NUMÉRO 1 · VOLET INFRASTRUCTURES CRITIQUES

Quand le cloud prend feu

Nizar Younes Mqam ORCID 0009-0008-5549-7620

Version 1.5, octobre 2026 · Première édition : avril 2026 · 29 pages

Les 1er et 2 mars 2026, des drones iraniens ont frappé deux centres de données d'Amazon Web Services aux Émirats arabes unis et endommagé un troisième au Bahreïn, perturbant plus de 109 services AWS dans la seule région des Émirats. Cette note soutient qu'il ne s'agit pas d'un incident de cybersécurité mais d'un basculement de doctrine : pour la première fois, selon plusieurs analystes, un État a délibérément visé par des moyens militaires conventionnels des centres de données commerciaux en temps de guerre, au point d'en rendre une partie irrécupérable.

SYNTHÈSE EXÉCUTIVE

Ce qui s'est passé le 1er mars 2026 n'est pas un incident de cybersécurité. C'est un basculement de doctrine. Pour la première fois, selon plusieurs analystes, un État a délibérément visé par des moyens militaires conventionnels des centres de données commerciaux en temps de guerre, au point d'en rendre une partie irrécupérable.

La question n'est plus de savoir si cela peut arriver. Elle est de savoir si votre organisation survivrait à la même chose demain matin. Ce document tire trois conclusions. Un datacenter n'est plus une infrastructure neutre : c'est un territoire souverain avec une adresse physique et une valeur stratégique militaire. Toute organisation qui héberge ses systèmes critiques chez un seul hyperscaler ne loue pas un service, elle paie un tribut à un suzerain dont elle dépend existentiellement. Et aucun plan de continuité ne vaut rien s'il n'a jamais été testé avant la crise.

Trois risques documentés dans ces pages méritent une attention immédiate : Le mythe du multi-cloud, qui diversifie les fournisseurs de calcul sans diversifier la connectivité physique ; l'angle mort réglementaire, car NIS2, CER et DORA n'imposent pas de tester la destruction physique simultanée de deux régions cloud, et seul DORA impose de tester des scénarios physiques ; et la vassalité numérique, qui laisse toute organisation sans plan de bascule testé à la merci d'un opérateur étranger en situation de crise.

Une seule question suffit pour savoir si ce document vous concerne : si vos deux régions cloud principales disparaissent ce soir, dans combien de temps reprenez-vous vos opérations critiques, et depuis où ?

Note méthodologique : cette analyse décrit des catégories de vulnérabilités et des logiques systémiques, et non des noeuds précis d'infrastructure, conformément aux standards de publication ouverte en matière de sécurité critique.

AVANT-PROPOS : POURQUOI CE DOCUMENT VOUS CONCERNE

Imaginez un lundi matin. Votre application de gestion s'arrête, votre site web disparaît, la messagerie ne répond plus. Vos équipes appellent le support IT, qui rappelle quelques minutes plus tard, hébété : les serveurs ne sont pas tombés à cause d'un bug. Ils ont été physiquement détruits par un drone militaire. Ce scénario n'est plus de la fiction. Le 1er mars 2026, des drones iraniens Shahed ont frappé deux datacenters d'Amazon Web Services aux Émirats arabes unis ; le lendemain, une frappe à proximité d'un site d'AWS au Bahreïn en a endommagé l'infrastructure. Oracle, lui, n'a fait l'objet que d'une revendication iranienne, non confirmée, le 2 avril. Dans la seule région des Émirats, plus de 109 services d'AWS ont été perturbés*, des banques régionales ont perdu l'accès à leurs systèmes, et de nombreux utilisateurs ont découvert que le cloud qu'ils croyaient immatériel avait une adresse physique, des murs, et une vulnérabilité bien réelle aux missiles. C'est, selon plusieurs analystes, la première fois qu'un État vise délibérément des centres de données commerciaux en temps de guerre, même si certains y voient des cibles d'opportunité. Les cyberattaques contre des infrastructures numériques civiles précédaient 2026, notamment la neutralisation du réseau satellitaire Viasat par la Russie en Ukraine en février 2022. Ce que mars 2026 a changé, c'est l'irruption du missile et du drone dans un espace que l'on croyait protégé par sa nature commerciale et son statut de tiers neutre. Ce ne sera pas la dernière.

(*)Source : APIStatusCheck, « AWS Middle East Outage March 2026 », 6 mars 2026 [7]. AWS tient la liste des services touchés, région par région, sur son tableau de bord public (AWS Health).

Poser les bases. Avant de construire, il faut comprendre. Les chapitres qui suivent posent les bases sans lesquelles aucune décision de résilience ne peut être prise sérieusement. Un lexique d'abord, parce que ces termes signifient des choses très différentes selon qu'on est à la direction ou en salle des serveurs, et que cet écart de compréhension coûte cher au moment des crises.

Une chronologie ensuite, parce que les frappes iraniennes de 2026 ne sont pas un accident isolé mais l'aboutissement d'une tendance qui s'accélère depuis 2021. Puis une déconstruction honnête du mythe du multi-cloud, qui rassure sans protéger. La raison est technique mais elle est simple : la plupart des architectures multi-cloud partagent des composants invisibles mais communs. Le même fournisseur DNS, le même réseau de distribution de contenu, les mêmes

routes de transit réseau en backbone, les mêmes points d'échange internet régionaux. Deux entreprises qui utilisent respectivement AWS et Azure peuvent voir leurs services simultanément paralysés si le point d'échange internet qui les relie au reste du monde est détruit ou saturé. Le multi-cloud diversifie les fournisseurs de calcul. Il ne diversifie pas la connectivité physique. Le cadre réglementaire européen qui transforme ces recommandations en obligations. Et une feuille de route sur douze mois pour passer de la lecture à l'action.

POSER LES BASES

Lexique

> **Hyperscaler.** Désigne les opérateurs de cloud à l'échelle mondiale : Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud. Leur point commun est d'exploiter des centaines de datacenters répartis sur plusieurs continents, interconnectés entre eux, et de vendre à des milliers d'entreprises la puissance de calcul, le stockage et les services numériques dont elles ont besoin sans qu'elles aient à construire leur propre infrastructure.

> **Région cloud.** Zone géographique dans laquelle un hyperscaler exploite un ou plusieurs datacenters interconnectés. AWS ME-SOUTH-1 désigne par exemple la région Bahreïn d'Amazon. Quand une entreprise choisit d'héberger ses données « dans le cloud », elle choisit en réalité une région précise, c'est-à-dire un ou plusieurs bâtiments physiques dans un pays précis, soumis aux lois de ce pays et exposés à ses risques géopolitiques.

> **Multi-cloud.** Stratégie consistant à utiliser simultanément les services de plusieurs hyperscalers, par exemple AWS et Azure en parallèle. Souvent présentée comme une protection contre les pannes et les dépendances, cette approche est insuffisante si les deux fournisseurs partagent les mêmes infrastructures de connectivité physique, ce que ce document démontre en détail.

> **Point d'échange internet (IXP).** Infrastructure physique, généralement un bâtiment, où plusieurs opérateurs de réseau se connectent entre eux pour échanger du trafic internet. C'est le nœud invisible qui relie les datacenters au reste du monde. Détruire ou saturer un IXP régional peut isoler simultanément des entreprises qui utilisent pourtant des fournisseurs cloud différents.

> **Backbone.** Désigne les grandes artères de transit du réseau internet mondial : les câbles à très haute capacité, souvent sous-marins, qui transportent les données entre continents et entre grandes métropoles. Un datacenter dont le backbone est coupé reste physiquement intact mais devient numériquement inaccessible.

DNS (Domain Name System). Système qui traduit les adresses lisibles par les humains comme « mabanque.ma » en adresses numériques compréhensibles par les machines. Si le serveur DNS qui gère ces traductions tombe, l'application ou le site devient inaccessible même si les données sont intactes, exactement comme un standard téléphonique qui ne fonctionnerait plus : les lignes existent, mais personne ne peut être mis en relation.

CDN (Content Delivery Network). Réseau de serveurs distribués géographiquement dont le rôle est de rapprocher les contenus numériques des utilisateurs finaux pour accélérer leur chargement. Un site web ou une application qui dépend d'un CDN unique partage une vulnérabilité commune avec tous les autres clients de ce CDN.

Control plane. Partie de l'infrastructure cloud qui orchestre et gère l'ensemble des opérations : démarrage des serveurs, routage du trafic, gestion des accès, allocation des ressources. C'est le cerveau du système. Si le control plane est détruit ou isolé, toute l'infrastructure qu'il pilote devient inutilisable, même si les données sont physiquement intactes.

Air-gapped. Se dit d'un système informatique physiquement déconnecté de tout réseau, internet ou intranet. Un backup air-gapped est une sauvegarde qui ne peut pas être atteinte à distance, ni par une cyberattaque ni par une coupure réseau. C'est la forme de protection la plus robuste contre les attaques à distance, mais elle impose une gestion physique rigoureuse.

RTO - Recovery Time Objective. Durée maximale acceptable entre une interruption de service et sa reprise complète. Si votre RTO est de 4 heures, cela signifie que votre organisation a décidé de ne pas tolérer plus de 4 heures d'interruption pour ce service. Définir un RTO sans tester régulièrement si l'infrastructure de secours peut effectivement le respecter est l'une des erreurs les plus fréquentes dans les plans de continuité.

RPO - Recovery Point Objective. Volume maximal de données qu'une organisation accepte de perdre en cas d'incident, exprimé en durée. Un RPO de 1 heure signifie que les données des 60 dernières minutes peuvent être perdues sans que cela soit jugé fatal. Ensemble, RTO et RPO définissent le niveau réel de résilience d'une organisation, pas ses intentions déclarées.

SLA - Service Level Agreement. Contrat par lequel un fournisseur cloud s'engage sur un niveau de disponibilité de ses services, généralement exprimé en pourcentage annuel. Un SLA de 99,9% autorise environ 8,7 heures d'indisponibilité par an. Ce document montre pourquoi ce type d'engagement contractuel ne couvre pas les scénarios de destruction physique, qui déclenchent généralement des clauses de force majeure exonérant le fournisseur.

Frappe cinétique. Terme militaire désignant une attaque par des moyens physiques conventionnels : missiles, drones, bombes. Par opposition à une cyberattaque, une frappe cinétique détruit physiquement l'infrastructure visée. C'est précisément ce que mars 2026 a introduit dans le champ des menaces pesant sur l'infrastructure numérique commerciale.

> **Latence.** Délai entre l'envoi d'une donnée et sa réception. Elle est exprimée en millisecondes et dépend notamment de la distance physique entre l'émetteur et le récepteur. C'est pourquoi un datacenter orbital, même en orbite basse, introduit une latence incompressible qui le rend inadapté à certains usages critiques comme les transactions financières en temps réel.

Chronologie : comment l'infrastructure numérique est devenue une cible militaire

Les frappes iraniennes du 1er mars 2026 ne sont pas sorties du néant. Elles sont l'aboutissement d'une tendance qui s'accélère depuis 2021, chaque épisode franchissant un seuil supplémentaire dans la nature et l'intensité des menaces pesant sur l'infrastructure numérique mondiale. Comprendre cette progression est indispensable pour ne pas traiter mars 2026 comme un accident isolé.

> **MARS 2021**
>
> L'incendie d'OVHcloud à Strasbourg. Un incendie accidentel détruit le datacenter SBG2 d'OVHcloud et endommage gravement SBG1. Plusieurs millions de sites web disparaissent brutalement, dont des services publics et des entreprises qui croyaient leurs données sauvegardées. Le choc n'est pas militaire mais il révèle pour la première fois à grande échelle une vérité que beaucoup refusaient d'admettre : le cloud brûle, littéralement, et les plans de continuité de la plupart des clients n'avaient jamais été testés contre un scénario de destruction physique totale. C'est le premier signal d'alarme massif sur la vulnérabilité physique des datacenters commerciaux.

> **FÉVRIER 2022**
>
> La neutralisation du réseau Viasat en Ukraine. Environ une heure avant l'invasion russe, une cyberattaque sophistiquée neutralise le réseau satellitaire KA-SAT opéré par Viasat, perturbant les communications militaires ukrainiennes et coupant des dizaines de milliers de modems civils à travers l'Europe. C'est la première démonstration à grande échelle qu'une infrastructure numérique commerciale peut être délibérément ciblée comme premier acte d'une opération militaire, avant même que les chars franchissent la frontière. La distinction entre infrastructure civile et cible militaire commence à s'effacer.

> **FÉVRIER 2024**
>
> Les câbles sous-marins sectionnés en Mer Rouge. L'ancre traînante d'un cargo touché par un missile houthi sectionne trois câbles sous-marins majeurs en Mer Rouge, perturbant immédiatement 25% du trafic numérique entre l'Asie, l'Europe et le Moyen-Orient. L'un de ces câbles nécessite cinq mois de réparation, parce que les navires spécialisés ne peuvent pas accéder à la zone de conflit en sécurité. Cet épisode révèle une vulnérabilité systémique que peu de décideurs avaient anticipée : les câbles sous-marins, qui transportent plus de 99 % du trafic de données intercontinental, sont aussi fragiles qu'une ligne électrique aérienne dans une tempête.

> **NOVEMBRE 2024 - JANVIER 2025**
>
> La guerre des câbles en Mer Baltique. Sept câbles sous-marins, dont un câble électrique, sont endommagés entre novembre 2024 et janvier 2025 dans la Mer Baltique. La majorité de ces incidents est soupçonnée d'être des sabotages d'acteurs étatiques, la Russie en tête, même si au moins une coupure a été jugée accidentelle par la justice suédoise. Ce qui distingue cet épisode des précédents, c'est la répétition : en temps de paix formelle, la frontière entre accident, sabotage et acte de guerre devient indécidable, et c'est cette ambiguïté même qui sert l'agresseur.

> **1ER MARS 2026**
>
> Les frappes iraniennes sur AWS et les datacenters du Golfe. Des drones iraniens Shahed frappent deux datacenters d'AWS aux Émirats arabes unis, puis, le 2 mars, endommagent un site d'AWS au Bahreïn par une frappe à proximité. C'est, selon plusieurs analystes, la première frappe délibérée, par des moyens militaires conventionnels, contre des centres de données commerciaux. Plus de 109 services d'AWS sont perturbés dans la région des Émirats. Des banques régionales perdent l'accès à leurs systèmes. De nombreux utilisateurs découvrent que le cloud qu'ils croyaient immatériel avait une adresse physique, des murs, et une vulnérabilité bien réelle aux missiles. La doctrine change.

Ce que cette chronologie démontre est simple et inquiétant : en cinq ans, les menaces pesant sur l'infrastructure numérique ont progressé de l'accident industriel à la cyberattaque stratégique, puis au sabotage présumé en temps de paix, et enfin à la frappe militaire cinétique délibérée. Chaque étape a été traitée comme une surprise alors qu'elle était prévisible depuis l'étape précédente. La prochaine étape l'est tout autant.

Le mythe du multi-cloud : pourquoi diversifier ses fournisseurs ne suffit pas

La stratégie multi-cloud est aujourd'hui présentée par la quasi-totalité des cabinets de conseil et des responsables informatiques comme la réponse naturelle au risque de dépendance envers un seul fournisseur. L'idée est intuitivement séduisante : si vous utilisez AWS et Azure simultanément, la panne de l'un ne devrait pas affecter l'autre. C'est exact dans un scénario de panne technique interne. C'est faux dans un scénario de destruction physique ou de coupure d'infrastructure régionale. Comprendre pourquoi est essentiel avant de prendre toute décision de résilience.

L'erreur fondamentale du raisonnement multi-cloud est de confondre la diversité des fournisseurs de calcul avec la diversité de la connectivité physique. Ce sont deux choses entièrement différentes. Un fournisseur de calcul, c'est l'entité qui vous loue des serveurs et du stockage. La connectivité physique, c'est l'ensemble des infrastructures qui permettent à ces serveurs de communiquer avec vos utilisateurs et avec le reste du monde. Et cette connectivité repose sur des équipements physiques qui, eux, ne sont pas dupliqués par le fait d'avoir deux fournisseurs cloud différents.

Prenons un exemple concret. Une entreprise utilise AWS pour ses applications métier et Azure pour ses sauvegardes, en se croyant protégée. Ses deux fournisseurs font transiter leurs données par le même point d'échange internet régional, le bâtiment physique où les réseaux de la région se connectent entre eux. Si ce point d'échange est détruit par une frappe, saturé par une attaque, ou simplement privé d'électricité par une coupure en surface, AWS et Azure deviennent simultanément inaccessibles depuis cette région. L'entreprise perd ses applications métier et ses sauvegardes en même temps, malgré ses deux fournisseurs distincts.

Le même raisonnement s'applique à d'autres couches invisibles de l'infrastructure. Deux fournisseurs cloud différents peuvent utiliser le même réseau DNS pour résoudre les noms de domaine, le même CDN pour distribuer leurs contenus, les mêmes routes de transit réseau en backbone pour acheminer les données vers les utilisateurs finaux. Ces dépendances communes sont rarement documentées dans les contrats ou les architectures techniques, précisément parce qu'elles sont considérées comme des commodités stables. Elles ne le sont plus dans un contexte de conflit hybride. Les frappes iraniennes de mars 2026 n'ont pas encore illustré cette limite : seul AWS a été touché, et Azure, Google Cloud et Oracle n'ont signalé aucune panne liée à l'incident. Mais tous opèrent dans la même zone de frappe, et partagent souvent les mêmes points d'échange et les mêmes câbles. Le multi-cloud diversifie les serveurs. Il ne diversifie pas, à lui seul, les routes vers le monde.

Certaines organisations ont anticipé ce problème en exigeant contractuellement des routes physiques entièrement indépendantes de leurs fournisseurs, avec des points d'échange internet distincts et une connectivité satellite de secours. Ces architectures avancées réduisent partiellement le risque de panne technique interne. Elles restent cependant largement minoritaires dans la pratique, et aucune d'entre elles n'avait été conçue pour résister à la destruction physique simultanée de deux régions cloud dans deux pays différents, précisément le scénario des 1er et 2 mars 2026.

La conclusion opérationnelle est donc la suivante. Une vraie stratégie de résilience physique ne se mesure pas au nombre de fournisseurs cloud utilisés. Elle se mesure à la capacité à maintenir ou à rétablir la connectivité entre vos systèmes et vos utilisateurs depuis des routes physiques entièrement indépendantes, passant par des points d'échange internet différents, des câbles différents, et si possible des zones géographiques soumises à des risques géopolitiques distincts. C'est un niveau d'exigence très différent de celui que le discours commercial autour du multi-cloud laisse entendre. Et c'est précisément ce que les chapitres suivants permettent de construire méthodiquement.

Les cinq piliers de la résilience physique réelle

La résilience n'est pas un état qu'on atteint. C'est une architecture qu'on construit délibérément, couche par couche, en sachant exactement ce que chaque couche protège et ce qu'elle ne protège pas. Les cinq piliers qui suivent ne sont pas des recommandations génériques. Ce sont les conditions minimales sans lesquelles aucun plan de continuité ne résiste à un scénario de destruction physique de l'infrastructure cloud.

Premier pilier : identifier le cerveau de votre infrastructure. Toute architecture numérique possède un point de défaillance unique, l'endroit dont la destruction ou l'isolement rend le reste inutilisable. C'est souvent le control plane, parfois un serveur DNS critique, parfois une base de données centrale. La première étape de toute démarche de résilience est de cartographier précisément cet endroit, de le nommer, et de vérifier que votre plan de continuité survit à sa disparition physique totale. Un plan de continuité qui ne répond pas à la question « que se passe-t-il si ce bâtiment précis brûle ce soir » n'est pas un plan de résilience. C'est un document rassurant.

Deuxième pilier : diversifier la connectivité physique, pas seulement les fournisseurs. Comme démontré dans le chapitre précédent, utiliser plusieurs hyperscalers ne protège pas si ces fournisseurs partagent les mêmes routes de transit, les mêmes points d'échange internet, ou les mêmes câbles sous-marins. La vraie diversification impose que vos systèmes critiques puissent atteindre vos utilisateurs par au moins deux routes physiques entièrement indépendantes, passant par des points d'échange internet distincts, situés dans des zones géographiques soumises à des risques géopolitiques différents. C'est un niveau d'exigence que la plupart des architectures cloud commerciales actuelles ne satisfont pas.

Troisième pilier : protéger les sauvegardes par une isolation totale. Une sauvegarde hébergée dans le même datacenter que les données primaires, ou dans un datacenter connecté aux mêmes réseaux, n'est pas une sauvegarde de résilience physique. C'est une copie. La protection réelle impose des sauvegardes air-gapped : physiquement déconnectées de tout réseau, stockées dans un site géographiquement distinct, et dont la restauration a été testée dans des conditions réelles. La règle minimale reconnue dans l'industrie est dite 3-2-1 : trois copies des données, sur deux supports différents, dont une hors site et déconnectée. Dans un contexte de conflit hybride, on y ajoute désormais l'exigence que ce site hors ligne soit dans une juridiction géopolitiquement distincte.

Quatrième pilier : définir et tester les plans de bascule avant la crise. Un RTO et un RPO définis sur le papier mais jamais testés sont des intentions, pas des garanties. La bascule vers une infrastructure de secours, dans des conditions de stress réel, fait apparaître systématiquement des problèmes que personne n'avait anticipés : des dépendances invisibles entre systèmes, des configurations qui n'ont pas été mises à jour, des accès qui ne fonctionnent plus, des équipes qui ne savent plus exactement quoi faire parce que la procédure n'a pas été répétée depuis dix-huit mois. La résilience opérationnelle exige des tests de bascule complets, documentés, et régulièrement répétés, au minimum une fois par an pour les systèmes critiques.

Cinquième pilier : ne pas dépendre d'un seul suzerain numérique pour les décisions critiques. Ce pilier est le moins technique et le plus stratégique. Il concerne la gouvernance, pas l'architecture. Toute organisation dont la continuité opérationnelle dépend entièrement d'un contrat avec un seul fournisseur américain, sans alternative activable sous 24 heures, a externalisé une décision souveraine à une entité étrangère soumise à ses propres contraintes légales, géopolitiques et commerciales. La diversification des fournisseurs, des juridictions d'hébergement, et des

architectures de repli n'est pas seulement une décision technique. C'est une décision de gouvernance qui appartient aux directions générales et aux conseils d'administration, pas aux équipes informatiques seules.

Ces cinq piliers ensemble ne garantissent pas l'invulnérabilité. Aucune architecture n'est invulnérable. Ils garantissent que si l'un de vos systèmes est frappé, détruit ou isolé, les dommages restent contenus, la reprise est possible dans un délai connu et testé, et aucun acteur extérieur ne détient seul les clés de votre continuité.

Cadre réglementaire européen : ce que NIS2, CER et DORA exigent concrètement, et ce qu'ils ne couvrent pas

L'Union européenne a produit ces dernières années trois textes majeurs qui transforment la résilience numérique d'une bonne pratique optionnelle en obligation légale contraignante. Comprendre ce que chacun exige et surtout ce qu'aucun des trois ne couvre est devenu indispensable pour tout dirigeant ou régulateur opérant en Europe ou avec des partenaires européens.

NIS2 : La directive sur la sécurité des réseaux et des systèmes d'information. Entrée en application en octobre 2024, NIS2 étend considérablement le périmètre de son prédécesseur en élargissant les secteurs concernés et en durcissant les obligations. Elle couvre désormais les opérateurs d'infrastructures critiques dans dix-huit secteurs, dont l'énergie, les transports, la santé, l'eau, les infrastructures numériques et les services cloud.

Concrètement, elle impose à ces organisations de mettre en place des mesures de gestion des risques cybernétiques, de notifier les incidents significatifs dans des délais stricts, 24 heures pour une alerte précoce, 72 heures pour une notification d'incident, un mois pour le rapport final, et de démontrer que leurs dirigeants ont suivi une formation adéquate sur les risques numériques.

Les sanctions en cas de non-conformité doivent pouvoir atteindre au moins 10 millions d'euros ou 2% du chiffre d'affaires mondial annuel, le montant le plus élevé étant retenu, pour les entités dites essentielles.

CER : La directive sur la résilience des entités critiques. Adoptée en parallèle de NIS2, entrée en vigueur en janvier 2023 et, comme elle, applicable depuis octobre 2024, CER va plus loin sur le plan physique. Elle oblige les opérateurs d'infrastructures critiques à conduire des analyses de risques qui incluent explicitement les menaces physiques : catastrophes naturelles, actes terroristes, sabotages. Elle impose un plan de résilience comprenant des mesures de continuité des activités, des procédures de reprise documentées, et une coopération renforcée avec les autorités nationales compétentes. C'est le texte qui se rapproche le plus des enjeux traités dans ce document, puisqu'il reconnaît explicitement que la menace sur une infrastructure critique peut être physique et pas seulement numérique.

DORA : Le règlement sur la résilience opérationnelle numérique du secteur financier. Entré en application en janvier 2025, DORA s'adresse spécifiquement aux institutions financières :

banques, assurances, gestionnaires d'actifs, infrastructures de marché. Il impose des exigences détaillées sur la gestion des risques liés aux prestataires tiers de services numériques, y compris les fournisseurs cloud. Concrètement, une banque européenne doit désormais cartographier précisément ses dépendances envers ses hyperscalers, tester régulièrement sa résilience opérationnelle, et s'assurer que ses contrats cloud incluent des droits d'audit et des garanties de continuité. DORA introduit également la notion de « prestataire tiers critique », ce qui signifie que des entités comme AWS ou Azure peuvent être directement soumises à la supervision des régulateurs financiers européens.

L'angle mort que ces trois textes partagent. Malgré leur ambition et leur portée, NIS2, CER et DORA laissent ouvert un point qui est devenu une vulnérabilité systémique depuis mars 2026. DORA va le plus loin : son règlement délégué de 2024 oblige déjà les banques à tester la perte de centres de données, les attaques physiques, l'instabilité politique dans la juridiction de leur prestataire et les coupures de courant à grande échelle. CER oblige à évaluer tous les risques, terrorisme compris, mais pas à tester. Aucun de ces textes, en revanche, n'impose explicitement de tester la destruction physique simultanée de deux régions cloud dans deux pays différents, qui est précisément le scénario que les frappes iraniennes ont matérialisé, et hors du secteur financier, rien n'oblige à tester un scénario physique. Une organisation peut donc être en pleine conformité tout en étant incapable de survivre à ce type d'événement. C'est le chantier réglementaire que les événements de mars 2026 ont ouvert, et que ni les régulateurs ni les opérateurs ne peuvent continuer d'ignorer. Ce que cela signifie concrètement pour un dirigeant est simple : la conformité réglementaire est nécessaire mais pas suffisante. Elle protège contre les sanctions. Elle ne protège pas contre une frappe. Les deux logiques doivent coexister, et c'est précisément ce que la feuille de route du chapitre suivant permet de construire pas à pas.

Feuille de route sur 12 mois : de la lecture à l'action

Lire ce document sans en tirer un plan d'action daté et responsabilisé, c'est transformer une analyse stratégique en exercice intellectuel. Ce qui suit est une séquence directrice à adapter selon votre secteur, votre maturité IT et vos contraintes réglementaires propres. Ce n'est pas un guide d'implémentation clé en main, les réalités d'une PME de cinquante personnes et d'une banque régionale n'appelleront pas les mêmes réponses. C'est un cadre de priorisation conçu pour que chaque organisation puisse identifier, dans sa situation propre, par où commencer et dans quel ordre agir.

> **MOIS 1 À 3**
>
> Cartographier avant de décider

La première erreur des organisations qui réagissent à une crise est de prendre des décisions d'infrastructure sans avoir cartographié ce qu'elles cherchent à protéger. La priorité absolue des trois premiers mois est donc une cartographie complète de vos dépendances numériques critiques. Cela signifie identifier précisément quels systèmes sont hébergés où, par qui, dans quelle région géographique, avec quelles dépendances vers des services tiers comme DNS, CDN, points d'échange internet. Cela signifie également identifier votre point de défaillance unique :

l'endroit dont la destruction rend le reste inutilisable. Ce travail doit être conduit conjointement par les équipes techniques et les directions métier, parce que les premières savent où sont les systèmes, et les secondes savent lesquels sont véritablement critiques pour la continuité de l'activité. L'écart entre ces deux perceptions est presque toujours plus grand qu'on ne le croit. Le livrable de cette phase est un document d'une à deux pages, accessible aux dirigeants sans formation technique, qui répond à trois questions : où se trouve le cerveau de notre infrastructure, que se passe-t-il si ce cerveau disparaît ce soir, et combien de temps mettons-nous à reprendre nos opérations critiques dans ce scénario.

> **MOIS 4 À 6**
>
> Tester ce qu'on croit avoir

La plupart des organisations disposent déjà de plans de continuité, de contrats de sauvegarde, et d'architectures multi-sites. Le problème n'est pas leur absence. C'est qu'ils n'ont jamais été testés dans des conditions réelles. La deuxième phase consiste donc à organiser un exercice de bascule complet sur au moins un système critique, en simulant la disparition totale de l'infrastructure primaire de manière réelle. Pas un test technique en salle des serveurs. Un exercice impliquant les décideurs opérationnels, les équipes métier, et si possible les prestataires externes concernés. Cet exercice révélera systématiquement des problèmes que personne n'avait anticipés : des configurations obsolètes, des accès expirés, des dépendances invisibles entre systèmes, des procédures que personne ne sait plus exécuter sous pression. C'est précisément pour cela qu'il faut le faire maintenant, et non au moment d'une crise réelle. Le livrable de cette phase est un rapport d'exercice documentant les écarts entre le RTO et le RPO contractuels et les délais réellement observés pendant le test, assorti d'un plan de correction priorisé.

> **MOIS 7 À 9**
>
> Corriger les vulnérabilités identifiées

Les résultats de l'exercice de bascule définissent l'agenda de cette phase. Les corrections à apporter sont rarement toutes de même nature. Certaines sont techniques et peuvent être traitées rapidement : mettre à jour des configurations, activer des routes de secours, restaurer des accès. D'autres sont contractuelles et prennent plus de temps : renégocier des SLA, intégrer des clauses de résilience physique dans les contrats cloud, exiger des droits d'audit sur les infrastructures de vos prestataires critiques. D'autres encore sont structurelles et impliquent des décisions d'investissement : migrer certaines données vers des juridictions géographiquement distinctes, mettre en place des sauvegardes air-gapped, diversifier les routes de connectivité physique.

La priorisation doit suivre un critère simple : commencer par les vulnérabilités dont la matérialisation serait fatale à l'organisation, indépendamment de leur probabilité estimée. Ce que mars 2026 a appris au monde, c'est que les scénarios jugés improbables se matérialisent. Le critère de priorisation n'est donc pas la probabilité, mais l'impact.

MOIS 10 À 12

Ancrer la résilience dans la gouvernance

La résilience physique ne peut pas rester un projet ponctuel confié aux équipes informatiques. Elle doit devenir un attribut permanent de la gouvernance de l'organisation, au même titre que la conformité financière ou la gestion des risques juridiques. Cette dernière phase consiste à institutionnaliser ce qui a été construit. Cela signifie intégrer la revue annuelle des plans de continuité à l'agenda des instances dirigeantes, former les décideurs non techniques aux concepts fondamentaux documentés dans ce lexique, et désigner un responsable explicitement en charge de la résilience physique de l'infrastructure, avec un mandat clair et des ressources dédiées.

Cela signifie également actualiser le registre des risques de l'organisation pour y intégrer explicitement le scénario de frappe physique sur infrastructure cloud, avec une évaluation de son impact potentiel et une description des mesures de mitigation mises en place. Dans le cadre de NIS2 et CER, cette documentation n'est pas optionnelle. Elle constitue la preuve de conformité que les régulateurs peuvent demander à tout moment.

À l'issue de ces douze mois, votre organisation ne sera pas invulnérable. Aucune organisation ne l'est. Mais elle aura accompli ce que la grande majorité de ses pairs n'a pas encore fait : elle saura précisément ce qu'elle protège, comment elle bascule, depuis où elle reprend, et en combien de temps. C'est cette différence, entre ceux qui savent et ceux qui supposent, que mars 2026 a rendue stratégiquement décisive.

La géostratégie des infrastructures numériques : un nouveau champ disciplinaire. Ce que nous avons vécu le 1er mars 2026 à Abu Dhabi ne sera pas classé dans les annales comme un incident de continuité d'activité. Ce sera le moment où un concept qui circulait depuis des années dans les cercles académiques et les think tanks a reçu sa confirmation la plus brutale et la plus visible : la géostratégie des infrastructures numériques existe, elle est réelle, et elle tue des services bancaires.

LA GÉOSTRATÉGIE DES INFRASTRUCTURES NUMÉRIQUES

De la géopolitique classique à la techno-géopolitique

La géopolitique classique étudie comment la géographie physique, les montagnes, les fleuves, les détroits, les ressources naturelles, détermine les rapports de puissance entre États. La Mer Rouge était déjà un détroit stratégique sous les Pharaons. Ce qui est radicalement nouveau, c'est que cette même Mer Rouge transporte aujourd'hui simultanément du pétrole et des données. 17 câbles fibre-optique sous-marins y transitent, portant l'essentiel des échanges numériques entre l'Europe, l'Asie et l'Afrique. Couper ces câbles produit le même type de dommage stratégique que bloquer les tankers. La géographie n'a pas changé. Ce qui a changé, c'est ce qui y circule.

La techno-géopolitique, champ que l'analyste Abishur Prakash a notamment contribué à développer sous le nom de géopolitique de la technologie, va plus loin. Elle étudie comment la technologie elle-même devient un territoire, avec des frontières, des ressources, des zones d'influence et des conflits d'appropriation. Dans cette lecture, un datacenter n'est pas une usine. C'est un territoire numérique souverain. Localiser ce datacenter sous une montagne norvégienne plutôt qu'à Abu Dhabi, c'est exactement la même décision stratégique que choisir où implanter un port militaire.

Trois disciplines convergentes

Ce que les frappes iraniennes ont révélé, c'est la convergence de trois champs intellectuels qui fonctionnaient jusqu'ici en silos et qui, désormais, ne peuvent plus être pensés séparément.

- **Géopolitique des infrastructures critiques.** Ce qu'elle étudie : la localisation physique du pouvoir numérique, où sont les câbles, les datacenters, les nœuds internet critiques, et qui les contrôle. Auteur(s) de référence : Frédérick Douzet (IFG Paris 8), Chaire Castex de Cyberstratégie.
- **Souveraineté numérique.** Ce qu'elle étudie : l'indépendance décisionnelle, qui peut couper l'accès à vos données, qui contrôle les algorithmes, qui détient les clés de chiffrement. Auteur(s) de référence : Asma Mhalla, *Technopolitique* (Seuil, 2024) ; émission *CyberPouvoirs*, France Inter.
- **Géostratégie technologique.** Ce qu'elle étudie : la compétition inter-étatique pour la maîtrise des technologies fondamentales, semi-conducteurs, IA, cloud, quantique, dont les datacenters sont l'expression physique la plus visible. Auteur(s) de référence : Abishur Prakash, *The World is Vertical* (2021) ; rapports IA/Énergie.

Le technoféodalisme comme grille d'analyse

Il existe un quatrième cadre conceptuel, économique celui-là, qui éclaire ce qui s'est passé le 1er mars 2026 d'une façon que les analyses purement techniques ne permettent pas. L'économiste Cédric Durand a développé dans son ouvrage Technoféodalisme (Zones, 2020) une analyse de la rente numérique : les grandes plateformes ne fonctionnent plus comme des marchés capitalistes classiques mais comme des fiefs qui extraient de la valeur de leurs utilisateurs captifs sans produire directement. Sa thèse porte d'abord sur les plateformes de distribution, Google, Apple, Amazon Marketplace. Ce document étend cette logique à l'infrastructure cloud elle-même, une extrapolation que Durand ne formule pas explicitement mais que les événements de mars 2026 rendent difficile à éviter : quand une entreprise héberge l'intégralité de ses systèmes critiques chez un seul hyperscaler, elle ne loue pas un service, elle paie un tribut à un suzerain dont elle dépend existentiellement. Quand une frappe iranienne sur AWS met simultanément hors ligne des services bancaires et de paiement aux Émirats et des applications régionales de livraison, c'est exactement cette structure féodale qui se révèle dans toute sa fragilité : un seul suzerain technologique, des milliers de vassaux qui ne l'ont pas choisi pour sa géographie, et quand le château brûle, tout le fief s'effondre.

La résilience que je recommande dans ce document n'est pas seulement une mesure technique. C'est un acte de souveraineté politique : s'affranchir partiellement de la vassalité numérique. On ne peut plus parler de cybersécurité sans parler de géographie, et on ne peut plus parler de géopolitique sans parler d'infrastructure numérique. Cette logique de vassalité ne s'applique pas qu'aux hyperscalers américains. Les acteurs chinois comme Alibaba Cloud, Huawei Cloud, Tencent, sont soumis à la loi sur le renseignement national de 2017, dont l'article 7 impose une obligation légale de coopération avec les services de renseignement de Pékin.

Une organisation qui migrerait vers ces plateformes chinoises pour « diversifier » sa dépendance créerait une vassalité symétrique sous une juridiction différente. La souveraineté numérique réelle n'est atteignable que par une infrastructure dont la juridiction est politiquement cohérente avec les intérêts propres de l'organisation. La frontière entre attaque militaire et cyberattaque est devenue aussi floue que la frontière entre un datacenter et une cible militaire. Les frappes du 1er mars 2026 à Abu Dhabi ont officiellement marqué ce basculement.

La perspective MENA/Maghreb

Cette grille d'analyse prend une acuité particulière pour les organisations opérant entre l'Europe, le Maghreb et le Golfe, parce que leur exposition structurelle est différente de celle des entreprises européennes ou américaines. Elle est à la fois plus concentrée et moins visible. Plus concentrée parce que le Maghreb ne compte presque aucune région cloud d'hyperscaler sur son sol. À ce jour, ni AWS, ni Azure, ni Google Cloud n'y opèrent de région ; seul Oracle a ouvert, début 2026, une région publique à Casablanca. Pour l'essentiel, une organisation maghrébine qui adopte une architecture cloud héberge donc ses systèmes critiques à l'étranger, et dans la quasi-totalité des cas, le choix s'est orienté vers les régions du Golfe, pour des raisons de latence, de proximité culturelle et de disponibilité des certifications sectorielles exigées par les régulateurs locaux. Cette absence d'ancrage territorial n'est pas un choix stratégique. C'est une contrainte subie, rarement nommée comme telle.

Moins visible parce que la dépendance ne s'arrête pas à l'hébergement des données. Elle touche la connectivité elle-même. En Algérie, la loi n°18-04 de 2018 oblige légalement tous les opérateurs à faire transiter leur trafic international (hors satellite) via les infrastructures d'Algérie Télécom [REF-AT]. La dépendance n'est pas ici géographique, puisque les câbles algériens rejoignent directement l'Europe (SEA-ME-WE 4 d'Annaba à Marseille, ORVAL d'Oran à Valence), mais institutionnelle : un seul opérateur détient toutes les portes de sortie du pays. Pour le Maroc, la bande passante internationale utilisée a atteint 7 351 Gbit/s à fin 2025, soit la moitié de la capacité déployée [REF-ANRT] : la marge existe, mais rien ne permet de savoir publiquement par quels nœuds étrangers transite ce trafic. La Tunisie disposait déjà de routes directes vers l'Europe (SEA-ME-WE 4 vers Palerme et Marseille, Hannibal vers l'Italie). Le câble Medusa, qui a atterri à Bizerte en novembre 2025 et dont la mise en service est annoncée pour 2026, ajoute une route directe vers Marseille, et dessert aussi l'Algérie (Alger, Collo) et le Maroc (Nador, Tétouan). Cette diversification reste récente et n'a pas encore été intégrée dans les plans de continuité de la majorité des organisations qui en dépendent [REF-MEDUSA].

Le câble Africa Coast to Europe (ACE), dont le tracé longe la façade atlantique africaine sur 17 000 km en reliant 24 pays, offre théoriquement une route alternative vers l'Europe sans passer par le Golfe [REF-ACE], mais il n'atterrit dans aucun pays du Maghreb central : y accéder suppose un transit terrestre ou un autre câble. Mais pour la plupart des organisations maghrébines, cette route n'a pas été contractualisée comme chemin de secours indépendant. Elle partage des nœuds de transit avec les routes principales, recréant exactement le problème décrit dans le chapitre sur le multi-cloud : la diversité apparente masque une dépendance physique commune.

Cette absence de contractualisation n'est pas documentée dans des rapports publics, c'est une lacune précisément parce qu'aucune organisation n'a à ce jour publié ses plans de continuité en détaillant ses routes de secours. Elle est cependant cohérente avec le niveau de peering enregistré au point d'échange CAS-IX de Casablanca (opéré par N+ONE) : trois réseaux inscrits, dont deux de PCH, pour une capacité de 30 Gbit/s [REF-CASIX].

Les points d'échange internet de Casablanca sont l'actif géostratégique le plus sous-exploité de la région. Ils pourraient servir de nœud de transit alternatif pour le trafic MENA vers l'Europe sans passer par les IXP du Golfe, à condition d'en changer l'échelle. Mais leur niveau de peering actuel reste insuffisant pour absorber un basculement d'urgence régional. Il leur manque les accords d'interconnexion directe avec les opérateurs cloud tier-1, les capacités de bande passante pour traiter un volume de crise, et surtout la reconnaissance contractuelle comme route de secours dans les plans de continuité des organisations qui en auraient le plus besoin. Ce n'est pas un problème technique. C'est un problème de décision politique et réglementaire.

C'est précisément là que la géostratégie des infrastructures numériques rencontre la politique industrielle régionale. Renforcer le point d'échange CAS-IX, développer des accords de peering direct avec les hyperscalers sur ce nœud, et inciter les entreprises maghrébines à contractualiser des routes de transit indépendantes du Golfe sont des décisions qui appartiennent aux régulateurs nationaux, à l'ANRT au Maroc, à l'ARPCE en Algérie, à l'ATI en Tunisie, et non aux équipes informatiques des entreprises concernées.

Le Maroc a amorcé ce mouvement : le référentiel de qualification cloud publié au Bulletin officiel en août 2025 impose désormais aux entités publiques et aux infrastructures d'importance vitale de ne recourir qu'à des prestataires cloud qualifiés selon ce référentiel, et le gouvernement a annoncé en juillet 2025 un projet de datacenter souverain de 500 MW dans le cadre de la feuille de route Digital Morocco 2030 [REF-DM2030]. Ces décisions vont dans le bon sens. Elles ne résolvent pas pour autant la question posée par ce document : disposer d'un datacenter souverain ne suffit pas si les routes de connectivité qui y mènent passent encore par les mêmes nœuds de transit.

Tant que cette question reste sans réponse testée, la question adressée à tout décideur maghrébin demeure entière : si votre route principale disparaît, avez-vous vérifié que votre route de secours ne passe pas elle-même par le même nœud ?

Ces recommandations portent sur les interdépendances entre infrastructure industrielle et continuité opérationnelle dans l'espace MENA. Elles ne constituent pas une ingérence dans les politiques publiques.

Une cartographie complète des dépendances numériques secteur par secteur, avec des recommandations opérationnelles adaptées aux contraintes réglementaires et budgétaires propres à chaque juridiction, fera l'objet d'une édition dédiée.

L'avenir de l'infrastructure physique : de la cible à la forteresse. Les datacenters sont devenus des cibles militaires. Cette phrase, qui aurait semblé exagérée il y a cinq ans, est aujourd'hui un fait documenté, revendiqué, et répété. Elle va transformer la manière dont ces infrastructures sont conçues, localisées et protégées, non pas parce que l'industrie le choisit, mais parce qu'elle n'a plus le choix. Ce qui suit n'est pas de la prospective spéculative. Ce sont cinq trajectoires déjà en cours, certaines opérationnelles depuis des années, d'autres en développement actif, toutes accélérées par les événements de mars 2026.

L'AVENIR DE L'INFRASTRUCTURE PHYSIQUE : DE LA CIBLE À LA FORTERESSE

Les datacenters souterrains et fortifiés : une réalité déjà opérationnelle

L'idée de placer un datacenter sous une montagne vient directement de la doctrine militaire de la Guerre froide. Les États construisaient des bunkers dans du granit pour y loger leurs centres de commandement : le roc absorbe les ondes de choc, protège des frappes directes et isole naturellement de la chaleur extérieure. Cette logique n'a jamais disparu. Le Pionen Data Center à Stockholm en est la démonstration la plus visible : creusé à 30 mètres de profondeur dans le granit suédois, c'est un ancien abri de la défense civile reconverti en datacenter de haute sécurité, avec de vraies portes blindées, des groupes diesel de secours, et une architecture conçue pour résister aux frappes conventionnelles. La Suisse a industrialisé ce modèle depuis des décennies. Des entreprises comme Mount10 ou Safe Host vendent la neutralité politique helvétique autant que le granite alpin : deux arguments que mars 2026 a rendus soudainement très concrets pour leurs clients. Ce modèle va s'exporter massivement dans les prochaines années, et pas uniquement vers des pays neutres.

L'Islande offre une variante différente mais complémentaire. Plutôt que la protection par la roche, elle propose la protection par l'éloignement géographique, combinée à des avantages énergétiques rares : des sources d'eau souterraine à température stable assurent un refroidissement naturel, tandis que l'hydraulique et la géothermie fournissent une électricité presque entièrement renouvelable et bon marché. Un pays sans armée, membre fondateur de l'OTAN, géologiquement stable, et éloigné des zones de conflit actuelles. Après 2026, ce profil vaut de l'or.

La protection par la roche est réelle, mais elle a une limite que l'actualité de 2025 a rendue visible de façon brutale. À Natanz, les premières frappes israéliennes ont d'abord détruit l'alimentation électrique en surface, et l'AIEA a estimé que cette seule coupure avait pu endommager les centrifugeuses souterraines, avant de conclure que la salle elle-même avait probablement été atteinte par des munitions pénétrantes. Un datacenter souterrain dépendant du réseau électrique national partage exactement cette vulnérabilité : la roche amortit la frappe directe, sans garantie face aux munitions pénétrantes, et ne protège en rien contre la coupure de courant à 50 kilomètres de là sur une sous-station non enterrée. Les batteries de Pionen tiennent douze minutes à pleine charge ; au-delà, tout repose sur deux groupes diesel et sur leur approvisionnement en carburant. Dans un conflit prolongé, ce n'est pas suffisant.

La vraie résilience souterraine impose donc trois critères simultanés :

La protection physique par la roche, une production d'électricité locale ou suffisamment enterrée pour être elle-même protégée, et un système de refroidissement intégré à l'architecture souterraine et non exposé en surface.

C'est pourquoi l'Islande offre un niveau de résilience énergétique rare : une part de l'électricité vient du sous-sol, le refroidissement vient de sources d'eau souterraines, et une partie de la chaîne énergétique peut être enfouie, même si les trois quarts de la production restent hydrauliques, donc en surface. Ce n'est pas un avantage de confort énergétique. C'est un avantage géostratégique.

Une deuxième vulnérabilité est rarement mentionnée : l'accès humain. Un datacenter nécessite des interventions physiques que l'automatisation ne peut pas entièrement remplacer. En situation de conflit, l'entrée souterraine est un point d'attaque évident et peu coûteux. Les frappes américaines complémentaires sur le site d'Ispahan n'ont pas nécessairement détruit les galeries : elles ont visé les entrées des tunnels, ce qui suffit à immobiliser l'installation à moyen terme sans la détruire physiquement. Un datacenter souterrain dont les accès sont bloqués reste intact, allumé, refroidi. Mais il est inutilisable. La résilience physique doit donc inclure des entrées redondantes, enfouies depuis des directions différentes, et des protocoles d'accès qui ne dépendent pas d'un seul point d'entrée.

La troisième vulnérabilité est la connectivité réseau. Les câbles de fibre optique qui relient un datacenter souterrain au reste du monde remontent en surface exactement comme les câbles électriques. Pionen à Stockholm est protégé contre les bombes, mais ses liaisons vers les points d'échange internet doivent, à un moment, rejoindre le réseau de la ville.

Couper ces connexions ne détruit pas le datacenter : il reste intact, allumé, refroidi. Mais il est coupé du monde, aussi utile qu'une bibliothèque dont on a verrouillé la porte. La résilience réseau impose des connexions enfouies, redondantes, arrivant de directions géographiques différentes, avec des routes de secours qui ne partagent aucun point de transit commun.

Une dernière fragilité systémique mérite d'être nommée franchement :

Le paradoxe de la recommandation. Si l'ensemble des acteurs critiques suit la stratégie préconisée dans ce document et migre vers l'Islande, la Norvège et la Suisse, ces trois pays deviennent à leur tour des cibles stratégiques prioritaires. On ne supprime pas la vulnérabilité, on la déplace géographiquement. La vraie résilience systémique n'est pas la concentration dans des juridictions sûres, mais une distribution suffisamment large pour qu'aucune frappe unique, même massive, ne puisse paralyser simultanément plusieurs nœuds critiques. Concrètement, cette distribution mondiale doit intégrer des zones géographiques aux profils de risque véritablement distincts. L'Afrique subsaharienne, notamment le Kenya et le Rwanda qui développent activement leurs infrastructures numériques souveraines, offre une exposition géopolitique radicalement différente de l'Europe du Nord. L'Amérique latine, avec le Brésil et le Chili comme pôles émergents d'infrastructure, représente une troisième zone de diversification crédible. C'est une carte de risques diversifiés, construite sur le même principe que celui que ce document défend depuis sa première page : aucune frappe unique, même massive, ne doit pouvoir atteindre simultanément des nœuds situés sous des juridictions géopolitiquement indépendantes.

C'est un déplacement permanent du point de faiblesse vers un endroit où il est plus difficile à atteindre, plus coûteux à exploiter, et moins fatal s'il est touché.

Les datacenters sous-marins : une réalité commerciale aux vulnérabilités déplacées

Les sauvegardes air-gapped placées dans un bunker souterrain constituent la combinaison de protection la plus robuste disponible aujourd'hui. Trois isolations simultanées : logique, parce que le système est déconnecté du réseau et donc inatteignable à distance ; physique, parce que la structure durcie absorbe les chocs et résiste aux frappes ; géographique, parce que le site est distinct du principal et ne partage aucune dépendance commune avec lui. C'est ce que les militaires appellent une position de repli durcie, le seul type d'infrastructure qui résiste en même temps à une frappe physique, une cyberattaque et une coupure réseau prolongée. Microsoft a conduit entre 2018 et 2020 l'expérience la plus documentée du secteur avec le Projet Natick : un datacenter dans un conteneur étanche, immergé à 36 mètres de profondeur au large des côtes écossaises pendant deux ans, sans aucune intervention humaine. Le bilan a contredit plusieurs intuitions initiales. La fiabilité des serveurs était 8 fois supérieure à celle d'un datacenter terrestre équivalent. La raison est contre-intuitive : en immersion, le conteneur est rempli d'azote inerte qui élimine l'oxygène, supprimant la corrosion qui est l'ennemi numéro un des composants électroniques. La mer absorbe par ailleurs la chaleur des serveurs de manière passive, supprimant l'essentiel des besoins en climatisation. La limite principale que ce projet a mise en évidence reste la maintenance. Quand quelque chose tombe en panne à l'intérieur, remonter le conteneur entier est coûteux et lent. L'architecture doit donc être conçue pour que les serveurs fonctionnent sans intervention humaine pendant toute leur durée de vie, une contrainte radicalement différente de celle des datacenters terrestres. Ce qu'implique cette contrainte opérationnellement n'est pas souvent précisé : pendant toute la durée de remontée, de maintenance et de réimmersion d'un module, l'intégralité de l'infrastructure hébergée dans ce

module est indisponible. Pour un opérateur commercial qui a contractuellement garanti à ses clients un niveau de disponibilité minimal (SLA), c'est une contrainte de continuité de service non résolue à ce jour. Le modèle modulaire de Hainan répond partiellement à ce problème : 100 modules permettent d'en remonter un sans affecter les autres. Mais cette redondance a un coût d'infrastructure qui n'est pas encore reflété dans les comparaisons économiques avec les datacenters terrestres. C'est pour cette raison que Microsoft a choisi en 2024 de ne pas commercialiser Natick : techniquement prouvé, mais pas encore économiquement viable à grande échelle. Ce que Microsoft n'a pas franchi, la Chine l'a franchi. En décembre 2023, la société Highlander a immergé à 35 mètres de profondeur au large de Lingshui, dans la province de Hainan, le premier datacenter sous-marin commercial au monde. En février 2025, un nouveau module a été ajouté ; l'ensemble peut désormais traiter environ 7000 conversations d'intelligence artificielle simultanées par seconde. Dix entreprises ont déjà signé des contrats pour utiliser cette infrastructure, et le plan prévoit à terme 100 modules immergés dans cette seule zone. HiCloud revendique un gain d'efficacité énergétique global de 40 à 60% pour ses modules de Hainan, selon des déclarations de l'opérateur relayées par Data Center Dynamics en 2024. Des annonces ultérieures font état de gains plus conservateurs : plus d'un cinquième de consommation en moins pour le projet de Shanghai-Lingang, selon le gouvernement chinois, et plus de 30% d'efficacité énergétique pour Lingshui en 2026. L'avantage énergétique est réel ; son amplitude exacte reste à ce stade auto-déclarée. Cette efficacité repose cependant sur une hypothèse qui mérite d'être nommée : la stabilité de la température de l'eau. Les datacenters sous-marins côtiers sont implantés à faible profondeur, précisément là où les océans se réchauffent le plus vite sous l'effet du changement climatique. L'efficacité énergétique annoncée est calculée sur des températures d'eau actuelles. Elle se dégradera progressivement, et le refroidissement peut devenir insuffisant lors des épisodes de chaleur marine exceptionnelle. C'est une vulnérabilité à horizon 10-20 ans qui n'est pas prise en compte dans les projections actuelles. Mais l'expérience chinoise révèle aussi ce que ce document cherche à démontrer depuis sa première page : chaque nouvelle forme d'infrastructure déplace la vulnérabilité sans l'éliminer. Hainan se trouve en Mer de Chine méridionale, l'une des zones maritimes les plus militairement contestées au monde. Un datacenter protégé des drones aériens reste accessible à d'autres formes de menace sous-marine, et elles sont désormais documentées, opérationnelles, et en cours de prolifération rapide.

La première est la menace acoustique. Le risque acoustique sur les structures immergées n'est pas théorique. En novembre 2024, Thales et FEBUS Optics ont signé un accord de co-développement d'une solution de surveillance acoustique des infrastructures critiques sous-marines, basée sur la détection de toute anomalie vibratoire en tout point d'une structure immergée. L’existence même de cet accord de co-développement confirme que les opérateurs d’infrastructures critiques sous-marines intègrent désormais le risque acoustique dans leurs architectures de protection (surveillance passive des signaux hydrophones). Les principes de la guerre acoustique sous-marine, exploitation des vibrations basse fréquence pour déstabiliser des structures ou des équipements sensibles, sont quant à eux documentés dans la littérature militaire depuis plusieurs décennies, et leur application aux datacenters immergés constitue un vecteur d'attaque que les opérateurs de ces infrastructures intègrent désormais dans leurs

analyses de risques Ces dispositifs sont discrets, peu coûteux comparés à un missile, et ne laissent aucune signature visible en surface. C'est une vulnérabilité que personne n'avait anticipée lors de la conception de ces infrastructures, précisément parce qu'elles ont été pensées comme des réponses à des menaces aériennes et non sous-marines. La contre-mesure existe, elle consiste en des systèmes d'isolation vibratoire des racks et des capteurs acoustiques de surveillance périmétrique. Mais elle n'est pas encore intégrée dans les standards de construction des datacenters sous-marins commerciaux actuels, Hainan inclus.

La deuxième est la menace des drones sous-marins autonomes. « L'ère de la guerre des fonds marins, où les infrastructures sous-marines seront de plus en plus ciblées, est arrivée », écrivait H I Sutton dans Naval News en février 2024. La Chine a développé en mars 2025 un outil capable de couper des câbles sous-marins blindés à une profondeur de 4000 mètres, monté sur un bras robotique utilisant une meule diamantée tournant à 1600 tours par minute. La Russie opère une flotte de navires, sous-marins et drones sous-marins via sa Direction principale de recherche en eaux profondes, spécifiquement dédiée aux opérations contre les infrastructures critiques sous-marines. Ces vecteurs ne sont pas des projets : ce sont des capacités opérationnelles déployées. Entre novembre 2024 et janvier 2025, sept câbles sous-marins ont été endommagés dans la mer Baltique, dans des incidents dont la majorité est soupçonnée d'être des sabotages d'acteurs étatiques. Un drone sous-marin autonome lancé à des centaines de kilomètres de sa cible peut approcher sans être détecté, localiser le module par sonar, et le neutraliser sans laisser de signature exploitable. La réponse à cette menace est en cours de développement : les ministères de la Défense de six pays riverains de la Baltique et de la mer du Nord ont créé en décembre 2023 le Centre d'expérimentation pour la sécurité des fonds marins (SeaSEC), qui a tenu en mai 2025 des semaines d'essais intégrant des drones de surveillance sous-marine, des capteurs acoustiques distribués et des véhicules autonomes de patrouille. Mais la capacité offensive précède la capacité défensive, comme toujours. Et la connectivité reste le maillon le plus fragile de tout le système. Les câbles qui relient un datacenter sous-marin au reste du réseau sont des câbles sous-marins, exactement ceux dont la mer Rouge a montré la vulnérabilité : en février 2024, trois câbles y ont été sectionnés par l'ancre traînante d'un cargo touché par un missile houthi, perturbant 25% du trafic entre l'Asie, l'Europe et le Moyen-Orient, et l'un d'eux a nécessité cinq mois de réparation parce que les navires spécialisés ne pouvaient pas accéder à la zone en sécurité. Un datacenter sous-marin dont les connexions sont coupées reste intact, allumé, refroidi, et complètement inaccessible depuis le reste du monde. La résilience n'est pas une destination. C'est un déplacement permanent du point de faiblesse vers un endroit où il est plus difficile à atteindre, plus coûteux à exploiter, et moins fatal s'il est touché.

Les datacenters en orbite : réalité physique et contraintes incontournables

Plusieurs entreprises travaillent sur des datacenters orbitaux. Starcloud (ex-Lumen Orbit), aux États-Unis, est l'une des plus avancées. L'étude européenne ASCEND, financée par la Commission européenne et coordonnée par Thales Alenia Space, a publié ses résultats de

faisabilité en juin 2024. En orbite basse, entre 400 et 2000 km d'altitude, un satellite dispose d'une énergie solaire continue et échappe à toute frappe militaire conventionnelle. Aucun drone Shahed ne monte à 500 km. Cette phrase est exacte mais elle appelle une précision importante : si aucun drone iranien ne monte à 500 km, la Chine, la Russie et les États-Unis disposent tous de missiles antisatellites opérationnels capables d'atteindre l'orbite basse. Un datacenter orbital échappe aux drones de conflits hybrides régionaux. Il ne résiste pas à une confrontation entre puissances majeures. La stratification vers l'orbite déplace donc la vulnérabilité vers un niveau de menace supérieur : d'un conflit régional à une confrontation stratégique entre grandes puissances. Ce déplacement peut être acceptable selon le contexte, mais il doit être assumé consciemment, pas ignoré. Mais la physique ne négocie pas.

La première contrainte est la latence, et elle est incompressible. Même en orbite très basse à 500 km, le signal met 3 à 5 millisecondes pour l'aller-retour. Ce délai est invisible pour de l'archivage ou du traitement scientifique, mais il est rédhibitoire pour une transaction financière temps réel ou une chirurgie à distance. Les datacenters orbitaux ne pourront pas servir tous les usages, seulement ceux qui tolèrent ce délai. En octobre 2024, la JAXA et NEC ont réussi une communication optique inter-satellitaire par laser à 1,8 gigabits par seconde sur une distance de 40 000 km, un record mondial de débit dans la bande de 1,5 μm, selon NEC. C'est une avancée réelle et significative, notamment parce qu'un faisceau laser de quelques centimètres de diamètre dirigé précisément vers un satellite est quasi impossible à intercepter ou à brouiller, contrairement aux communications radio classiques. Sur le plan de la sécurité des infrastructures critiques, cette technologie est donc très pertinente. Mais elle ne change rien à la latence. La lumière laser voyage à la même vitesse que les ondes radio. Ce que le laser améliore, c'est la quantité d'informations transportées dans le même temps, pas la vitesse à laquelle le signal fait l'aller-retour. La contrainte physique de la latence reste entière, quelle que soit la technologie de transmission utilisée.

La deuxième contrainte est le refroidissement, et elle est contre-intuitive. On pourrait croire que le vide spatial, à moins 270 degrés, est un congélateur idéal.

En réalité, sans atmosphère, la seule manière d'évacuer la chaleur est le rayonnement infrarouge. Pour dissiper les watts produits par des serveurs à haute densité, il faudrait des panneaux radiateurs de plusieurs centaines de mètres carrés par mégawatt de puissance installée, une surface impossible à déployer dans l'état actuel des lanceurs.

La troisième contrainte est la maintenance. Envoyer un technicien réparer un serveur en orbite coûte des dizaines de millions de dollars par mission. L'architecture doit donc être conçue dès le départ pour fonctionner sans aucune intervention humaine pendant 10 à 15 ans, ce qui impose une redondance matérielle extrême et limite fondamentalement la densité de calcul embarquable.

Une quatrième contrainte mérite d'être ajoutée, parce qu'elle échappe à toute analyse géopolitique : Un événement de type Carrington, dont les estimations scientifiques situent la probabilité d'occurrence entre moins de 2% et 12% par décennie selon les modèles retenus; les travaux de Riley (Space Weather, AGU, 2012) l'estimant à environ 12%, tandis que Moriña et al.

(Scientific Reports, Nature, 2019) retiennent une fourchette de 0,46% à 1,88%, représente un risque de faible probabilité mais d'impact potentiellement catastrophique pour toute infrastructure numérique non protégée contre les surtensions électromagnétiques à grande échelle. Les satellites commerciaux actuels ne sont pas conçus pour résister à ce niveau d'exposition. Un datacenter orbital serait vulnérable à un phénomène naturel qu'aucun acteur étatique ne peut ni provoquer ni empêcher, et contre lequel il n'existe pas encore de solution technique économiquement viable. C'est la seule menace identifiée dans ce document qui soit totalement indépendante de la géopolitique.

Les données froides, c'est-à-dire celles qu'on doit conserver mais qu'on consulte rarement, archives légales, séquences génomiques, patrimoine culturel numérique, enregistrements scientifiques à long terme, rejoindront l'orbite dans un horizon de 15 à 20 ans, à condition que les coûts de lancement continuent de chuter au rythme qu'impose la réutilisation des lanceurs.

Ce n'est pas de la prospective spéculative. C'est une trajectoire déjà en cours, dont chaque étape est conditionnée par des variables économiques et technologiques mesurables.

Elle reste cependant soumise à une condition géopolitique fondamentale :

L'orbite basse est hors de portée des conflits régionaux, mais pas des confrontations entre grandes puissances. Stocker des archives légales ou du patrimoine culturel en orbite a du sens dans un monde où la menace principale reste le drone ou le missile de théâtre.

Ce sens disparaît si le contexte bascule vers une confrontation directe entre puissances nucléaires. C'est un choix stratégique à faire consciemment, pas une évidence technique.

En termes simples : le souterrain pour le critique, le sous-marin pour le sensible, l'orbite pour le froid. Sous réserve que le ciel reste un espace suffisamment préservé pour que cette dernière couche tienne ses promesses.

Cette stratification est une architecture de destination. Elle ne se met pas en place au moment de la crise : elle doit exister avant. Ce point est crucial et souvent mal compris. On ne migre pas des données critiques vers un bunker souterrain en réponse à une frappe imminente. La migration prend du temps, de la bande passante, et suppose que la décision de basculer ait été prise et testée longtemps avant que la menace n'arrive.

La vraie résilience opérationnelle impose donc que chaque couche de cette stratification soit accompagnée d'un plan de bascule défini : le RTO (Recovery Time Objective, temps maximal acceptable avant reprise de service) et le RPO (Recovery Point Objective, perte de données maximale acceptable) pour chaque type de données et chaque type d'incident.

Un datacenter souterrain qui n'a jamais testé la bascule depuis le datacenter primaire n'est pas une forteresse. C'est une salle de secours que personne ne sait utiliser sous pression.

Vers une stratification des infrastructures selon le risque

Les horizons temporels indiqués sont des estimations conditionnelles, non des prédictions. La colonne Signal concret ancre chaque trajectoire dans des faits observables à la date d'avril 2026. Les mentions ⚠ signalent les vulnérabilités résiduelles après déplacement de la menace.

HORIZON	TYPE D'INFRASTRUCTURE	USAGE OPTIMAL	SIGNAL CONCRET	NIVEAU DE RÉALITÉ
Aujourd'hui	**Souterrain / bunker fortifié** Dans un pays neutre géopolitiquement	Services critiques, données souveraines, sauvegardes air-gapped.	**Pionen, Stockholm** : ancien abri de la défense civile reconverti, opérationnel depuis 2008. **Mount10 et Safe Host**, en Suisse, vendent la neutralité helvétique autant que le granite alpin, deux arguments que mars 2026 a rendus très concrets.	**Opérationnel. Argument renforcé par les frappes sur AWS de mars 2026.** ⚠ Limite : alimentation électrique et refroidissement remontent en surface (cf. Natanz, 2025). Autonomie diesel : quelques jours seulement. L'Islande (géothermie souterraine) offre un niveau de résilience supérieur.
2026 à 2030	**Sous-marin côtier** Immergé à 30 à 40 m de profondeur	Stockage distribué, données chaudes, réduction de la latence régionale.	**Hainan, Chine** : premier datacenter sous-marin commercial (Highlander / HiCloud), opérationnel en décembre 2023, étendu en février 2025. **Projet Natick** (Microsoft) : fiabilité 8 fois supérieure prouvée sur deux ans.	**Viabilité commerciale prouvée. Déploiements en cours.** ⚠ Menaces identifiées : guerre acoustique (vibrations basse fréquence), drones sous-marins autonomes (la Chine a développé un outil de coupe à 4 000 m, mars 2025), câbles de connectivité exposés en surface. Réchauffement des océans côtiers : efficacité énergétique à surveiller à horizon 10 à 20 ans.
2030 à 2035	**Edge computing orbital (LEO)** Micro-nœuds embarqués sur satellites	Traitement satellite, données d'observation, IA embarquée, surveillance maritime.	**SpaceX Starlink** : intégration de calcul en cours d'évaluation. **Starcloud (ex-Lumen Orbit)** : feuille de route active et levée de fonds. **JAXA et NEC** : liaison laser inter-satellitaire à 1,8 Gbps démontrée en octobre 2024 sur 40 000 km.	**Feuilles de route actives. Premières démonstrations réussies.** ⚠ Hors de portée des conflits régionaux (drones, missiles de théâtre). Vulnérable aux missiles antisatellites (ASAT) de la Chine, de la Russie et des États-Unis. Ce déplacement vers l'orbite doit être assumé consciemment.
2035 à 2045	**Datacenter orbital haute densité** Infrastructure lourde en orbite basse	Archives froides, calcul scientifique massif, données patrimoniales à très long terme.	**Conditionné à trois variables mesurables :** 1. coût de lancement sous 200 USD/kg (SpaceX Starship en cours) ; 2. résolution du problème des radiateurs thermiques (plusieurs centaines de m² par mégawatt) ; 3. stabilité géopolitique de l'orbite basse (risque ASAT).	**Prospectif conditionnel. Variables de déclenchement identifiées et mesurables.** ⚠ Risque additionnel : événements solaires extrêmes (type Carrington) susceptibles de détruire l'électronique non blindée en LEO. Aucune solution économiquement viable à ce jour.

CONCLUSION : LA RÉSILIENCE, UNE PHILOSOPHIE AUTANT QU'UNE TECHNIQUE

Le cloud n'est pas une infrastructure abstraite et immatérielle. C'est du béton, des câbles, des batteries, des groupes électrogènes, et donc une cible physique, comme un pont, une centrale électrique ou un aéroport. Les frappes iraniennes sur AWS en mars 2026 ont officiellement mis fin à une illusion de deux décennies : l'idée que les datacenters sont des infrastructures commerciales neutres, en dehors des équations géopolitiques et militaires. Trois cadres permettent désormais de lire cette réalité avec précision. La géostratégie des infrastructures numériques, d'abord, comme discipline qui nomme ce que beaucoup pressentaient sans pouvoir le formuler. Le technoféodalisme ensuite, comme grille économique qui explique pourquoi la destruction d'un seul château numérique peut paralyser des milliers de vassaux sur cinq continents. La stratification de l'infrastructure physique enfin, du bunker souterrain au

datacenter orbital, comme horizon de transformation à vingt ans qui est déjà en cours, pas encore à venir.

Ces trois dimensions ensemble permettent de penser la résilience non plus seulement comme un plan de continuité d'activité, mais comme un choix de souveraineté. Ce choix doit être fait les yeux ouverts. Ce que ce document préconise n'est pas une forteresse unique, aussi sophistiquée soit-elle. C'est une fédération de noeuds souverains distribués, dont chaque couche physique répond à un niveau de menace distinct. Le souterrain protège contre la frappe conventionnelle et reste sous contrôle territorial direct. Le sous-marin échappe aux conflits aériens tout en maintenant une connectivité physique contrôlée par des opérateurs identifiés. L'orbital soustrait les données froides à toute portée régionale, sous réserve que la juridiction de lancement reste politiquement cohérente avec les intérêts de l'organisation.

Ces trois couches ne fonctionnent pas en silos. Elles fonctionnent comme les noeuds d'une architecture fédérée : distribuée pour qu'aucune frappe unique ne paralyse l'ensemble, mais contrôlée pour que la souveraineté sur chaque noeud reste clairement attribuée. Ce n'est pas une blockchain décentralisée sans autorité. C'est une fédération souveraine dans laquelle la confiance est redistribuée entre des acteurs qui se contrôlent mutuellement, exactement comme des États membres qui coopèrent sans se dissoudre.

Ce document l'a démontré section par section : chaque solution proposée déplace la vulnérabilité sans l'éliminer. Le datacenter souterrain résiste mieux à la bombe, mais pas à la coupure d'électricité en surface. Le datacenter sous-marin échappe aux drones aériens mais pas aux drones sous-marins ni à la guerre acoustique. Le datacenter orbital échappe aux conflits régionaux mais pas aux missiles antisatellites des grandes puissances. Il faut nommer également un angle mort réglementaire : hors du secteur financier, aucun texte européen n'impose de tester un scénario de destruction physique, et même DORA, qui exige de tester la perte d'un centre de données ou une attaque physique, ne vise pas la destruction simultanée de deux régions cloud dans deux pays différents.

Les événements de mars 2026 ont révélé un chantier réglementaire ouvert que ni les régulateurs ni les opérateurs ne peuvent ignorer. La résilience n'est pas une forteresse imprenable. C'est une architecture d'arbitrages conscients : choisir où déplacer le risque, à quel niveau de menace l'exposer, et s'assurer que si ce niveau est atteint, les dommages restent supportables. C'est pour cela qu'elle est une philosophie autant qu'une technique.

La vraie résilience n'est pas la technologie. C'est la diversité d'infrastructure, la capacité à basculer vite, et la décision politique de ne plus dépendre d'un seul suzerain numérique. Parce que le château peut brûler. La forteresse, elle, doit tenir.

NOTICE BIBLIOGRAPHIQUE

Titre	Quand le cloud prend feu
Auteur	Nizar Younes Mqam, ORCID 0009-0008-5549-7620
Publication en série	Cahiers de technopolitique, n° 1
Éditeur	Nizar Younes Mqam, Tourcoing, France
Directeur de publication	Nizar Younes Mqam
Date de publication	Septembre 2026 (première édition : avril 2026)
Révision	7 octobre 2026 : vérification de toutes les citations, de tous les chiffres et de toutes les attributions sur les sources primaires ; corrections de dates, de chiffres, d'attributions et de références, coupures de citations signalées par [...]. Le propos est inchangé. Version 1.4, même jour : nettoyage des restes de conversion du document d'origine (intertitres, sommaire et en-têtes de page résiduels, tableau des trois disciplines, phrase tronquée, glossaire), suppression d'un bloc de contact égaré dans la référence 43, correction de quatre incohérences (câbles de la mer Rouge, date du scénario des 1er et 2 mars, point d'échange CAS-IX, période de vérification des sources). Version 1.5, 9 octobre 2026 : rétablissement du tableau « Vers une stratification des infrastructures selon le risque », perdu à la régénération des versions 1.2 à 1.4, harmonisé avec le texte vérifié (abri de la défense civile de Pionen, extension de Hainan en février 2025, Starcloud ex-Lumen Orbit) ; deux affirmations sans source adoucies (Mount10 et Safe Host, demande du marché).
Langue	Français · version anglaise (DOI 10.5281/zenodo.23270771)
DOI	10.5281/zenodo.23270770 Toutes versions : 10.5281/zenodo.22812310
Dépôt pérenne	Zenodo, hébergé par le CERN
Licence	CC BY-NC-ND 4.0

SOURCES ET RÉFÉRENCES

Toutes les sources ont été consultées et vérifiées entre le 1er mars et le 4 avril 2026, puis revérifiées sur les sources primaires le 7 octobre 2026. La numérotation est celle du document.

FRAPPES IRANIENNES SUR AWS : FAITS ET CHRONOLOGIE

1. Rest of World, « Iranian drone strikes at Amazon sites raise alarms over protecting data centers », 4 mars 2026. https://restofworld.org/2026/iran-amazon-data-center-strikes/
2. The Conversation, « Why Iran targeted Amazon data centers », 1 avril 2026. https://theconversation.com/why-iran-targeted-amazon-data-centers-278642
3. Fortune, « Iran's attacks signal a new kind of war », 9 mars 2026. https://fortune.com/2026/03/09/irans-attacks-on-amazon-data-centers-in-uae-bahrain-signal-a-new-kind-of-war-as-ai-plays-an-increasingly-strategic-role-analysts-say/
4. Bloomberg, « How Amazon Data Centers Became a Casualty of Iran War », 5 mars 2026. https://bloomberg.com/news/articles/2026-03-05/how-amazon-data-centers-became-a-casualty-of-iran-war
5. Data Centre Magazine, « Reports: Iran Missiles Hit AWS Cloud Site in Bahrain », 2 avril 2026. https://datacentremagazine.com/news/iran-missiles-hit-aws-cloud-infrastructure-in-bahrain
6. CNBC, « Data centers become military targets », 6 mars 2026. https://cnbc.com/2026/03/06/iran-war-data-centers.html

IMPACT TECHNIQUE : AWS HEALTH DASHBOARD ET ANALYSES

1. APIStatusCheck, « AWS Middle East Outage March 2026 », 6 mars 2026. https://apistatuscheck.com/blog/aws-middle-east-drone-strike-outage-march-2026
2. Network World, « Amazon waives March AWS charges », 30 mars 2026. https://networkworld.com/article/4151880

CÂBLES SOUS-MARINS ET CONNECTIVITÉ MONDIALE

1. Rest of World, « U.S.-Iran war threatens Gulf AI infrastructure », mars 2026. https://restofworld.org/2026/us-iran-war-gulf-ai-submarine-cables/
2. TeleGeography, « Submarine Cable Infrastructure and Hormuz », mars 2026. https://resources.telegeography.com/submarine-cable-infrastructure-strait-hormuz
3. Submarine Networks, « War in the Gulf Severs the World's Digital Arteries », mars 2026. https://submarinenetworks.com/en/nv/insights/war-in-the-gulf-severs-the-world-s-digital-arteries
4. German Marshall Fund, « Stuck in Hostile Waters », mars 2026. https://gmfus.org/news/stuck-hostile-waters

MENACES SOUS-MARINES ET GUERRE DES FONDS MARINS

1. Naval News, « Cable Attack: New Undersea Threat Is Starting To Reshape Naval Wars », février 2024. https://navalnews.com/naval-news/2024/02/cable-attack-new-undersea-threat-is-starting-to-reshape-naval-wars/
2. Asia Times, « PLAN's big underwater drones push undersea power toward US shores », décembre 2025. https://asiatimes.com/2025/12/plans-big-underwater-drones-push-undersea-power-toward-us-shores/
3. Internationale Politik Quarterly, « The Underwater Battlefield: Protecting Submarine Critical Infrastructure », janvier 2025. https://ip-quarterly.com/en/underwater-battlefield-protecting-submarine-critical-infrastructure

4. University of Washington / Jackson School, « Baltic Sea Undersea Cable Security », billet de Sophie Himka, étudiante de licence, 9 juillet 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/

5. Blueye Robotics / SeaSEC, « Surveillance of Critical Underwater Infrastructure using modern underwater technology », Oda Ryggen, juillet 2025. https://blueyerobotics.com/blog/surveillance-of-critical-underwater-infrastructure-using-underwater-technology

6. Thales & FEBUS Optics, « Accord de co-développement pour la protection des infrastructures critiques sous-marines par surveillance acoustique distribuée », 6 novembre 2024. https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/thales-and-febus-optics-sign-strategic-co-development

INSTALLATIONS SOUTERRAINES : RÉFÉRENCE EMPIRIQUE NATANZ

1. Institute for Science and International Security, « Post-Attack Assessment of the First 12 Days of Israeli and U.S. Strikes on Iranian Nuclear Facilities », David Albright et Spencer Faragasso, 24 juin 2025. https://isis-online.org/isis-reports/post-attack-assessment-of-the-first-12-days-of-israeli-strikes-on-iranian-nuclear-facilities

2. Arms Control Association, « Iran's Nuclear Facilities: Status Updates », juin 2025. https://armscontrol.org/blog/2025-06-25/irans-nuclear-facilities-status-updates

3. New Civil Engineer, « What we know about Iran's underground nuclear facilities », juin 2025. https://newcivilengineer.com/latest/what-we-know-about-irans-underground-nuclear-facilities-19-06-2025/

CADRE RÉGLEMENTAIRE EUROPÉEN : NIS2, CER, DORA

1. Commission européenne, « CER and NIS-2 Directives enter into application », octobre 2024. https://ec.europa.eu/newsroom/cipr/items/859754/

2. Bird & Bird, « Understanding NIS2, CER, and CRA », mars 2025. https://twobirds.com/en/insights/2025/understanding-key-eu-cybersecurity-legislative-acts-nis2,-cer,-and-cra

3. nFlo, « CER: six months to full implementation », novembre 2025, mis à jour en février 2026. https://nflo.tech/knowledge-base/cer-six-months-critical-infrastructure-implementation/

PROJETS DATACENTERS DU FUTUR

1. Microsoft Research, Project Natick. https://natick.research.microsoft.com/

2. Data Centre Dynamics, « Project Natick: Microsoft's underwater voyage of discovery », janvier 2021. https://datacenterdynamics.com/en/analysis/project-natick-microsofts-underwater-voyage-discovery/

3. Highlander / HiCloud, Hainan Undersea Data Center. https://www.highlander.com.cn

4. Data Center Dynamics, « China's HiCloud reports commercial underwater data center modules are working », 2024. https://www.datacenterdynamics.com/en/news/chinas-hicloud-reports-commercial-underwater-data-center-modules-are-working/

5. Lumen Orbit (devenue Starcloud), Orbital computing. https://www.starcloud.com

6. Bahnhof AB, Pionen Data Center Stockholm. https://bahnhof.se/foretag/colocation/datacenter/pionen/

7. JAXA et NEC, Communication laser inter-satellitaire LUCAS, 1,8 Gbps, janvier 2025. https://nec.com/en/press/202501/global_20250123_01.html

CADRE INTELLECTUEL : GÉOSTRATÉGIE NUMÉRIQUE ET TECHNO-GÉOPOLITIQUE

1. Asma Mhalla, Technopolitique. Seuil, 2024.
2. Cédric Durand, Technoféodalisme. Critique de l'économie numérique. Zones, 2020.
3. Frédérick Douzet, Chaire Castex de Cyberstratégie (2013–2018), IHEDN / Institut Français de Géopolitique (IFG) - Université Paris 8. Page de l'auteure (GEODE) : https://geode.science/frederick-douzet/ - IFG Paris 8 : https://www.univ-paris8.fr/Institut-francais-de-geopolitique-IFG
4. Abishur Prakash, analyses techno-géopolitiques. https://www.abishurprakash.com

PROBABILITÉ CARRINGTON

1. Riley, P. (2012). « On the probability of occurrence of extreme space weather events ». Space Weather, American Geophysical Union. https://doi.org/10.1029/2011SW000734
2. Moriña, D., Serra, I., Puig, P., & Corral, Á. (2019). « Probability estimation of a Carrington-like geomagnetic storm ». Scientific Reports, Nature Publishing Group. https://doi.org/10.1038/s41598-019-38918-8

LA PERSPECTIVE MENA/MAGHREB

1. [REF-AT-1] Loi n°18-04, article 126, Journal officiel algérien. [REF-AT-2] Algérie Télécom, Catalogue d'Interconnexion 2025-2026, https://www.algerietelecom.dz/docs/document/autres/CATALOGUE-D-INTERCONNEXION-D-ALGERIE-TELECOM-2025-2026-14776.pdf
2. [REF-MEDUSA] Tunisie Telecom, câble sous-marin Medusa (Bizerte–Marseille, 22 Tbps), partenariat signé février 2025, atterrissement à Bizerte le 1er novembre 2025. https://www.leaders.com.tn/article/37431-tunisie-telecom-celebre-l-atterrissement-du-cable-sous-marin-medusa-a-bizerte-un-tourna
3. [REF-ACE] Africa Coast to Europe Submarine Cable (ACE), 2021. https://ace-submarinecable.com/le-systeme-de-cable-ace-relie-desormais-leurope-lafrique-de-louest-et-lafrique-du-sud/
4. [REF-ANRT] ANRT, Observatoires ANRT, Le Mémo T4-2025, mars 2026. https://anrt.ma/sites/default/files/2026-03/Observatoires%20ANRT%20-%20le%20Memo%20-%20T4-2025.pdf
5. [REF-CASIX] Internet Society Pulse / PeeringDB, Casablanca Internet Exchange Point, CAS-IX, données novembre 2025. https://pulse.internetsociety.org/fr/ixp-tracker/ixp/760/
6. [REF-DM2030-1] Arrêté du Chef du gouvernement n° 3-17-25 du 1er août 2025 fixant le référentiel des exigences de qualification des prestataires de services cloud, Bulletin officiel n°7432, DGSSI Maroc (réglementaire). [REF-DM2030-2] Agence Ecofin / Reuters, « Cloud hybride et souveraineté : le Maroc annonce un nouveau datacenter de 500 MW », juillet 2025. + Bulletin officiel n°7432, référentiel de qualification cloud, 21 août 2025. https://www.agenceecofin.com/actualites-numerique/1107-129990 https://www.digital.ma/articles/le-maroc-impose-un-referentiel-cloud-pour-proteger-sa-souverainete-numerique

POUR CITER CE DOCUMENT

Mqam, N. Y. (2026). *Quand le cloud prend feu.* Cahiers de technopolitique, n° 1. https://doi.org/10.5281/zenodo.23270770

Cahiers de technopolitique, n° 1 · Étude · Septembre 2026
Éditeur et directeur de la publication : Nizar Younes Mqam · Lieu d'édition : Tourcoing, France
DOI : 10.5281/zenodo.23270770
Contact : y.nizar@proton.me · https://technopolitique.eu/cahiers/n1/
ORCID de l'auteur : https://orcid.org/0009-0008-5549-7620

© 2026 Nizar Younes Mqam. Publié en accès ouvert sous licence Creative Commons Attribution – Pas d'Utilisation Commerciale – Pas de Modification 4.0 International (CC BY-NC-ND 4.0). Partage et citation autorisés avec attribution ; modification et usage commercial interdits. creativecommons.org/licenses/by-nc-nd/4.0/deed.fr