

CYBERATTAQUE VIASAT KA-SAT

24 Février 2022 — Un Cas d'École en Cyberguerre

Analyse technique et stratégique

Édité par AkDevSystem | Alexandre Kerbaol

Web <https://architecture-du-reel.fr> | Avril 2026

Classification Document confidentiel à usage pédagogique

Fiche d'identité de l'incident

Vue synthétique des caractéristiques essentielles de l'attaque

DATE DE L'INCIDENT

24 février 2022, 03h02 UTC

Quelques heures avant l'invasion terrestre de l'Ukraine

ATTRIBUTION

GRU russe (Sandworm / APT28)

Attribution confirmée par l'UE, les USA et le RU le 10 mai 2022

MALWARE UTILISÉ

AcidRain (wiper)

Effaceur de firmware, destruction complète en ~45 minutes

MODEMS AFFECTÉS

40 000 — 45 000

Plus de 30 000 modems de remplacement expédiés par Viasat

IMPACT MAJEUR

5 800 éoliennes Enercon (11 GW)

Perte de télésurveillance et de télécommande à distance

CLASSIFICATION

Attaque la plus perturbatrice

De la guerre russo-ukrainienne selon les analystes

AKDEVSYSTEM — Contact

Responsable : Alexandre Kerbaol

Email : alexk29@live.fr | Tel : 07 67 58 94 12

Adresse : Quai Nicolas Fouquet, BP63, 56360 Le Palais, France

Web : <https://architecture-du-reel.fr>

Sommaire

1. Contexte géopolitique et chronologie
 2. Le Groupe Viasat — Profil de l'entreprise
 3. Infrastructure réseau Viasat KA-SAT
 4. Vecteurs d'attaque et méthodologie
 5. Le malware AcidRain — Analyse technique
 6. Impact et dégâts
 7. Cas Enercon : effet de débordement critique
 8. Attribution et réponse internationale
 9. Enseignements et recommandations
 10. Note du rédacteur — Alexandre Kerbaol
 11. Sources et références
-

1. Contexte géopolitique et chronologie

Le 24 février 2022 marque un tournant historique dans l'histoire de la cyberguerre. Quelques heures avant le début de l'invasion terrestre russe de l'Ukraine, une attaque cybernétique d'une ampleur sans précédent frappe le réseau satellite KA-SAT de Viasat, fournisseur d'accès Internet par satellite majeur en Europe et en Ukraine.

Cette attaque n'est pas une coïncidence temporelle. Elle s'inscrit dans une stratégie dite « *hybrid warfare* » (guerre hybride), où les moyens cybernétiques sont employés en coordination avec les opérations militaires conventionnelles pour désorganiser les communications adverses, affaiblir la résilience civile et créer un brouillard de guerre informationnel.

Chronologie détaillée de l'attaque

23 fév. ~17h00**Tentative d'intrusion initiale**

Les attaquants ciblent le centre de gestion de Turin (Italie), exploité par Eutelsat/Skylogic pour le compte de Viasat. Après plusieurs échecs, ils parviennent à s'authentifier sur un VPN mal configuré — soit par défaut de paramétrage, soit via des identifiants déjà compromis — et pénètrent le réseau de gestion de confiance. Ce premier accès reste discret, sans déclencher d'alerte majeure.

24 fév. ~00h00**Reconnaissance et compromission des serveurs**

Une fois à l'intérieur, les attaquants effectuent une reconnaissance du réseau, identifient les serveurs de gestion critiques et atteignent le serveur de distribution des mises à jour firmware. Ce serveur, disposant de privilèges élevés, leur permet de préparer la propagation massive du malware vers l'ensemble des terminaux clients.

24 fév. 03h02 UTC**Déclenchement du double vecteur d'attaque**

Attaque DDoS coordonnée : les modems compromis émettent un trafic DHCP malveillant en boucle, saturant le réseau de gestion Viasat et empêchant toute réaction ou diagnostic en temps réel. Simultanément, le serveur de mise à jour commence la distribution d'AcidRain.

24 fév. 04h15 UTC

Déploiement massif d'AcidRain

Le malware **AcidRain** est poussé simultanément vers 40 000+ modems via le canal de mise à jour officiel. En environ 45 minutes, la mémoire flash de chaque terminal est écrasée. Les modems deviennent définitivement inopérants — un reset usine est impossible, le firmware étant totalement détruit.

24 fév. 05h00-08h00 UTC

Effondrement des communications

Perte totale de connectivité satellite pour les forces armées ukrainiennes, les commandements territoriaux, les hôpitaux de campagne et les infrastructures critiques civiles. En Europe, des milliers de clients résidentiels et professionnels constatent la panne. Les parcs éoliens Enercon perdent simultanément leur télésurveillance et leur télécommande à distance.

24 fév. Matinée

Constat et premier bilan

Viasat confirme une « anomalie réseau » affectant massivement ses modems KA-SAT. Les équipes de crise sont mobilisées. L'ampleur réelle de l'attaque n'est pas encore mesurée. L'Ukraine, coupée d'une partie de ses communications militaires stratégiques, évalue en urgence ses alternatives.

26 fév. ~48 h après

Contre-mesure ukrainienne : appel à Starlink

Mykhailo Fedorov, Vice-Premier ministre ukrainien, tweete directement Elon Musk pour solliciter l'activation de Starlink sur le territoire ukrainien. Elon Musk répond en moins de 10 heures et annonce le déploiement. Les premiers terminaux arrivent dès le lendemain.

28 fév. - 1er mars

Starlink opérationnel en Ukraine

Les premiers kits Starlink (antennes + routeurs) arrivent en Ukraine. En moins de 72 heures après la demande officielle, le service est partiellement opérationnel, fournissant une connectivité par satellite alternative et redondante aux forces armées et aux infrastructures critiques ukrainiennes.

2. Le Groupe Viasat — Profil de l'entreprise

Comprendre l'attaque du 24 février 2022 nécessite de connaître l'acteur qui en a été la cible : **Viasat Inc.**, l'un des plus grands opérateurs de télécommunications par satellite au monde. Cette section présente le profil complet du groupe, son histoire, son périmètre d'activités et les jalons qui ont conduit au contrôle du réseau KA-SAT, quelques mois seulement avant la cyberattaque.

Fiche d'identité de l'entreprise

Tableau 1 — Informations générales sur Viasat Inc.

INDICATEUR	DÉTAIL
Dénomination	Viasat Inc. (anciennement ViaSat Inc.)
Fondation	Mai 1986, Carlsbad, Californie
Fondateurs	Mark Dankberg, Mark Miller, Steve Hart (anciens ingénieurs de Linkabit)
Capital initial	25 000 USD (bootstrap, sans VC)
Siège social	6155 El Camino Real, Carlsbad, Californie 92009
Cotation boursière	NASDAQ : VSAT
Capitalisation boursière	~7,7 Mds USD (avril 2026)
Effectifs	~7 000 employés dans 24+ pays
Chiffre d'affaires (FY2025)	4,52 Mds USD (+5,5% vs FY2024)
Secteur d'activité	Télécommunications par satellite — Broadband, Mobilité, Défense, Gouvernement

Chronologie du développement de Viasat

1986	Création à Carlsbad Trois ingénieurs de Linkabit (pionnier des communications satellite) fondent Viasat avec 25 000 USD dans une maison privée. Premiers contrats de défense et développement de modems DAMA (Demand Assigned Multiple Access) pour les militaires.
1996	Introduction en bourse Viasat entre au NASDAQ. L'entreprise diversifie son portefeuille vers le commercial tout en conservant une forte présence dans le secteur de la défense.
2011	Lancement de ViaSat-1 ViaSat-1 établit un record de capacité satellite : 140 Gbps, soit plus que la totalité des satellites Nord-Américains réunis à l'époque. Viasat bascule de fabricant de composants à opérateur de services broadband.
2016	Joint-venture avec Eutelsat Viasat et Eutelsat créent Euro Broadband Infrastructure (EBI). Eutelsat apporte KA-SAT et détient 51 % ; Viasat apporte sa technologie et détient 49 % pour 132,5 M EUR. Objectif : développer le marché européen du broadband satellite.
2020	Acquisition des parts d'Eutelsat Viasat rachète les 51 % restants d'Eutelsat dans EBI pour 140 M EUR (166 M USD). Le groupe devient propriétaire à 100 % du satellite KA-SAT et de toute l'infrastructure sol associée. L'acquisition est finalisée en avril 2021.
Mai 2023	Acquisition d'Inmarsat Viasat finalise le rachat d'Inmarsat pour 7,3 Mds USD, créant un géant mondial des communications satellite multi-orbites (GEO + LEO). Le groupe double de taille et étend sa présence dans la mobilité maritime et aéronautique.

FY2025

Chiffre d'affaires record

Viasat atteint 4,52 Mds USD de revenus annuels, en croissance de +5,5 %, portée par l'intégration d'Inmarsat et la diversification de ses activités broadband, mobilité et gouvernement.

Périmètre d'activités

Tableau 2 — Segmentation des activités de Viasat

SEGMENT	DESCRIPTION	CLIENTS
Broadband résidentiel	Internet haut débit par satellite pour zones rurales et mal desservies	Particuliers, PME, zones rurales (USA, Europe, Amérique latine)
Mobilité aéronautique	Connectivité en vol (IFC — In-Flight Connectivity) pour compagnies aériennes	Compagnies aériennes, avions commerciaux et d'affaires
Mobilité maritime	Communications haut débit pour navires et plates-formes offshore	Armateurs, croisières, pêche, offshore (via Inmarsat)
Gouvernement & Défense	Communications sécurisées, réseaux tactiques, systèmes cryptographiques	US DoD, OTAN, agences gouvernementales européennes et alliées
Entreprises & Énergie	Broadband professionnel, communications d'urgence, IoT industriel	Industrie, énergie, services d'urgence, administrations

Viasat et le réseau KA-SAT : une acquisition stratégique

Le satellite KA-SAT, lancé en décembre 2010 par Eutelsat, représentait une capacité de 90 Gbps en orbite géostationnaire à 9° Est, couvrant l'Europe, le Moyen-Orient et le bassin méditerranéen. Après avoir co-exploité ce satellite via la joint-venture EBI, Viasat a pleinement contrôlé KA-SAT à partir d'avril 2021 — moins d'un an avant la cyberattaque.

Cette chronologie est significative : la transition d'un modèle de co-exploitation à une gestion directe et intégrée a pu introduire des vulnérabilités opérationnelles. Le centre de gestion de Turin, hérité de l'ancienne organisation Eutelsat, est précisément le point d'entrée utilisé par les attaquants. L'acquisition d'Inmarsat en 2023, bien qu'elle ait renforcé le périmètre mondial de Viasat, a également complexifié l'homogénéité des politiques de sécurité à travers les différentes infrastructures héritées.

■ Point clé

Au moment de l'attaque (février 2022), Viasat venait de finaliser son acquisition totale de KA-SAT. Le groupe était en phase de consolidation de ses systèmes et de migration des infrastructures — une période où la surface d'attaque est souvent maximale et où la surveillance de sécurité peut présenter des lacunes.

Ramifications européennes — Un écosystème de dépendances

L'attaque contre Viasat n'a pas touché un acteur isolé. Elle a frappé le nœud central d'un **écosystème de dépendances européennes** tissé depuis plus d'une décennie, impliquant opérateurs satellite, distributeurs, fournisseurs d'énergie, compagnies aériennes et infrastructures militaires alliées.

Partenaires et co-contractants européens

Tableau 3 — Acteurs européens liés à Viasat et au réseau KA-SAT

ACTEUR EUROPÉEN	PAYS	NATURE DU LIEN AVEC VIASAT	IMPACT DE L'ATTAQUE
Eutelsat Communications	France	Co-fondateur de la JV EBI (2016-2021), opérateur historique de KA-SAT, fournisseur de services transitoires post-acquisition	Rupture de la chaîne de distribution ; Eutelsat avait déjà pivoté vers Konnect VHTS
Skylogic (Eutelsat)	Italie	Opérateur du centre de gestion de Turin — le point d'entrée de l'attaque	Centre de gestion compromis via VPN mal configuré
Bigblu Broadband Europe	UK, Irlande, France, Allemagne, Italie, Espagne, Portugal, Pologne, Hongrie, Grèce	Distributeur wholesale acquis par Eutelsat (~50 000 abonnés) ; client de capacité KA-SAT	Perte de connectivité pour ~50 000 abonnés répartis sur 10 pays

Orange (France Telecom)	France	A acheté toute la capacité française sur le satellite Eutelsat Konnect (successeur de KA-SAT)	Indirect — confirmation de la stratégie de diversification d'Orange
Telecom Italia (TIM)	Italie	A acquis toute la capacité italienne sur Eutelsat Konnect et Konnect VHTS	Indirect — TIM n'était plus dépendant de KA-SAT à ce moment
Brdy	Royaume-Uni, Europe du Nord	Partenaire revendeur Viasat pour le broadband satellite professionnel en Europe	Service interrompu pour clients professionnels britanniques et nordiques
Finnair	Finlande	Client de connectivité en vol Viasat/Eutelsat sur flotte A320	Pas d'impact direct (réseau aéronautique séparé)
Enercon	Allemagne	Client de supervision satellite via KA-SAT pour 5 800 turbines	5 800 éoliennes sans télésurveillance ni télécommande

Clients militaires et gouvernementaux européens

Au-delà du secteur commercial, Viasat est un **contractant de plusieurs organisations de défense européennes et alliées** :

- **OTAN** — Viasat fournit des équipements de communication sécurisés et des systèmes cryptographiques pour les forces alliées.
- **Royal Navy (UK)** — La marine britannique utilise des terminaux Viasat pour ses communications satellite.
- **Forces armées ukrainiennes** — Bien qu'ukrainienne, l'armée ukrainienne utilisait KA-SAT comme canal de communication militaire via des contrats de Viasat.
- **Agences de cybersécurité européennes** — L'attaque a conduit l'ENISA, l'ANSSI française et le NCSC britannique à enquêter conjointement avec la NSA américaine.

Impact par pays européens

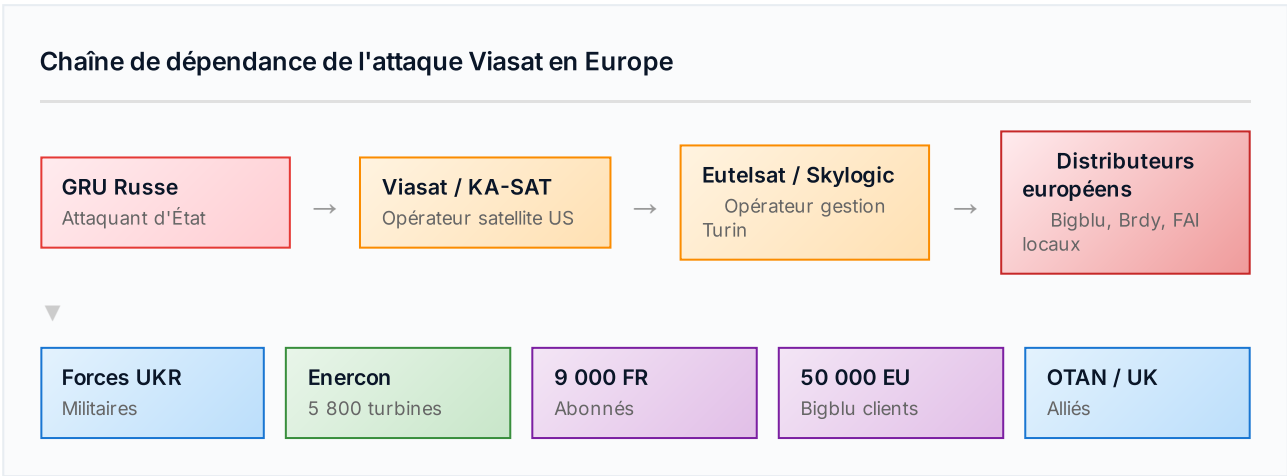
Tableau 4 — Impact de l'attaque par pays européen

PAYS	TYPE D'IMPACT	ESTIMATION
Ukraine	Perte de communications militaires et civiles, « huge loss of communications » (Victor Zhora)	Majorité des modems actifs du pays HS

Allemagne	5 800 éoliennes Enercon sans supervision + clients broadband	~11 GW de capacité éolienne non supervisée
France	Près de 9 000 abonnés d'un FAI satellite	9 000 modems hors service
Pologne	Clients broadband KA-SAT impactés	Milliers de modems
Royaume-Uni	Clients Bigblu Broadband et utilisateurs professionnels	Milliers de modems
Tchéquie	Clients broadband KA-SAT impactés	Centaines de modems
Italie, Espagne, Grèce, Hongrie	Clients Bigblu Broadband Europe	Distribution proportionnelle des ~50 000 abonnés Bigblu

La chaîne de dépendance critique

Cette attaque illustre un mécanisme de **propagation en cascade** propre aux infrastructures critiques interconnectées :



■ Constat stratégique

L'attaque Viasat n'a pas seulement visé une entreprise américaine. Elle a exploité une **chaîne de dépendances transatlantique** où un point d'entrée en Italie (Skylogic/Turin) a permis de paralyser des infrastructures critiques dans au moins **7 pays européens**, incluant des fonctions militaires (Ukraine, OTAN), énergétiques (Enercon/Allemagne) et civiles (9 000 abonnés en France, 50 000 via Bigblu). Cette interdépendance est le résultat

direct d'une stratégie de Viasat visant à intégrer verticalement un écosystème européen hérité de son partenariat avec Eutelsat.

3. Infrastructure réseau Viasat KA-SAT

Le service KA-SAT est une infrastructure de communication par satellite à haut débit couvrant l'Europe, le Moyen-Orient et une partie de l'Afrique du Nord. Elle repose sur une architecture en étoile classique de type VSAT (Very Small Aperture Terminal).

Architecture technique

Tableau 5 — Architecture en couches du réseau KA-SAT et rôle dans l'attaque

COUCHE	COMPOSANT	FONCTION	RÔLE DANS L'ATTAQUE
Espace	Satellite KA-SAT (Eutelsat)	Relais radiofréquence en bande Ka	Non compromis directement
Segment sol	Hubs / Gateways (Turin, etc.)	Concentration du trafic, routage vers Internet	Point d'entrée via VPN mal configuré
Segment sol	Serveurs de gestion	Supervision, provisioning, authentification	Compromis — accès latéral
Segment sol	Serveur de mise à jour	Distribution du firmware aux modems	Compromis — vecteur de propagation
Utilisateur	Modems VSAT clients	Terminaux d'accès satellite (antenne + modem)	Cibles finales du wiper AcidRain
Utilisateur	Réseaux LAN clients	Réseaux internes des abonnés	Impact indirect (Enercon, etc.)

Flux d'attaque





Ukraine

Communications
militaires HS

Enercon

5 800 turbines
aveuglées

Europe

Accès Internet coupés



26/02

Starlink

Opérationnel en 72h

Point clé d'architecture

Le segment sol, et non le segment spatial (satellite), constitue le maillon faible. Les attaquants n'ont pas eu besoin de compromettre le satellite en orbite — une intrusion dans l'infrastructure terrestre de gestion a suffi à paralyser l'ensemble du service.

4. Vecteurs d'attaque et méthodologie

Vecteur initial : le VPN mal configuré

L'entrée dans le réseau s'est faite via un point d'accès VPN au centre de gestion de Turin, exploité par Eutelsat/Skylogic pour le compte de Viasat. Ce VPN, mal configuré ou doté de certificats/identifiants compromis, a permis aux attaquants de s'authentifier et de pénétrer le réseau de gestion de confiance.

Mouvement latéral et élévation de privilèges

Une fois à l'intérieur du réseau de gestion, les attaquants ont procédé à un mouvement latéral (*lateral movement*) pour atteindre le serveur de distribution des mises à jour firmware. Ce serveur, critique pour la gestion à distance des parcs de modems, disposait des privilèges nécessaires pour pousser du code exécutable vers l'ensemble des terminaux clients.

Double vecteur d'attaque final

Tableau 6 — Les deux vecteurs d'attaque déployés simultanément

VECTEUR	MÉCANISME	OBJECTIF	RÉSULTAT
DDoS DHCP	Modems compromis émettent un trafic DHCP malveillant en boucle	Saturation du réseau de gestion, déni de service	Paralysie des capacités de réponse et de diagnostic
Wiper AcidRain	Écrasement de la mémoire flash des modems avec des données aléatoires	Rendre les terminaux physiquement inopérants	40 000+ modems HS, nécessitant remplacement ou reset usine

5. Le malware AcidRain — Analyse technique

AcidRain est un malware de type *wiper* (effaceur), conçu spécifiquement pour détruire la mémoire flash des équipements embarqués. Il ne vise pas à exfiltrer des données ni à établir une persistance long terme : son objectif est la destruction rapide et irréversible des terminaux.

Caractéristiques techniques

Tableau 7 — Propriétés techniques du malware AcidRain

PROPRIÉTÉ	DESCRIPTION
Type	Wiper / Destructeur de firmware
Cible	Mémoire flash des modems VSAT (architecture MIPS/ARM)
Mécanisme	Écrasement des blocs de mémoire avec des données aléatoires ou un pattern fixe
Vitesse	Destruction complète en ~45 minutes pour un parc de 40 000+ modems
Persistance	Aucune — destruction immédiate et irréversible
Lien VPNFilter	Similitudes techniques « non triviales » avec le malware VPNFilter (2018), attribué au GRU par FBI/NSA
Détection	Difficile à détecter avant exécution car distribué via canal de mise à jour légitime

■ Particularité stratégique

AcidRain a été distribué via le canal de mise à jour officiel du serveur de provisioning. Cela signifie que les modems ont reçu et exécuté le malware en toute confiance, pensant installer une mise à jour firmware légitime. Cette technique, dite « *supply chain attack* » ou attaque de la chaîne d'approvisionnement logicielle, rend la détection préventive extrêmement difficile.

6. Impact et dégâts

Bilan quantitatif

Tableau 8 — Bilan quantitatif des impacts de l'attaque

INDICATEUR	VALEUR	COMMENTAIRE
Modems rendus inopérants	40 000 — 45 000	Données Viasat ; ENISA cite « au moins 27 000 »
Zones géographiques touchées	Ukraine, Allemagne, France, Pologne, UK, Tchéquie, etc.	Effet de débordement continental
Éoliennes Enercon sans supervision	5 800	Capacité totale : ~11 gigawatts
Modems de remplacement expédiés	> 30 000	Intervention logistique massive de Viasat
Durée de restauration	Plusieurs jours à semaines	Selon la criticité et la localisation
Coût estimé	Non divulgué	Viasat évoque des pertes « matérielles importantes »

Impact militaire ukrainien

Selon Victor Zhora, responsable ukrainien de la cybersécurité, l'attaque a provoqué une « *huge loss of communications* » (perte massive de communications) pour les forces armées ukrainiennes au moment précis où l'invasion terrestre débutait. Cette déconnexion a contraint l'Ukraine à solliciter en urgence l'aide de Starlink, qui s'est révélé plus résistant aux brouillages et aux attaques cybernétiques.

Impact civil européen

Au-delà de l'Ukraine, des milliers de clients résidentiels et professionnels en Europe ont perdu leur accès Internet. Des entreprises, des administrations et des infrastructures critiques ont été touchées, illustrant la vulnérabilité des dépendances croisées dans l'écosystème numérique européen.

Le rôle décisif de Starlink : une réponse en moins de 72 heures

Face à l'effondrement de ses communications satellite, l'Ukraine a dû trouver une solution de remplacement en un temps record. C'est dans ce contexte d'urgence absolue que Starlink, le réseau satellite à constellation basse orbite (LEO) d'Elon Musk, est intervenu.

Chronologie de l'intervention Starlink

26 fév. 10h28	Demande officielle ukrainienne Mykhailo Fedorov, Vice-Premier ministre ukrainien chargé de la transformation numérique, adresse un tweet public à Elon Musk : « @elonmusk, pendant que vous essayez de coloniser Mars, la Russie essaie d'occuper l'Ukraine ! [...] Nous vous demandons de fournir à l'Ukraine des stations Starlink. »
26 fév. ~20h00	Réponse immédiate d'Elon Musk En moins de 10 heures, Elon Musk répond sur Twitter : « Starlink service is now active in Ukraine. More terminals en route. » Le service est techniquement activé dès la réponse, avant même l'arrivée physique du matériel.
28 fév. - 1er mars	Arrivée des terminaux et déploiement Un premier convoi de kits Starlink (antennes paraboliques motorisées, routeurs, blocs d'alimentation) traverse la Pologne et atteint l'Ukraine. En moins de 72 heures après la demande initiale, les premiers terminaux sont opérationnels sur le terrain. Le débit offert atteint 50-150 Mbps par terminal, avec une latence de 20-40 ms.
Mi-mars 2022	Contribution opérationnelle confirmée Plus de 5 000 terminaux Starlink sont déployés en Ukraine. Le service assure les communications des forces armées, des hôpitaux, des services d'urgence et des infrastructures critiques. Starlink s'avère plus résistant aux tentatives de brouillage russes que les systèmes géostationnaires traditionnels.

Pourquoi Starlink a-t-il été si efficace ?

Tableau 9 — Comparaison technique Viasat KA-SAT vs. Starlink

CARACTÉRISTIQUE	VIASAT KA-SAT	STARLINK

Type d'orbite	Géostationnaire (GEO) à ~36 000 km	Orbite basse (LEO) à ~550 km
Débit par terminal	Jusqu'à 50 Mbps	50-150 Mbps
Latence	600-700 ms	20-40 ms
Couverture cible	Europe, Moyen-Orient, Afrique du Nord	Global (constellation en déploiement)
Résilience au brouillage	Vulnérable (satellites fixes, fréquences prévisibles)	Plus résistant (satellites mobiles, faisceaux directionnels, mise à jour OTA)
Fiabilité post-attaque	40 000+ modems détruits, service partiellement indisponible pendant des semaines	Aucune compromission, service opérationnel en 72 h sur le terrain ukrainien

Leçon opérationnelle : la redondance sauve des vies

La rapidité de déploiement de Starlink — 72 heures entre la demande et l'opérationnel — illustre une rupture fondamentale dans la géopolitique des infrastructures critiques. Pour la première fois, une entreprise privée a fourni une capacité de communication militaire-grade en réponse à une cyberattaque d'État en temps réel. Cet épisode a conduit de nombreux analystes à considérer Starlink comme un acteur géopolitique à part entière, et non plus comme un simple fournisseur de connectivité.

7. Cas Enercon : effet de débordement critique

C'est ici que l'incident devient particulièrement intéressant pour un ingénieur : Enercon est l'un des plus grands constructeurs d'éoliennes au monde. Le 24 février 2022, 5 800 de ses éoliennes — représentant une capacité de production d'environ 11 gigawatts — ont perdu simultanément leur télésurveillance et leur télécommande à distance.

Architecture de dépendance : un single point of failure

Les parcs éoliens d'Enercon utilisaient le réseau satellite KA-SAT de Viasat comme *backbone* de communication unique pour la télésurveillance de 5 800 turbines réparties sur plusieurs pays européens (Allemagne, France, Pologne, Espagne, Portugal, Grèce, etc.). Cette architecture, bien que courante dans l'industrie des énergies renouvelables, reposait sur un **fournisseur unique de connectivité** sans redondance active.

Les parcs éoliens sont souvent situés dans des zones géographiquement isolées — zones rurales, collines, sites *offshore* — où le déploiement de fibre optique ou de liaisons terrestres dédiées représente un coût élevé. Le satellite apparaissait donc comme une solution économique et pragmatique. Mais cette approche a créé une **dépendance critique** sans plan de continuité opérationnelle.

Données chiffrées de l'incident Enercon

Tableau 10 — Bilan chiffré de l'impact sur Enercon

INDICATEUR	VALEUR	CONTEXTE
Turbines affectées	5 800	Environ 40 % du parc mondial Enercon à cette date
Capacité de production	~11 GW	Équivalent à environ 3 réacteurs nucléaires EPR
Pays touchés	7+	Allemagne, France, Pologne, Espagne, Portugal, Grèce, Turquie
Durée de la coupure de supervision	Plusieurs jours	Aucune basculement automatique vers un réseau de secours
Production électrique interrompue	Non	Grâce au mode autonome des turbines

Intervention nécessaire	humaine	Oui, sur chaque site	Envoi d'équipes techniques pour vérification et monitoring local
-------------------------	---------	----------------------	--

Conséquences opérationnelles

Tableau 11 — Conséquences opérationnelles sur les parcs éoliens Enercon

FONCTION AFFECTÉE	IMPACT	MITIGATION
Télesurveillance (SCADA)	Perte de visibilité temps réel sur l'état des turbines	Mode automatique/local activé
Télécommande	Impossibilité d'arrêter/démarrer à distance	Intervention sur site nécessaire
Maintenance prédictive	Pas de remontée de données de capteurs	Maintenance programmée différée
Production d'énergie	NON INTERROMPUE	Les turbines sont passées en mode autonome
Sécurité	Risque accru (pas d'arrêt d'urgence à distance)	Surveillance humaine renforcée sur site

Leçon clé pour l'ingénierie des systèmes critiques

Les turbines Enercon ont continué de produire de l'électricité grâce à un mode de fonctionnement dégradé/autonome. Cette conception — où le système local garde une capacité opérationnelle minimale sans connectivité — a évité une coupure électrique massive. C'est un principe fondamental de la résilience : la défaillance d'un sous-système de communication ne doit pas entraîner l'arrêt total du système physique.

■ Le phénomène de « spillover » (débordement)

Une attaque cybernétique ciblant des communications militaires en Ukraine a eu des effets collatéraux directs sur l'infrastructure énergétique allemande. Cela illustre l'interdépendance critique des infrastructures modernes et la difficulté à prévoir les chaînes de défaillance en cascade.

8. Attribution et réponse internationale

Attribution au GRU russe

L'attaque est officiellement attribuée au GRU (Direction principale du renseignement général des forces armées russes), et plus spécifiquement au groupe Sandworm (également connu sous APT28). Les preuves techniques reposent sur :

- Similitudes techniques entre AcidRain et VPNFilter (malware 2018 attribué au GRU par le FBI et la NSA), qualifiées de « non triviales » par les analystes.
- La chronologie : l'attaque coïncide exactement avec le début de l'invasion de l'Ukraine.
- La méthodologie : utilisation d'un wiper massif pour détruire des infrastructures de communication, signature des opérations du GRU.

Réponse internationale (10 mai 2022)

Le 10 mai 2022, l'Union européenne, les États-Unis et le Royaume-Uni ont publié une déclaration commune condamnant officiellement la Russie pour cette attaque. Cette attribution internationale coordonnée est rare en cybersécurité et témoigne de la gravité de l'incident.

« L'attaque cybernétique contre le réseau satellite Viasat le 24 février 2022 a eu un impact significatif sur les communications civiles et militaires ukrainiennes, ainsi que sur les infrastructures critiques en Europe. Cette attaque fait partie d'une campagne de cyberattaques menée par la Russie contre l'Ukraine. »

— Déclaration commune UE / États-Unis / NCSC UK, 10 mai 2022

9. Enseignements et recommandations

Pour les architectes réseau et système

Tableau 12 — Enseignements et applications pour les architectes système

ENSEIGNEMENT	APPLICATION CONCRÈTE
Segmentation stricte	Isoler physiquement ou logiquement les réseaux de gestion des réseaux de production/mise à jour
Hygiène VPN	Configuration rigoureuse, MFA, rotation des certificats, monitoring des accès
Mode dégradé/autonome	Concevoir les systèmes critiques pour fonctionner sans connectivité externe
Chaîne d'approvisionnement	Signer et vérifier cryptographiquement toutes les mises à jour firmware
Redondance de connectivité	Ne pas dépendre d'un seul fournisseur de backbone (satellite + terrestre)
Détection d'anomalies	Surveiller les patterns de trafic DHCP et les distributions de firmware massives
Plan de continuité	Procédures documentées pour basculer sur réseau secondaire en moins de 4 heures
Cartographie des dépendances	Identifier et documenter toutes les interdépendances critiques (ex : Enercon → Viasat)

Pour les infrastructures critiques (type Enercon)

- **Dual-homing** : connectivité satellite + liaison terrestre (4G/5G/fibre) avec basculement automatique.
- **SCADA air-gapped** : maintenir une capacité de supervision locale indépendante du cloud.
- **Tests de résilience** : simulations régulières de coupure de communication satellite.
- **Contrats de SLA** : exiger des fournisseurs de connectivité des garanties de redondance et des plans de continuité documentés.

10. Note du rédacteur — Alexandre Kerbaol

■ À propos de l'auteur

Alexandre Kerbaol est le fondateur d'AkDevSystem, société spécialisée en architecture des systèmes d'information et cybersécurité des infrastructures critiques. Depuis 1997, il conçoit et intègre des systèmes de haute disponibilité prévoyant des solutions de secours en temps réel.

Un constat d'architecte : l'inexcusable fragilité

Depuis 1997, j'ai intégré des systèmes de haute disponibilité prévoyant des solutions de secours en temps réel sur les serveurs, les redondances concernant les réseaux de télécommunication pour palier à ce genre de « pannes réseaux » sans nécessiter l'intervention humaine. L'architecture était déjà autonome pour détecter et basculer automatiquement sur le système de secours.

Il est aberrant, à notre époque, que des groupes de l'envergure de Viasat, Enercon et d'autres acteurs critiques de l'écosystème énergétique et télécom européen se soient appuyés sur un **unique système de télécommunication** pour leur supervision. Cette configuration, qualifiable de défaut architectural flagrant, constitue ce que l'on nomme en ingénierie un *single point of failure* — un point unique de défaillance dont la rupture paralyse l'ensemble du système.

Le principe fondamental de toute architecture résiliente est pourtant clair : **aucun sous-système critique ne doit reposer sur une voie unique**. Cela s'appelle la redondance active, le *dual-homing*, la diversité de routage — des concepts établis depuis des décennies, que j'ai implémentés dès 1997 pour des infrastructures bancaires et télécom françaises.

Une aberration architecturale, pas une fatalité

Ce qui s'est produit le 24 février 2022 n'est pas le résultat d'une sophistication technique insurmontable des attaquants. C'est le fruit direct d'une **négligence architecturale** : un VPN mal configuré, un serveur de mise à jour sans segmentation, 40 000 modems sans mécanisme de vérification cryptographique du firmware, et surtout — aucune redondance de connectivité pour des infrastructures classées critiques.

Les groupes pour lesquels j'ai travaillé — France Telecom, le Crédit Agricole, Predica, Pacifica, Indosuez, Free, Iliad — ont tous basé leurs systèmes sur cette exigence de redondance. Ils savaient qu'une panne réseau, qu'elle soit accidentelle ou malveillante, est non pas un risque hypothétique mais un événement statistiquement certain. La seule question est quand, pas si.

Ce que l'incident révèle sur la maturité cyber des infrastructures critiques européennes

Ce cas d'école devrait alerter l'ensemble des décideurs techniques européens. Quand une cyberattaque contre un opérateur satellite peut à la fois paralyser les communications militaires d'un pays en guerre **et** aveugler la supervision de 5 800 éoliennes représentant 11 GW de capacité de production électrique, nous ne sommes plus face à un risque informatique : nous sommes face à un **risque systémique de société**.

La différence entre une panne gérable et une catastrophe systémique ne réside pas dans la complexité de l'attaque, mais dans la robustesse de l'architecture qui la subit. Le mode dégradé autonome des turbines Enercon a sauvé la production électrique — mais il n'aurait pas dû être le dernier rempart. Une architecture correctement conçue aurait prévu une bascule automatique vers un réseau de secours dès la détection de la perte de connectivité Viasat.

Le verdict d'architecte

Ce qui s'est passé le 24 février 2022 n'est pas une cyberattaque exceptionnelle par sa sophistication technique. C'est un **défaut d'architecture basique** — la dépendance à un fournisseur unique sans redondance — qui a transformé une intrusion modérée en effondrement systémique. Des groupes comme Viasat et Enercon, acteurs critiques de la souveraineté énergétique et communicationnelle européenne, devaient savoir que la redondance n'est pas une option : c'est une obligation. C'est le constat factuel que je tire de près de 30 ans d'architecture de systèmes critiques.

— Alexandre Kerbaol, AkDevSystem, avril 2026

11. Sources et références

Rapports officiels et analyses techniques

1. ENISA — « Viasat KA-SAT cyber incident » (rapport d'analyse post-incident)
2. SentinelOne — Analyse du malware AcidRain et liens avec VPNFilter
3. Viasat — Communiqués post-incident et témoignage de Mark Colaluca (CISO)
4. Union européenne / État américain / NCSC UK — Déclaration commune du 10 mai 2022
5. Reuters / Associated Press — Couverture journalistique de l'impact sur Enercon
6. Victor Zhora (SSSCIP Ukraine) — Déclarations sur la perte de communications militaires

MOTS-CLÉS : AcidRain, Viasat KA-SAT, VPNFilter, Sandworm APT, GRU cyberattaque, Enercon wind turbines, satellite network cyberattack, supply chain attack firmware, wiper malware 2022, Ukraine cyberwar Starlink.



AKDEVSYSTEM

l'innovation dans chaque ligne de code.

Document généré à des fins pédagogiques. Ce cas d'école vise à illustrer les enjeux de la cybersécurité des infrastructures critiques et l'importance de la résilience architecturale.

Responsable : Alexandre Kerbaol | **Email** : alexk29@live.fr | **Tél** : 07 67 58 94 12

Adresse : Quai Nicolas Fouquet, BP63, 56360 Le Palais, France | **Web** : <https://architecture-du-reel.fr>