'utilisateurs en sept semaines. L'État avait montré la voie avec succès : les registres publics ont migré vers les grands clouds commerciaux dès 2022, et quatre années de frappes sur les data centers n'ont jamais mis l'État ukrainien hors service (le RUSI estime que cette seule décision a sauvé le gouvernement).

La protection parfaite d'un nœud de réseau est hors de prix, et elle est de surcroît provisoire. Une campagne contre les infrastructures peut être mise en échec par la décentralisation du réseau : assez de production distribuée, de stockage, de routage et de solutions de repli pour qu'aucune frappe isolée, ni aucun millier de frappes, ne produise de panne décisive. L'Ukraine se dote aujourd'hui de l'architecture que les Alliés prêtaient à tort au réseau allemand.

La décentralisation reste toutefois un problème de logistique avant d'être un problème de technologie, et l'Ukraine a connu des échecs dans ce domaine : des chaufferies d'urgence financées par des donateurs ont passé l'hiver 2025-2026 en entrepôt parce que personne n'avait organisé leur raccordement au réseau. Acheter les machines est la partie facile.

Les problèmes non résolus

Après un an de mesures et de contre-mesures, plusieurs problèmes restent sans solution en Ukraine, et ils concernent tout autant les réseaux européens.

La défense contre les FPV filoguidés reste à inventer : sans signature radio, ces drones échappent au brouillage comme à la détection radiofréquence, et les contrer supposera de combiner détection acoustique ou optique et neutralisation autonome à courte portée, site par site. L'interception des drones à réaction commence à peine, avec une contrainte simple : rester sous environ 10 000 dollars le tir contre une cible à 500 km/h, dans une course où chaque trimestre apporte sa génération. Le logiciel d'orchestration de réseau est un segment presque vide alors qu'il conditionne tout le reste : îlotage, redémarrage après effondrement, pilotage de milliers de petits actifs sous attaque ; l'Ukraine fait aujourd'hui cela à moitié manuellement. L'eau a des années de retard sur l'électricité : les stations de pompage n'ont pas même la protection de premier

niveau, et une charge de Shahed vient à bout de toute salle de contrôle non durcie. La cybersécurité des systèmes industriels tient, mais sur des effectifs minces : aucune attaque majeure réussie contre les systèmes de contrôle n'a été rendue publique depuis 2022, et cette défense repose sur une poignée d'équipes. La capacité satellitaire souveraine manque : environ 250 Gbit/s de débit Starlink au-dessus de l'Ukraine contre 5,5 Gbit/s pour OneWeb, en attendant la constellation européenne IRIS², prévue pour 2029-2030. Les grands transformateurs, enfin, sont un goulot d'étranglement mondial : 2,5 à 4 ans de délai pour les grandes unités, avant toute demande de guerre.

Presque chacun de ces problèmes est dual au sens littéral : le même capteur acoustique, le même contrôleur de microréseau, la même brique de cybersécurité industrielle servent un énergéticien en temps de paix et un ministère en temps de crise. Les segments matériels comptent déjà une vingtaine de fabricants ukrainiens et une dizaine de concurrents européens ; la couche d'orchestration, le logiciel qui fait de dix mille actifs dispersés un réseau capable de tenir sous le feu, ne mobilise aucune startup ni aucune entreprise du secteur pour le moment.

L'Europe face à la même menace

La campagne hybride contre les infrastructures européennes est déjà en cours. Onze câbles sous-marins baltes ont été endommagés dans les quinze mois précédant janvier 2025, ce qui a déclenché les patrouilles Baltic Sentry de l'OTAN. Des incursions de drones ont fermé des aéroports européens à répétition en 2025, et le survol de la Pologne par des drones russes en septembre 2025 a déclenché Eastern Sentry.

En cas de conflit ouvert, la Russie a déjà démontré ce dont elle est capable : des salves coordonnées de plusieurs centaines de drones et de missiles par nuit, soutenues pendant des mois,

contre des cibles électriques, gazières et de chauffage, avec des portées qui couvrent l'essentiel du continent. C'est ce que l'Ukraine a subi pendant l'hiver 2025-2026.

Les infrastructures européennes ne satisfont aucun des standards défensifs ukrainiens. Aucune sous-station de l'Union n'est sous sarcophage ; aucun pays européen n'est couvert par un réseau de détection acoustique ; il n'existe de stock massif d'intercepteurs nulle part dans l'Europe de l'OTAN, et l'European Drone Defence Initiative vise une capacité complète fin 2028, un délai dans lequel la Russie a fait tenir l'invention du contournement des sarcophages environ onze fois. La redondance du réseau européen a été conçue pour les tempêtes et le couplage des marchés, non pour l'attaque délibérée : en janvier 2026, la défaillance par le gel de deux lignes à haute tension a suffi à plonger la Moldavie dans le noir et à réduire le trafic internet de Kyiv et de Kharkiv de 46 %. La vulnérabilité la plus profonde est industrielle : les grands transformateurs de puissance, les composants que la Russie a appris à détruire pour 2 000 dollars, s'obtiennent en 2,5 à 4 ans en temps de paix, avec une demande mondiale déjà tirée par les data centers et aucune réserve stratégique significative en Europe.

Pendant ce temps, le savoir-faire s'exporte. La Lituanie a acheté le réseau de détection acoustique ukrainien en 2025. Les États-Unis en déploient un dérivé sur leurs bases et négocient l'achat d'intercepteurs ukrainiens. General Cherry, le premier fabricant ukrainien d'intercepteurs, ouvre une usine dans le New Hampshire. La seule filière de défense d'infrastructures éprouvée au feu ennemi est prête à s'exporter ; reste à savoir si l'Europe va acheter au rythme de la menace ou à celui de son système d'achat traditionnel.

Ce qui reste à organiser

Le programme SAFE de l'Union européenne, 150 milliards d'euros de prêts pour l'acquisition en commun, inscrit explicitement la protection des infrastructures critiques parmi ses priorités et finance déjà ses premiers contrats. La demande est dans la loi, mais la filière reste à constituer : personne n'a tracé le périmètre qui réunirait capteurs acoustiques, drones intercepteurs, logiciels de pilotage de microréseaux, cybersécurité industrielle et alternatives aux transformateurs, ni dans les statistiques, ni dans les politiques industrielles.

Les enquêteurs du Strategic Bombing Survey ont conclu que le réseau décisif de la dernière guerre industrielle n'avait pas été attaqué parce que l'attaquant s'était trompé sur son architecture. L'attaquant de cette guerre n'a pas répété l'erreur. L'Ukraine a redessiné l'architecture de son réseau sous les bombes et les missiles, en quatre ans, au prix des hivers les plus durs que ses civils aient connus depuis la Seconde Guerre mondiale. Une telle adaptation après coup est peut-être supportable pour une nation qui n'en a pas le choix, elle devrait être inacceptable comme plan pour quiconque peut encore choisir, et l'Europe peut encore choisir. Dans les précédents historiques, les institutions ne se sont ajustées qu'après la crise. La guerre des infrastructures ne devrait pas faire exception. Mais cette fois, la crise prendrait la forme de villes sans électricité, sans eau et sans communications, en plein hiver.