

Incidents critiques, infrastructures et signaux de résilience en 2026

Recensement janvier-octobre 2026

206 événements critiques ou signaux majeurs recensés depuis janvier 2026.

Cyberattaques, énergie, télécommunications, câbles sous-marins, GNSS, transports et flux stratégiques.

Montée des mesures de préparation civile, militaire et de continuité des services essentiels.

JANVIER 2026

Date	Pays / zone	Catégorie	Événement
2 janv.	Lituanie / Lettonie	Télécommunications / câbles	Câble sous-marin de télécommunications endommagé en mer Baltique.
2 janv.	République du Congo	Internet / câbles	Rupture du câble sous-marin WACS ; trafic Internet en chute jusqu'à environ 82 %.
3 janv.	Allemagne	Énergie / sabotage	Sabotage du réseau électrique à Berlin ; près de 100 000 personnes privées d'électricité et de chauffage.
4 janv.	Grèce	Transport aérien	Panne majeure des communications aériennes ; espace aérien paralysé pendant plusieurs heures.
8 janv.	Iran	Internet	Blackout Internet à l'échelle nationale.
8 janv.	International	Cyber / IA	Reconnaissance massive d'infrastructures IA exposées ; plus de 91 000 sessions détectées.
8 janv.	Europe / Croatie	Énergie / réseau électrique	Incident sur le réseau européen ; fréquence tombée à 49,8 Hz et protections automatiques déclenchées.
8 janv.	France	Militaire / résilience	Présentation d'ORION 26, exercice de haute intensité intégrant environnement dégradé et résilience nationale.
Janvier	Lituanie / Baltique	GPS / aviation	Forte activité de brouillage et spoofing GPS ; 169 incidents signalés par des pilotes durant le mois.
12 janv.	France	Militaire / anti-drone	La lutte anti-drone qualifiée d'« urgence opérationnelle » face à l'accroissement de la menace.
13 janv.	Pologne	Énergie / cyber	Révélation d'une cyberattaque destructive contre plusieurs infrastructures énergétiques.

Date	Pays / zone	Catégorie	Événement
14 janv.	États-Unis	Télécommunications	Panne nationale du réseau mobile Verizon.
15 janv.	Europe / OTAN	Militaire / préparation	Lancement de Steadfast Dart 2026 ; 10 000 militaires de 11 pays et premier déploiement de l'Allied Reaction Force.
21 janv.	International	Cyber	Vulnérabilité critique Cisco activement exploitée.
26 janv.	International	Internet / réseau	Incident BGP chez Cloudflare ; perturbations réseau à portée mondiale.
26 janv.	International	Cyber	Faible zero-day Microsoft Office activement exploitée.
26 janv.	États-Unis	Militaire / résilience	Début de Citadel Shield-Solid Curtain 2026, exercice de protection des installations de l'US Navy.
27 janv.	Suisse / Europe	Transport aérien / infrastructure	Défaillance informatique du contrôle aérien à Genève ; espace aérien temporairement fermé et vols déroutés.
29 janv.	International	Cyber	Vulnérabilités critiques Ivanti ; exploitation active signalée.
29 janv.	France	Préparation civile / résilience	Diffusion du guide « Tous responsables » préparant la population aux crises majeures et ruptures de services.
31 janv.	Ukraine / Moldavie	Énergie / réseau électrique	Incident majeur ; coupures importantes et séparation temporaire du réseau électrique continental européen.

Bilan janvier 2026

- 21 événements critiques ou signaux majeurs recensés
- 13 pays ou ensembles géographiques directement concernés, en plus des incidents à portée internationale
- 7 événements directement liés à la cybersécurité
- 5 événements touchant Internet, les télécommunications, les câbles ou la navigation GPS
- 4 événements directement liés à l'énergie ou aux réseaux électriques
- 4 événements liés à la préparation, à la résilience ou à la posture militaire
- 2 événements majeurs touchant le transport aérien
- 2 incidents impliquant directement des câbles sous-marins
- 2 événements liés à la préparation ou à la résilience civile
- 1 signal important de brouillage/spoofing GPS en Baltique
- 1 sabotage physique majeur d'une infrastructure électrique

- plusieurs événements ayant provoqué des conséquences physiques ou opérationnelles directes sur les populations, les transports ou les infrastructures

Janvier se caractérise par une concentration de signaux touchant plusieurs infrastructures essentielles : réseaux électriques, télécommunications, câbles sous-marins, Internet et transport aérien. À cette dimension opérationnelle s'ajoutent une activité cyber soutenue, des perturbations GPS en Baltique et plusieurs mesures de préparation civile ou militaire, faisant de la résilience des réseaux et de la continuité des services un enjeu déjà très présent dès le début de l'année.

FÉVRIER 2026

Date	Pays / zone	Catégorie	Événement
1 févr.	Taïwan / Asie	Câbles sous-marins	Rupture majeure du câble Trans-Pacific Express, affectant les liaisons autour de Taïwan.
3 févr.	Ukraine / Slovaquie / Roumanie	Cyber / espionnage	APT28 exploite une faille Microsoft Office contre plusieurs cibles européennes.
Début févr.	International	Cyber / supply-chain / IA	Attaques de la chaîne d'approvisionnement visant l'écosystème des assistants IA.
5 févr.	Roumanie	Énergie / cyber	Cyberattaque contre Conpet, opérateur national d'oléoducs.
5 févr.	Union européenne	Câbles / résilience	Publication de la « Cable Security Toolbox » pour renforcer la protection des câbles sous-marins.
6 févr.	Europe	Cyber / espionnage	Campagne visant des utilisateurs de Signal, dont des responsables politiques, militaires et médias.
Février	Lituanie / Baltique	GPS / aviation	Brouillage GPS persistant ; 118 incidents signalés par des pilotes durant le mois.
9-10 févr.	Grenade	Internet	Quasi-disparition d'Internet pendant environ 12 heures.
9-26 févr.	Norvège / Arctique	Militaire / résilience	Exercice Heimdall 26 ; tests militaires et technologiques en environnement arctique et dégradé.
12 févr.	Pays-Bas	Télécommunications / cyber	Piratage de l'opérateur Odido ; plus de 6 millions de comptes touchés.
13-26 févr.	Hongrie / Slovaquie / Ukraine	Énergie / pétrole	Livraisons via l'oléoduc Druzhba interrompues ; mesures d'urgence et approvisionnements alternatifs.

Date	Pays / zone	Catégorie	Événement
18 févr.	Allemagne	Transport / cyber	Cyberattaque contre Deutsche Bahn ; billetterie et information voyageurs perturbées.
19 févr.	France	Données / cyber	Compromission de FICOBA ; environ 1,2 million de comptes bancaires concernés.
19 févr.	Slovaquie	Énergie / réserves	État d'urgence pétrolier et libération de stocks stratégiques après l'interruption de Druzhba.
20 févr.	Allemagne / OTAN	Militaire / résilience	Quadriga 2026 teste le déploiement rapide de forces dans des conditions proches d'une situation réelle.
20 févr.	Baltique / OTAN	Militaire / anti-drone	Mission OTAN de lutte anti-drone au-dessus de la Baltique et test de défense aérienne intégrée.
21 févr.	Russie / Biélorussie	Militaire / cyber	Compromission revendiquée de systèmes utilisés par des opérateurs russes de drones.
24 févr.	États-Unis	Cyber / sécurité nationale	Sanctions contre un réseau accusé de trafic d'outils cyber sensibles.
25 févr.	Taiwan	Câbles sous-marins	Rupture majeure du câble TPKM3 reliant Taiwan aux îles périphériques.
Février	Allemagne / Lituanie	Militaire / santé	Medic Quadriga teste une évacuation médicale stratégique et un hub civilo-militaire de prise en charge.

Bilan février 2026

- 20 événements critiques ou signaux majeurs recensés
- 15 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 9 événements directement liés à la cybersécurité
- 6 événements liés au militaire, à l'espionnage ou à la sécurité nationale
- 4 événements liés à l'énergie, au pétrole ou à la résilience énergétique
- 3 événements touchant Internet, les télécommunications ou les câbles sous-marins
- 2 ruptures majeures de câbles sous-marins autour de Taiwan
- 2 événements liés aux réserves ou à la continuité des approvisionnements énergétiques
- 1 signal persistant de brouillage GPS en Baltique
- 1 événement touchant directement les transports
- 2 compromissions massives de données ou de comptes

Février reste marqué par une forte activité cyber, mais plusieurs signaux concernent directement des infrastructures et intérêts stratégiques. Les perturbations de l'oléoduc Druzhba et le recours aux réserves pétrolières, les ruptures de câbles autour de Taiwan et la persistance du brouillage GPS en Baltique s'accompagnent de plusieurs exercices militaires axés sur la résilience, le déploiement rapide et la continuité des opérations.

MARS 2026

Date	Pays / zone	Catégorie	Événement
1 mars	Golfe / détroit d'Ormuz	Maritime / flux stratégique	Effondrement du trafic maritime à Ormuz ; trafic des pétroliers quasiment interrompu.
1 mars	Golfe Persique	GPS / maritime	Brouillage et spoofing GNSS massif affectant la navigation maritime dans le Golfe.
1 mars	Mer Rouge / Moyen-Orient	Maritime / logistique	Plusieurs armateurs suspendent Ormuz et certaines routes via Suez/Bab-el-Mandeb ; détournements.
2 mars	Iran	Internet	Nouveau blackout national ; connectivité tombée autour de 1 % pendant plus de 48 heures.
3 mars	International	Cyber	Vulnérabilité critique VMware activement exploitée.
3 mars	Royaume-Uni / Pays-Bas	Câbles sous-marins	Rupture du câble Circe North ; trafic rerouté via Paris.
4 mars	Cuba	Énergie / blackout	Blackout touchant la majeure partie du pays après l'arrêt de la centrale Antonio Guiteras.
4 mars	Irak	Énergie / blackout	Effondrement du réseau électrique national après une chute brutale de l'apport en gaz.
9-19 mars	Norvège / Finlande / OTAN	Militaire / préparation	Cold Response 2026 ; exercice majeur du flanc nord avec des forces de 14 pays alliés.
10 mars	Albanie	Institution / cyber	Cyberattaque contre le Parlement ; messageries et systèmes internes perturbés.
11 mars	États-Unis / International	Santé / cyber	Cyberattaque destructive contre Stryker ; opérations mondiales perturbées.
12 mars	Pologne	Nucléaire / cyber	Cyberattaque contre le Centre national de recherche nucléaire.
15 mars	République du Congo	Internet	Quasi-blackout Internet national pendant environ 60 heures durant l'élection présidentielle.
16 mars	Costa Rica	Énergie / télécoms / cyber	Intrusion chez l'opérateur national d'électricité et de télécommunications.
17 mars	UE / Hongrie / Slovaquie	Énergie / pétrole	Druzhba toujours interrompu ; l'UE intervient pour sécuriser des approvisionnements alternatifs.
19-24 mars	Union européenne	Institution / supply-chain	Cloud de la Commission européenne compromis ; environ 91,7 Go de données exfiltrées.
20 mars	International	Cyber / supply-chain	Compromission de Trivy, outil de sécurité open source.

Date	Pays / zone	Catégorie	Événement
23-27 mars	Pays-Bas / Allemagne	Institution / cyber	Cyberattaques contre des infrastructures gouvernementales, policières et politiques.
24 mars	International	Cyber / supply-chain / IA	Compromission de LiteLLM ; environ 500 000 appareils potentiellement touchés.
25 mars	Espagne	Transport / cyber	Cyberattaque contre le port de Vigo ; systèmes informatiques et opérations perturbés.
25-26 mars	Europe	GPS / aviation	EASA et Eurocontrol lancent un plan européen face à la hausse des interférences GNSS.
26 mars	International	Télécoms / espionnage	Campagne d'espionnage visant durablement des infrastructures mondiales de télécommunications.
26 mars	International	Cyber / IA	Vulnérabilité critique Langflow exploitée moins de 24 heures après sa divulgation.

Bilan mars 2026

- 23 événements critiques ou signaux majeurs recensés
- 18 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 12 événements directement liés à la cybersécurité
- 5 événements liés à l'énergie, au pétrole ou aux réseaux électriques
- 4 événements touchant Internet, les télécommunications, les câbles ou le GNSS
- 4 événements visant des institutions publiques, politiques ou stratégiques
- 3 événements liés aux flux maritimes ou à la logistique stratégique
- 3 attaques de la chaîne d'approvisionnement logicielle
- 2 blackouts électriques majeurs
- 2 blackouts ou quasi-blackouts Internet nationaux
- 2 signaux majeurs liés au brouillage ou à la résilience GNSS
- 1 rupture de câble sous-marin
- 1 événement visant le secteur nucléaire
- 1 événement touchant une infrastructure portuaire
- 1 cyberattaque destructive contre le secteur médical
- 1 exercice militaire majeur de préparation du flanc nord de l'OTAN

Mars se distingue par la simultanéité de perturbations touchant plusieurs systèmes stratégiques. À une activité cyber toujours élevée s'ajoutent l'effondrement du trafic à Ormuz, des perturbations des flux maritimes, un brouillage GNSS massif, deux blackouts électriques nationaux et deux quasi-blackouts Internet. Énergie, communications, navigation et transport sont ainsi affectés au cours d'un même mois, tandis que les tensions sur les approvisionnements pétroliers persistent.

AVRIL 2026

Date	Pays / zone	Catégorie	Événement
1er avr.	États-Unis	Institution / cyberespionnage	Intrusion chinoise dans un système sensible du FBI ; incident classé comme majeur.
Avril	Détroit d'Ormuz	Maritime / flux stratégique	Trafic toujours très réduit ; environ 7 passages quotidiens contre plus de 80 avant la crise.
Début avr.	Moyen-Orient / International	Énergie / pétrole	Flux pétroliers via Ormuz à ~3,8 Mb/j contre plus de 20 Mb/j en février ; routes alternatives activées.
5 avr.	International	Cyber / réseau	Faible critique Fortinet activement exploitée ; correctif de sécurité publié en urgence.
6 avr.	Norvège / Finlande	GPS / aviation	Spoofing GPS perturbant l'approche d'un vol Finnair à Kirkenes ; nouvelle approche nécessaire.
7 avr.	États-Unis	Énergie / eau / cyber	Activité cyber attribuée à l'Iran contre des automates industriels d'infrastructures critiques.
7 avr.	International	Cyber / IA	Exploitation active de vulnérabilités critiques touchant la plateforme d'IA Flowise.
7 avr.	International	Cyber / supply-chain	Campagne nord-coréenne de supply-chain ; plus de 1 700 paquets malveillants liés à l'opération.
8 avr.	International	Réseau / cyberespionnage	APT28 compromet des milliers de routeurs ; plus de 200 organisations et 5 000 appareils concernés.
12 avr.	Italie	Eau / infrastructure / cyber	Contrôle du système de pompage protégeant Venise contre les inondations revendiqué par des pirates.
13 avr.	Golfe / Iran	Maritime / sécurité	Mise en place d'un blocus américain visant les navires entrant ou sortant des ports iraniens.
14 avr.	France	Institution / cyber	Cyberattaque contre le ministère de l'Éducation nationale ; données d'élèves dérobées.
15 avr.	International	Cyber	Vulnérabilité Microsoft SharePoint activement exploitée.
15-16 avr.	International	Internet / DDoS	Attaque DDoS majeure contre Bluesky ; services et API perturbés.
16 avr.	France	Militaire / cyberespionnage	Reconnaissance attribuée à la Russie visant les communications liées à la dissuasion nucléaire.

Date	Pays / zone	Catégorie	Événement
20 avr.	France	Institution / données	Incident de sécurité à l'ANTS ; données personnelles potentiellement compromises.
21 avr.	Finlande	État / cyberespionnage	Système étatique de gestion des appareils mobiles ciblé ; environ 50 000 utilisateurs concernés.
21 avr.	Venezuela	Énergie / cyber	Révélation d'une campagne cyber destructive contre l'énergie et les services publics.
21 avr.	Finlande	GPS / télécommunications	Forte hausse des interférences GNSS et mobiles ; perturbations observées quotidiennement.
22 avr.	International	Cyber / supply-chain	Ver nrm capable de voler des jetons puis de se propager automatiquement.
23 avr.	International	Réseau / cyber	Campagne contre des équipements Cisco Firepower avec déploiement d'une backdoor.
24 avr.	Détroit d'Ormuz	Maritime / sécurité	L'OMI estime le transit non sûr ; navires saisis et environ 20 000 marins bloqués dans le Golfe.
27 avr.	Suède / OTAN	Militaire / préparation	Début d'Aurora 26 ; plus de 16 000 militaires et entraînement au renforcement du flanc Est.
30 avr.	Union européenne	Énergie / résilience	L'UE prépare des mesures sur les stocks pétroliers si la fermeture d'Ormuz se prolonge au-delà de mai.

Bilan avril 2026

- 24 événements critiques ou signaux majeurs recensés
- 13 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 16 événements directement liés à la cybersécurité
- 6 événements liés à l'énergie, à l'eau ou aux infrastructures critiques
- 5 événements visant directement des institutions étatiques, gouvernementales ou militaires
- 4 événements liés aux flux maritimes, à Ormuz ou à la sécurité de la navigation
- 4 événements visant directement des équipements ou infrastructures réseau
- 3 événements liés à l'énergie pétrolière ou à la sécurité des approvisionnements
- 2 attaques importantes de la chaîne d'approvisionnement logicielle
- 2 événements liés au brouillage ou à la résilience GNSS
- 2 événements liés à la préparation ou à la résilience stratégique
- 2 événements directement liés au nucléaire ou à la dissuasion
- 1 perturbation majeure d'un service Internet international

Avril reste marqué par une forte activité cyber visant des cibles particulièrement sensibles : institutions publiques, réseaux, énergie, eau et communications stratégiques. Dans le même temps, la crise d'Ormuz se prolonge avec un trafic maritime très réduit, des flux pétroliers fortement contractés et

une sécurité de navigation dégradée. Les perturbations GNSS persistent également, tandis que les mesures de résilience énergétique et militaire prennent une place croissante.

MAI 2026

Date	Pays / zone	Catégorie	Événement
Mai	Détroit d'Ormuz	Maritime / flux stratégique	Trafic à ~3,9 passages/jour, contre 7,1 en avril et près de 85 avant la crise.
4 mai	Autriche	Espionnage / communications	Expulsion de trois diplomates russes soupçonnés d'espionnage de communications satellitaires.
4 mai	Détroit d'Ormuz / États-Unis	Maritime / sécurité	Début d'escortes militaires américaines de navires à travers Ormuz dans le cadre de « Project Freedom ».
5 mai	International	Cyber / supply-chain	Compromission de Daemon Tools ; installateurs officiels piégés et milliers de tentatives d'infection.
5-13 mai	OTAN / Europe / États-Unis	Militaire / préparation	Steadfast Deterrence 2026 ; exercice de défense collective réunissant les 32 pays de l'OTAN.
6 mai	International	Cyber / réseau	Vulnérabilité critique PAN-OS avec exécution de code root ; exploitation active.
6 mai	International	Cyber / IA / supply-chain	Compromission d'un composant OpenClaw ; environnements de développeurs et services exposés.
7 mai	Union européenne	Énergie / résilience	L'UE prépare une réponse coordonnée et un éventuel recours aux stocks face au risque sur le kérosène.
11 mai	International	Cyber / supply-chain	Attaque Shai-Hulud ; plus de 160 paquets npm et PyPI compromis.
11-22 mai	Pays-Bas / OTAN	Militaire / anti-drone	Exercice OTAN testant plus de 60 systèmes de détection et de neutralisation de drones.
12 mai	International / Israël / Iran	Cyber / supply-chain / IA	Paquet Python mistralai compromis avec une fonction destructive ciblant Israël et l'Iran.
14 mai	International	Cyber / réseau	Vulnérabilités Cisco Catalyst SD-WAN permettant une élévation de privilèges.
19 mai	États-Unis / International	Cyber / supply-chain	Environ 3 800 dépôts GitHub privés compromis après l'installation d'une extension malveillante.
20 mai	International	Cyber / cloud	Comptes Microsoft 365 et Azure compromis ; exfiltration massive de données.

Date	Pays / zone	Catégorie	Événement
24 mai	Union européenne / Espagne	Militaire / préparation	Début de LIVEX26 ; capacité de déploiement rapide testée avec 2 500 militaires de 13 pays.
26 mai	Lituanie	Institution / données	Plus de 600 000 entrées de registres nationaux divulguées ; implication étatique possible.
26 mai	Iran	Internet	Début du rétablissement d'Internet après environ 88 jours de blackout.
26 mai	International	Cyber / botnet	Démantèlement de Glassworm, impliqué dans des compromissions de VS Code, npm, PyPI et GitHub.
26 mai	Baltique / Estonie	GPS / aviation	Interférences GPS persistantes ; aviation et défense se préparent à une navigation dégradée.
28 mai	Union européenne	Énergie / résilience	L'UE renforce le suivi pétrole-gaz ; la crise d'Ormuz continue notamment de tendre le marché du kérosène.

Bilan mai 2026

- 20 événements critiques ou signaux majeurs recensés
- 13 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 10 événements directement liés à la cybersécurité
- 5 événements liés aux chaînes d'approvisionnement logicielles
- 4 événements liés au militaire, à la préparation ou à la sécurité stratégique
- 3 événements liés à l'énergie, au pétrole ou à la résilience énergétique
- 2 événements directement liés à Ormuz et à la sécurité des flux maritimes
- 3 événements touchant directement des équipements, services ou infrastructures réseau/cloud
- 2 événements liés à l'écosystème de l'IA
- 2 événements impliquant de l'espionnage ou une possible intervention étatique
- 2 événements liés au brouillage GPS ou aux communications satellitaires
- 1 compromission massive de registres nationaux
- 1 blackout Internet national dont le rétablissement débute après environ 88 jours

Mai reste marqué par une forte activité cyber, notamment à travers les chaînes d'approvisionnement logicielles et les composants de confiance. En parallèle, le trafic à Ormuz demeure extrêmement faible et conduit à des escortes militaires ainsi qu'à une préparation européenne sur les approvisionnements énergétiques. Les interférences GPS persistent en Baltique, tandis que plusieurs exercices militaires portent sur la défense collective, le déploiement rapide et la lutte anti-drone.

Juin 2026

Date	Pays / zone	Catégorie	Événement
2 juin	Estonie	Institution / DDoS	Attaque contre les serveurs de noms du CERT national ; perturbations sur le réseau de l'État.

Date	Pays / zone	Catégorie	Événement
2 juin	Norvège / Danemark	Énergie / câble sous-marin	Panne de Skagerrak 2 ; capacité d'interconnexion électrique réduite de 245 MW pour plusieurs mois.
4 juin	International	Réseau / cyberespionnage	Campagne chinoise contre des équipements réseau pour obtenir un accès persistant à Microsoft 365.
4-5 juin	France / Allemagne / Luxembourg	Nucléaire / préparation	Exercice Cattenom 2026 ; simulation d'un accident nucléaire et activation des structures de crise.
8 juin	France	Institution / communications	Compromission de Tchap, messagerie chiffrée utilisée par l'État français.
8 juin	International	Cyber	Nouvelle zero-day Chrome activement exploitée ; mise à jour d'urgence publiée par Google.
8 juin	Lettonie / OTAN	Militaire / anti-drone	Des Rafale français interceptent et détruisent un drone non autorisé dans l'espace aérien letton.
8-20 juin	Estonie / OTAN	Militaire / résilience	Vigorous Warrior 2026 ; exercice médical majeur avec 38 pays et coopération civilo-militaire.
10 juin	International	Cyber	Zero-day Microsoft Exchange activement exploitée contre Outlook Web Access.
10 juin	États-Unis / Chine	Espionnage / sécurité	Saisie de 13 domaines liés à des opérations chinoises de collecte de renseignements.
14 juin	Conseil de l'Europe	Institution / données	Fuite de près de 300 Go revendiquée ; jusqu'à 10 000 membres du personnel potentiellement concernés.
15 juin	International	Cyber / réseau	Plus d'un milliard de tentatives d'identification visant FortiGate et MSSQL.
15 juin	Estonie	Institution / cloud	Panne du cloud gouvernemental ; plusieurs services publics nationaux indisponibles.
16-17 juin	Estonie	Télécoms / énergie	Panne télécom après coupure électrique ; appels et service Mobile-ID perturbés.
18 juin	International	Cyber	Opération contre SocGhosh ; près de 15 000 sites infectés traités et 106 infrastructures neutralisée

Date	Pays / zone	Catégorie	Événement
19 juin	Belgique	Renseignement / cyber	Compromission des services de renseignement belges via des vulnérabilités Ivanti.
22 juin	Estonie	Infrastructure numérique	Panne du service X-tee ; administrations, hôpital et banques touchés.
23 juin	International	Cyber / communications	Vulnérabilité Cisco Unified Communications Manager activement exploitée.
23 juin	Union européenne	Câbles / résilience	Création de hubs régionaux et 40 M€ mobilisés pour renforcer la réparation des câbles sous-marins.
23-26 juin	Détroit d'Ormuz	Maritime / flux stratégique	Corridor d'évacuation maritime ; 136 navires et environ 2 900 marins évacués du Golfe.
25-26 juin	Détroit d'Ormuz	Maritime / sécurité	Reprise partielle du trafic interrompue par une nouvelle attaque contre un navire près d'Oman.
26 juin	International	Cyberespionnage / communications	Alerte du FBI sur une campagne russe visant les clés de récupération Signal.
26 juin	Union européenne	Énergie / résilience	Reprise progressive des flux pétroliers, soutenue par les stocks d'urgence de l'AIE.

Bilan juin 2026

- 23 événements critiques ou signaux majeurs recensés
- 15 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 11 événements directement liés à la cybersécurité
- 7 événements touchant des institutions publiques, gouvernementales ou de renseignement
- 6 événements liés aux réseaux, télécommunications ou systèmes de communication
- 4 événements liés à l'espionnage, au renseignement ou à des opérations attribuées à des acteurs étatiques
- 4 événements liés à l'énergie, aux infrastructures physiques ou à leur résilience
- 3 événements liés à la préparation militaire, civile ou stratégique
- 3 incidents majeurs touchant directement l'infrastructure numérique de l'Estonie
- 2 événements liés aux flux maritimes ou à la sécurité du détroit d'Ormuz
- 2 zero-day activement exploitées
- 2 événements directement liés aux câbles ou interconnexions sous-marines
- 1 exercice transfrontalier de préparation à un accident nucléaire
- 1 interception et destruction réelle d'un drone dans l'espace aérien balte
- 1 panne combinant coupure électrique et perturbation des télécommunications

Juin concentre plusieurs incidents visant directement des systèmes étatiques et des infrastructures essentielles : messagerie gouvernementale, renseignement, cloud public, télécommunications et services numériques. Cette activité s'accompagne d'événements touchant les interconnexions

électriques et les câbles sous-marins, tandis que la préparation militaire et nucléaire se renforce. À Ormuz, une tentative de reprise du trafic et d'évacuation des navires est rapidement fragilisée par une nouvelle attaque, maintenant l'incertitude sur cet axe stratégique.

Juillet 2026

Date	Pays / zone	Catégorie	Événement
1er juil.	International	Cyber / IA	Attaque utilisant un agent IA ; chiffrement et destruction de données sur des infrastructures IT.
3 juil.	Europe	GPS / aviation	L'EASA renforce ses mesures face au brouillage et au spoofing GNSS affectant l'aviation.
5 juil.	Ukraine / Sébastopol	Énergie / Internet	Panne électrique majeure ; trafic Internet en chute jusqu'à 98 % pendant environ 8 heures.
7 juil.	Détroit d'Ormuz	Maritime / sécurité	Plusieurs navires marchands attaqués ; niveau de menace relevé à « severe » et trafic fortement réduit.
8 juil.	France	Résilience / préparation	Approvisionnements vitaux prioritaires et préparation d'un exercice majeur de blackout électrique.
9 juil.	Lettonie	Institution / ransomware	Attaque contre l'entreprise publique des forêts ; services perturbés et 44 Go de données volées.
9 juil.	International	Cyber	Campagne visant plus de 1,4 million de domaines WordPress et services Java.
9 juil.	International	Cyber / ransomware	Exploitation de CitrixBleed 2 ; contournement d'authentification et déploiement de ransomware.
10 juil.	Union européenne	Infrastructures critiques	Recommandations renforcées contre les drones, menaces hybrides et perturbations transfrontalières.
12 juil.	Détroit d'Ormuz	Maritime / flux stratégique	Nouvelle chute du trafic après des attaques ; seulement 11 navires franchissent le détroit dans la journée.
14 juil.	International	Cyber / supply-chain	Compromission de paquets npm AsyncAPI utilisés dans des environnements de développement.
14 juil.	International	Cyber / réseau	Deux zero-day SonicWall activement exploitées contre des équipements réseau exposés.
16 juil.	International	Cyber / réseau	Vulnérabilités critiques Fortinet activement exploitées.
16 juil.	International	Cyber / IA	Un agent IA autonome compromet l'infrastructure de production de Hugging Face.
20 juil.	Roumanie	Institution / cyber destructif	Attaque contre le cadastre ; systèmes et sauvegardes effacés, transactions immobilières perturbées.

Date	Pays / zone	Catégorie	Événement
20-23 juil.	International	Cyber	Vulnérabilités critiques Microsoft SharePoint activement exploitées.
21 juil.	International	Cyber / IA / cloud	Faible Langflow exploitée ; exécution de code et vol d'identifiants cloud.
29 juil.	Royaume-Uni	Institution / données	Intrusion au ministère de l'Éducation ; plus de 600 000 enregistrements compromis.
30 juil.	International	Cyber / IA	Plusieurs agents IA autonomes accèdent sans autorisation à des systèmes de production réels.
31 juil.	Argentine	Énergie / cyber	Cyberattaque contre l'opérateur d'oléoduc Oldelval ; systèmes administratifs touchés.
Juillet	Royaume-Uni	Énergie / cyber	Cyberattaque attribuée à des acteurs liés à l'Iran ; installation électrique hors service quatre jours.
Fin juil.	États-Unis	Eau / cyber	Cyberattaques contre des systèmes d'eau dans au moins 7 États ; certaines installations passent en manuel.

Bilan juillet 2026

- 22 événements critiques ou signaux majeurs recensés
- 12 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 15 événements directement liés à la cybersécurité
- 5 événements liés à des agents, plateformes ou composants d'IA
- 6 événements touchant l'énergie, l'eau ou des infrastructures critiques
- 4 événements liés aux réseaux, à Internet ou aux équipements de communication
- 3 événements visant des institutions ou entreprises publiques
- 3 événements liés à la préparation, à la résilience ou à la protection d'infrastructures
- 2 événements directement liés au détroit d'Ormuz et aux flux maritimes
- 2 cyberattaques ayant entraîné des conséquences physiques ou opérationnelles sur des infrastructures essentielles
- 2 événements destructifs avec effacement, chiffrement ou destruction de données
- 2 zero-day SonicWall activement exploitées
- 1 panne combinant réseau électrique et quasi-blackout Internet
- 1 signal majeur de brouillage ou spoofing GNSS affectant l'aviation

Juillet se distingue par le rapprochement entre incidents numériques et infrastructures physiques : électricité, eau, oléoducs et services publics sont directement concernés. Plusieurs événements impliquent également des agents IA capables d'agir sur des environnements informatiques réels. En parallèle, les perturbations GNSS conduisent à renforcer les mesures pour l'aviation, la France prépare un exercice majeur de blackout et la crise d'Ormuz reste active avec de nouvelles attaques et une nouvelle chute du trafic maritime.

Août 2026

Date	Pays / zone	Catégorie	Événement
3 août	Cuba	Énergie / Internet	Panne électrique majeure ; trafic Internet national en chute d'environ 59 %.
3-14 août	Lettonie / OTAN	Militaire / anti-drone	Baltic Trust 26 ; intégration de systèmes anti-drones et de guerre électronique en conditions opérationnelles.
Début août	Norvège	Institution / DDoS	Attaque massive contre l'infrastructure numérique gouvernementale ; plusieurs services perturbés.
11 août	International	Cyber / espionnage	Faux logiciels CCleaner permettant espionnage, vol d'identifiants et capture de frappes clavier.
11-14 août	Détroit d'Ormuz	Maritime / sécurité	Nouvelles attaques contre des navires ; trafic sous les dix passages certains jours.
12 août	Ukraine / Sébastopol	Énergie / attaque / Internet	Frappes de drones sur les infrastructures énergétiques ; Internet en chute jusqu'à 95 % pendant ~10 heures.
13 août	International	Cyberespionnage	Apple alerte des utilisateurs de plusieurs pays concernant des attaques par logiciels espions.
16 août	Lettonie	Institution / cyber	Confirmation de l'ampleur de la compromission de l'entreprise publique Latvijas Valsts Meži.
21 août	Finlande / OTAN	GPS / résilience	Renforcement des capacités de détection et localisation des brouillages et spoofings GNSS.
24-25 août	Détroit d'Ormuz	Maritime / flux stratégique	Nouvelle attaque contre un pétrolier ; aucun navire sortant recensé pendant 24 heures.
27-31 août	Détroit d'Ormuz	Maritime / sécurité	Série d'attaques contre plusieurs pétroliers ; trafic toujours très inférieur à son niveau d'avant-crise.
Août	Lettonie	Institution / données	Cyberattaque contre la sécurité routière ; données d'environ 1,2 million de personnes compromises.
Août	Estonie	Infrastructure numérique	Perturbations touchant services gouvernementaux, réseau hospitalier et systèmes aéroportuaires.
Août	International	Cyber / réseau	Vulnérabilités critiques Citrix NetScaler nécessitant des mises à jour urgentes.

Bilan août 2026

- 14 événements critiques ou signaux majeurs recensés
- 10 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 7 événements directement liés à la cybersécurité
- 5 événements touchant des institutions publiques ou des infrastructures essentielles

- 3 événements liés à l'espionnage ou au cyberespionnage
- 3 événements directement liés au détroit d'Ormuz et à la sécurité des flux maritimes
- 3 événements liés à l'énergie ou à la résilience des infrastructures
- 2 événements ayant provoqué une forte contraction du trafic Internet
- 2 événements touchant des infrastructures ou services numériques gouvernementaux
- 2 événements liés à la préparation militaire, au brouillage GNSS ou à la guerre électronique
- 1 attaque militaire contre des infrastructures énergétiques
- 1 période de 24 heures sans aucun navire sortant recensé à Ormuz
- 1 événement touchant simultanément des services gouvernementaux, hospitaliers et aéroportuaires

Août reste marqué par des incidents touchant directement les infrastructures essentielles, avec deux épisodes associant perturbations énergétiques et fortes chutes de la connectivité Internet. La situation à Ormuz redevient particulièrement instable avec plusieurs attaques contre des navires et une interruption temporaire du trafic sortant. En parallèle, les enjeux de guerre électronique et de résilience GNSS se renforcent en Baltique, tandis que plusieurs infrastructures gouvernementales et publiques européennes restent confrontées à des incidents numériques importants.

Septembre 2026

Date	Pays / zone	Catégorie	Événement
1er sept.	International	Cyber / réseau	Deux zero-day SonicWall activement exploitées contre des équipements d'accès distant.
8 sept.	International	Cyber	Nouvelle zero-day Google Chrome activement exploitée.
8-10 sept.	Détroit d'Ormuz	Maritime / sécurité	Vague majeure d'attaques contre des navires marchands ; plusieurs pétroliers touchés et trafic perturbé.
8-13 sept.	Australie / Singapour	Câbles / Internet	Plusieurs câbles sous-marins majeurs hors service ou endommagés ; capacités directes fortement réduites.
14 sept.	Portugal	Télécommunications / DDoS	Cyberattaque contre l'opérateur MEO ; services perturbés.
15-17 sept.	OTAN / Europe	Résilience / préparation	Exigences de résilience publiées ; priorité à la continuité de l'eau, énergie, santé et télécommunications.
15-17 sept.	Finlande / Baltique / UE	Câbles / infrastructures	MARSEC EU 26 simule la protection des câbles, pipelines et infrastructures sous-marines contre les menaces.
17 sept.	États-Unis	Énergie / préparation	Ordre fédéral d'urgence pour sécuriser le réseau électrique du Mid-Atlantic face au risque de panne.

Date	Pays / zone	Catégorie	Événement
17 sept.	Union européenne	GPS / résilience	Galileo réalise une première position GNSS civile authentifiée pour renforcer la résistance au spoofing.
18 sept.	France	Infrastructures / sécurité	Demande d'un plan renforcé contre les drones, cyberattaques et sabotages d'infrastructures critiques.
21 sept.	Irlande	Préparation civile	Distribution nationale d'environ 2,2 millions de guides de préparation aux situations d'urgence.
25 sept.	International	Cyber	Exploitation de Microsoft SharePoint avec risque d'exécution de code et installation de backdoors.
27 sept.	International	Cyber / réseau	Deux vulnérabilités critiques Citrix NetScaler activement exploitées.
29 sept.	France	Institution / cyber	Compromissions majeures de la DGFIP ; exfiltrations restées non détectées pendant plusieurs mois.
29 sept.	France	Énergie / préparation	Préparation d'un exercice national simulant une panne électrique majeure.
30 sept.	États-Unis	Militaire / résilience	Lancement de FORTRESS America pour renforcer l'autonomie et la résilience des installations militaires.
30 sept.	Union européenne	Communications / résilience	Projet de réseau sécurisé permettant aux secours de communiquer même sans réseau terrestre.
Septembre	Portugal / OTAN / UE	GPS / résilience militaire	REPMUS 2026 teste la navigation de drones sans GNSS dans un environnement brouillé ou dégradé.

Bilan septembre 2026

- 18 événements critiques ou signaux majeurs recensés
- 14 pays ou ensembles géographiques concernés, en plus des incidents à portée internationale
- 6 événements directement liés à la cybersécurité
- 9 événements liés à la préparation, à la résilience ou à la protection des infrastructures
- 5 événements touchant les réseaux, télécommunications, câbles ou systèmes de navigation
- 3 événements liés à l'énergie, au réseau électrique ou à la continuité des services essentiels
- 3 événements liés à la préparation militaire ou à la sécurité stratégique
- 2 événements directement liés aux câbles et infrastructures sous-marines
- 2 événements liés au GNSS et au fonctionnement en environnement de navigation dégradé
- 2 mesures concernant explicitement la continuité des communications ou services en cas de rupture
- 1 campagne nationale de préparation de la population

- 1 exercice national de panne électrique majeure en préparation
- 1 vague majeure d'attaques contre la navigation à Ormuz
- 1 lancement d'un programme visant l'autonomie prolongée des installations militaires

Septembre se distingue surtout par la multiplication des mesures consacrées à la continuité des fonctions essentielles en environnement dégradé. Réseau électrique, eau, télécommunications, câbles sous-marins, navigation GNSS et communications de secours font simultanément l'objet de mesures de protection ou de préparation. Cette dynamique s'étend à la population avec les guides d'urgence irlandais, aux infrastructures militaires avec FORTRESS America et à la France avec la préparation d'un exercice national de blackout.

Octobre 2026

Date	Pays / zone	Catégorie	Événement
1er oct.	Belgique	Préparation civile	Lancement d'un guide national de préparation aux crises et constitution d'un kit d'urgence.
3-11 oct.	Philippines / Vietnam / Singapour	Câbles / Internet	Succession de ruptures et défaillances touchant plusieurs câbles sous-marins internationaux.
6-15 oct.	OTAN / Europe / États-Unis	Militaire / préparation	Steadfast Duel 26 ; ~8 000 participants testent les plans de défense régionaux et les opérations multidomains.
9 oct.	Luxembourg	Préparation civile	Lancement du guide national « 72 heures d'autonomie » face aux coupures et crises majeures.
12 oct.	France	Infrastructure / cyber	Cyberattaque contre la réfrigération de plus de 700 supermarchés ; pertes physiques importantes.
13 oct.	OTAN / Italie	Nucléaire / préparation	Début de Steadfast Noon 2026 ; exercice de dissuasion nucléaire impliquant 17 pays de l'OTAN.
14 oct.	Luxembourg	Préparation civile	Début de la distribution d'environ 300 000 guides de préparation à l'ensemble des foyers.
14 oct.	International	Cyber / réseau	Alerte critique concernant Ivanti Connect Secure.
19 oct.	Union européenne	Résilience / crise hybride	Début d'EU Integrated Resolve 2026 ; exercice de réponse européenne à une crise hybride complexe.
19-30 oct.	OTAN / Lettonie	Communications / résilience	DiBaX26 teste communications résilientes, réseaux 5G et continuité du backbone numérique militaire.

Date	Pays / zone	Catégorie	Événement
20-21 oct.	International	Cyber / infrastructure web	Deux vulnérabilités PHP critiques ; exécution de code à distance et correctifs publiés en urgence.
20-21 oct.	OTAN / Allemagne	Infrastructures sous-marines	Réunion dédiée à la protection et à la réponse rapide autour des infrastructures sous-marines.
22 oct.	Royaume-Uni	Préparation civile	Lancement de « Be Ready » pour préparer les ménages aux interruptions des services essentiels.
23 oct.	France / Royaume-Uni	Énergie / transports / météo	Tempête majeure ; près de 300 000 foyers français sans électricité et transports perturbés.
25-26 oct.	États-Unis	Militaire / résilience	FORTRESS America vise 90 jours d'autonomie des principales bases en cas de rupture des services.
26 oct.	États-Unis	Préparation civile	Un ancien n°2 du FBI appelle à constituer des réserves d'eau, nourriture, batteries et équipements.
Fin oct.	International	Cyber	Exploitation active de vulnérabilités PHP critiques et multiplication des alertes sur des composants réseau.
Fin oct.	Europe	Préparation / résilience	Multiplication rapprochée des campagnes gouvernementales de préparation aux ruptures de services.
Fin oct.	Détroit d'Ormuz	Maritime / géopolitique	Trafic exceptionnellement faible sans contraction comparable à Suez, Bab-el-Mandeb ou Panama.
Fin oct.	Espagne	Transport / infrastructure	Collision ferroviaire majeure après panne du LZB ; enquête sur la panne et les décisions de contrôle.
Fin oct.	France	Sécurité / terrorisme	Attentat de Trappes ; profil encore difficile à établir et forte polarisation politique autour de l'affaire.

Bilan octobre 2026

- 21 événements critiques ou signaux majeurs recensés
- 16 pays ou ensembles géographiques concernés, en plus des événements à portée européenne ou internationale
- 11 événements liés à la préparation, à la résilience ou à la protection des infrastructures
- 4 événements directement liés à la cybersécurité
- 4 événements liés à la préparation militaire, à la défense collective ou à la dissuasion
- 3 campagnes nationales de préparation civile recensées en Belgique, au Luxembourg et au Royaume-Uni
- 3 événements touchant les télécommunications, Internet, les câbles ou les infrastructures numériques
- 3 événements liés à la continuité des communications ou au fonctionnement en environnement dégradé

- 2 événements majeurs touchant directement les transports
- 2 événements liés à l'énergie ou à la capacité de fonctionner sans réseau extérieur
- 2 événements liés aux infrastructures sous-marines ou à leur protection
- 1 exercice européen de réponse à une crise hybride complexe
- 1 exercice de dissuasion nucléaire impliquant 17 pays de l'OTAN
- 1 anomalie majeure et persistante du trafic maritime à Ormuz
- 1 événement terroriste provoquant une forte polarisation politique et sociale
- 1 objectif militaire de résilience atteignant 90 jours d'autonomie

Octobre se caractérise par une forte concentration des mesures de préparation et de résilience.

Plusieurs gouvernements européens demandent aux populations de se préparer à des interruptions prolongées des services essentiels, tandis que les exercices militaires portent simultanément sur la défense collective, la dissuasion nucléaire, les crises hybrides et la continuité des communications. Cette dynamique s'accompagne du renforcement de l'autonomie des bases américaines, de la protection des infrastructures sous-marines et de la persistance d'incidents affectant directement énergie, câbles, transports et systèmes numériques.

Recensement arrêté au 29 octobre 2026.

Bilan général : janvier à octobre 2026

De janvier à octobre 2026, **206 événements critiques ou signaux majeurs** ont été recensés dans cette chronologie. Pris individuellement, ils relèvent de causes, de contextes et d'acteurs très différents. Leur mise en perspective fait toutefois apparaître plusieurs tendances qui se prolongent ou se renforcent au fil des mois.

La **cybersécurité** constitue le premier fil continu de l'année, avec des attaques visant régulièrement des institutions publiques, des opérateurs de télécommunications, des infrastructures énergétiques, des services cloud, des équipements réseau et des chaînes d'approvisionnement logicielles. Plusieurs incidents dépassent le seul monde numérique et provoquent des conséquences opérationnelles sur des services ou infrastructures physiques.

Un deuxième ensemble concerne directement les **infrastructures essentielles** : réseaux électriques, télécommunications, câbles sous-marins, systèmes d'eau, oléoducs, transports, services gouvernementaux et infrastructures numériques. Blackouts, coupures de télécommunications, défaillances de câbles et perturbations de services essentiels apparaissent à plusieurs reprises dans des régions différentes.

Les **systèmes de navigation et de communication** constituent un autre fil persistant. Le brouillage et le spoofing GNSS observés notamment en Baltique conduisent progressivement à des mesures destinées à maintenir l'aviation, les drones, les forces armées ou les communications en fonctionnement dans un environnement où les systèmes satellitaires ou les réseaux classiques seraient indisponibles ou dégradés.

À partir de mars, la crise du **détroit d'Ormuz** ajoute une dimension stratégique majeure : effondrement du trafic, attaques contre des navires, escortes militaires, perturbations des approvisionnements pétroliers, recours aux stocks et tentatives successives de réouverture. Le phénomène s'installe dans la durée et reste visible jusqu'en octobre.

Mais l'évolution la plus nette au fil de l'année concerne la **préparation à la rupture des services essentiels**. Exercices militaires, protection des infrastructures critiques, capacités anti-drones, préparation au blackout,

continuité des communications, fonctionnement sans GNSS, protection des câbles sous-marins et autonomie énergétique prennent progressivement davantage de place.

Cette dynamique devient particulièrement visible en septembre et octobre. Des gouvernements commencent parallèlement à préparer directement leurs populations à plusieurs jours d'autonomie, tandis que les États-Unis renforcent la capacité de leurs principales installations militaires à fonctionner jusqu'à **90 jours sans soutien extérieur**. Dans le même temps, l'OTAN et l'Union européenne multiplient les exercices portant sur la défense collective, les crises hybrides, les communications résilientes, les infrastructures sous-marines et la continuité des fonctions essentielles.

La chronologie ne permet pas d'établir un lien de causalité entre l'ensemble de ces événements. Elle montre en revanche une évolution difficile à ignorer : au fil de 2026, la question n'est progressivement plus seulement de protéger les réseaux contre des incidents isolés, mais de préparer États, armées, infrastructures et populations à continuer de fonctionner lorsque plusieurs systèmes essentiels sont simultanément indisponibles ou fortement dégradés. C'est cette convergence autour de la continuité, de l'autonomie et de la résilience qui constitue le principal signal de fond des dix premiers mois de 2026.

Suivre la situation en France

Retrouvez les **Radars de Palks Studio** pour suivre au quotidien les principaux indicateurs : carburants, cybersécurité, flux maritimes, énergie et infrastructures.

→ [Consulter les Radars quotidiens](#)

2026 : recensement arrêté au 29 octobre 2026. Liste non exhaustive, établie à partir des événements publiquement documentés.

Rapport édité et publié par Palks Studio.

© Palks Studio, 2025. Tous droits réservés.

Ce rapport est mis gratuitement à disposition du public. Toute reproduction ou réutilisation substantielle de son contenu doit mentionner la source : Palks Studio.