L'Institut de Recherche en Géopolitique et d'Etudes Stratégiques (IRGES) est, en République Démocratique du Congo, le principal centre indépendant de recherche, de formation, d'information et de débat sur les grandes questions internationales. Créé en 2016 par le Professeur Kabwita Kabolo Iko, l'IRGES est un établissement d'utilité publique reconnu par les Arrêtés–Ministériels N°MIN.RST/CAB.MIN/054/2018 portant agrément des activités scientifiques et technologiques de l'Institut de Recherche en Géopolitique et d'Etudes Stratégiques et N°125/CAB/MIN/CA/PKB/2018 accordant avis favorable valant autorisation de fonctionnement de la Maison d'éditions IRGES.

Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux. Il associe, au travers de ses études et ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale et dispose d'un personnel-ressource capable de réfléchir largement sur les domaines indiqués et de proposer en forme textuelle et contextuelle des orientations, de la documentation et même des projets finalisés.

DOMAINES DE RECHERCHE
Prospections diplomatiques et géopolitique africaine
Organisations intergouvernementales et Intégration régionale
Etudes stratégiques sur le monde asiatique
Résolution des conflits, Conseil stratégique et prospection sur la paix et la sécurité
Pratique de négociation internationale et d'affaires
Droits humains et Droit humanitaire
Gender et Promotion des droits de la femme
Pratiques démocratiques et de bonne gouvernance
Communication, Coaching politique et Relations publiques
Marketing politique et leadership axés sur les résultats
Développement durable, Environnement et Ecologie
Management des projets nationaux et internationaux
Statistiques, Etudes économiques et sociales
Santé publique
Intelligence Artificielle et Télécommunications
Psychopédagogie

SERVICES OFFERTS
Formations
Réunions scientifiques
Gestion de projets
Revue Intelligence Stratégique
Accueil de stagiaires
Consultation d'experts
Bibliothèque numérique et en dur
IRGES éditions

L'Institut de Recherche en Géopolitique et d'Etudes Stratégiques (IRGES) est ouvert et intéressé vis-à-vis de toutes personnes, structures, institutions, entreprises ou organisations dont les domaines d'interventions et les services susmentionnés pourraient être de plus utiles à leur progrès, leur rentabilité, leur notoriété et leur reconnaissance populaire.

E-ISSN : 3006-5488 ; P-ISSN : 3006-547X
https://doi.org/10.62912/JYTU3565
www.revue-is.org

Maquette couverture : Editions IRGES Kinshasa-Genève

PARTENARIAT STRATEGIQUE USA-RDC
Enjeux, opportunités & appropriation effective

2026

Revue Intelligence Stratégique

3ème

GRANDE CONFERENCE

CORPS DE L'ELITE SCIENTIFIQUE DE L'UDPS
CES-UDPS

THEME

PARTENARIAT STRATEGIQUE USA-RDC
Enjeux, opportunités & appropriation effective

Du 22 au 23 Juin 2026 - HILTON KINSHASA

NUMERO SPECIAL

«La science au service au peuple»

INSTITUT DE RECHERCHE EN GEOPOLITIQUE ET D'ETUDES STRATEGIQUES

Revue

Intelligence Stratégique

Vol. 009, Numéro Spécial, Juillet 2026
E-ISSN : 3006-5488, P-ISSN : 3006-547X
https://doi.org/10.62912/JYFU3565

Siège social : 292, avenue Mweka, Commune de Lingwala, Kinshasa, République Démocratique du Congo.
Téléphone : +243 89 7175 074 ; 82 006 1696
E-mail : felly.lukunga@revue-is.org, article@revue-is.org, info@revue-is.org ;
Internet : www.revue-is.org ; www.irges.org
Europe : 59, Rue du Rhône, 1204 Genève, Suisse, + 41 22 810 88 68, Chambre de Commerce Suisse-RD Congo, info@ccsc.ch

Revue Intelligence Stratégique
Journal des publications scientifiques
Volume 9, Numéro Spécial
Juillet 2026
p-ISSN : 3006-547X ; e-ISSN : 3006-5488
https://doi.org/10.62912/CES-UDPS00010
www.revue-is.org

INFRASTRUCTURES CRITIQUES ET RESILIENCE AUX MENACES HYBRIDES. LE CAS PARADIGMATIQUE DE L'EPIDEMIE D'EBOLA BUNDIBUGYO (MAI 2026) ET LES ENJEUX DE SOUVERAINETE POUR LA REPUBLIQUE DEMOCRATIQUE DU CONGO

Dr. Donat Soft MUKUNA MUYA
Coordonnateur National du Corps de l'Élite Scientifique de l'UDPS (CES-UDPS)
Chercheur en Sécurité, Défense et Stratégie
Spécialiste des nouvelles conflictualités et des enjeux géostratégiques contemporains (Hybrid warfare)

Arly NTUMBA TSHIELA
Doctorante en Stratégie, Sécurité et Défense. Collège des Hautes Études de Stratégie et Défense (CHESD), Kinshasa, RDC

RÉSUMÉ

L'étude porte sur la vulnérabilité des infrastructures critiques face aux menaces hybrides, notamment les cyberattaques, le sabotage, la désinformation, la coercition économique et les crises sanitaires. À partir du cas de l'épidémie d'Ebola Bundibugyo de mai 2026, il montre qu'une crise naturelle peut devenir un instrument stratégique lorsqu'elle rencontre des faiblesses préexistantes en matière de surveillance, d'expertise et de maîtrise de l'information. L'étude recommande à la RDC de renforcer sa résilience par la cartographie des infrastructures vitales, la cybersécurité, la diversification des réseaux, la coopération régionale et la souveraineté technologique.

Mots-clés *: infrastructures critiques ; menaces hybrides ; cybersécurité ; résilience ; souveraineté.*

ABSTRACT

The study examines the vulnerability of critical infrastructure to hybrid threats, including cyberattacks, sabotage, disinformation, economic coercion, and health crises. Using the Bundibugyo Ebola outbreak of May 2026 as a case study, it demonstrates that a natural crisis can become a strategic tool when it intersects with preexisting weaknesses in

surveillance, expertise, and information management. The study recommends that the DRC strengthen its resilience through the mapping of vital infrastructure, cybersecurity, network diversification, regional cooperation, and technological sovereignty.

Keywords : *critical infrastructure; hybrid threats; cybersecurity; resilience; sovereignty.*

INTRODUCTION

Imaginons Kinshasa, un matin ordinaire. La ville s'éveille sans électricité ; les antennes-relais sont muettes et aucun réseau mobile ne répond ; les paiements par téléphone sont impossibles, gelant d'un coup l'économie informelle qui fait vivre des millions de ménages ; et, dans les quartiers, l'eau courante ne coule plus. Cette paralysie ne résulte ni d'une guerre déclarée ni d'un orage tropical. Elle peut survenir parce qu'à des milliers de kilomètres un câble sous-marin a été sectionné, ou parce qu'une ligne de code malveillante a éteint un poste électrique. Ce scénario, qui relevait de la fiction il y a encore une décennie, décrit aujourd'hui le visage le plus probable du conflit contemporain : une agression qui ne vise plus les armées, mais les systèmes qui font fonctionner la nation.

Le déplacement est profond. Hier, la guerre se menait avec des chars, des avions et des armées visibles ; l'agresseur était identifié, l'attaque attribuable et la riposte légitime. Aujourd'hui, on ne renverse plus un pays en alignant des divisions blindées : on le fait vaciller en s'attaquant à ce qui le fait tenir debout. Les coups portés aux infrastructures critiques empruntent des moyens qui demeurent délibérément en deçà du seuil de la guerre ouverte : la cyberattaque, le sabotage discret, la désinformation, la coercition économique. Leur efficacité tient précisément à cette zone grise où il devient ardu de désigner un coupable, donc de justifier une réponse coordonnée.

Cette mutation n'est pas une abstraction théorique pour la République Démocratique du Congo (RDC). Le partenariat stratégique noué entre Kinshasa et Washington consacre explicitement la protection des infrastructures critiques comme un axe de coopération (Article II sur les objectifs, point 2). En reconnaissant que la sécurité d'un État se mesure désormais à la robustesse de ses réseaux énergétiques, numériques et logistiques autant qu'à celle de ses frontières, ce partenariat inscrit la question au cœur de l'agenda national. Encore faut-il en saisir toute la portée conceptuelle et opérationnelle, c'est l'objet de cet article.

Cette contribution poursuit trois objectifs. Premièrement, clarifier les concepts d'infrastructure critique et de menace hybride, et exposer les mécanismes systémiques qui rendent les sociétés hyperconnectées si fragiles. Deuxièmement, documenter empiriquement la banalisation de ces modes d'action à travers une

jurisprudence d'incidents mondiaux récents, et en mesurer l'exposition particulière du continent africain et de la RDC. Troisièmement, à partir d'une étude de cas paradigmatique — la séquence observée autour de l'épidémie d'Ebola Bundibugyo de mai 2026, proposer un cadre national de résilience qui fasse de la protection des infrastructures un véritable exercice de souveraineté.

La thèse défendue est volontairement contre-intuitive, et nous l'énonçons d'emblée comme une hypothèse de travail à valeur heuristique, non comme une accusation établie. On suppose habituellement qu'une menace requiert un agresseur identifié animé d'un dessein offensif explicite. Nous soutenons au contraire qu'il suffit qu'un acteur dispose d'une capacité asymétrique à exploiter des vulnérabilités préexistantes. Une crise n'a pas besoin d'être fabriquée pour devenir une arme : il suffit qu'elle survienne dans un environnement où la surveillance, l'expertise et le contrôle du récit sont distribués de manière inégale. Comprendre cette logique, c'est cesser de courir après des coupables pour commencer à réduire des vulnérabilités.

I. CADRE CONCEPTUEL ET DÉMARCHE MÉTHODOLOGIQUE

I. 1. Définir l'infrastructure critique

On désigne par infrastructure critique l'ensemble des systèmes, réseaux et installations dont la défaillance produirait un effet débilitant sur la sécurité, l'économie, la santé publique ou le fonctionnement même de l'État. La littérature internationale et les doctrines nationales convergent vers une liste de secteurs universellement reconnus comme vitaux.

Elle inclut l'énergie (barrages, lignes à haute tension, postes de transformation), les télécommunications (câbles, centres de données, réseaux mobiles), les transports (ports, voies ferrées, routes, aéroports), l'eau et l'assainissement, la santé (hôpitaux, chaîne du froid, laboratoires), la finance (systèmes de paiement, banque, monnaie mobile) et l'alimentation (chaînes agroalimentaires). Ces sept domaines ne forment pas une nomenclature administrative neutre : ils dessinent la carte des points où la vie collective peut être interrompue. Toute défaillance dans un seul d'entre eux affecte directement et simultanément la sécurité, l'économie et la santé publique de la nation.

Il importe de souligner que la criticité d'une infrastructure ne tient pas à sa taille ou à son coût, mais à sa fonction dans l'écosystème social. Un poste électrique modeste, un point d'atterrissement de câble sous-marin ou un serveur d'autorité de certification peuvent concentrer une criticité disproportionnée par rapport à

leur emprise physique. C'est cette concentration fonctionnelle qui en fait des cibles privilégiées.

I. 2. La menace hybride : un cadre théorique

La notion de menace hybride désigne une stratégie unique qui combine, dans un même dessein, des moyens militaires conventionnels et des moyens non conventionnels. Son répertoire est large : cyberattaques, sabotage physique, campagnes de désinformation, coercition économique, instrumentalisation du droit (lawfare) et pressions diplomatiques. Ce qui en fait l'unité n'est pas l'addition de ces outils, mais leur orchestration au service d'un effet stratégique recherché en dessous du seuil qui déclencherait une riposte armée.

La caractéristique définitionnelle de la menace hybride est l'ambiguïté. L'agresseur opère dans la pénombre et exploite méthodiquement la difficulté d'attribution : « Ce n'était pas nous », « C'était un accident », « C'était un acteur privé ». En maintenant le doute, il impose des coûts à sa cible sans s'exposer à une réponse coalisée. C'est cette économie du déni — infliger un dommage tout en conservant la possibilité de le nier — qui constitue le cœur stratégique de l'approche hybride.

Le cadre conceptuel mobilisé ici s'appuie sur trois apports majeurs. Frank G. Hoffman (2007) a théorisé la « guerre hybride » comme la fusion, sur un même espace de bataille, de modes d'action ordinaires et particuliers, brouillant la distinction classique entre combattant et non-combattant, entre une période de guerre et de paix. Mikael Wigell (2019) a prolongé cette réflexion en décrivant l'« interférence hybride » comme une stratégie de coin (wedge strategy) visant à diviser les sociétés et les alliances de l'intérieur, en exploitant leurs vulnérabilités ouvertes.

Patrick J. Cullen et Erik Reichborn-Kjennerud (2017), enfin, ont proposé une grammaire opérationnelle de la guerre hybride en insistant sur la synchronisation d'instruments relevant de domaines distincts. De ces travaux, on retiendra un enseignement essentiel pour notre propos : la menace hybride ne se définit pas par la nature de ses outils, mais par la vulnérabilité qu'elle exploite. Elle est moins une doctrine d'agression qu'une économie de l'opportunité.

I. 3. Démarche méthodologique

La présente étude adopte une démarche qualitative et interprétative, adaptée à un objet, la conflictualité hybride, qui se prête mal à la quantification directe et dont une part de la logique réside précisément dans l'invisibilité. Trois instruments sont combinés. Le premier est une revue de la littérature stratégique et des

doctrines de protection des infrastructures, destinée à stabiliser les concepts. Le deuxième est une analyse de cas comparée : une sélection raisonnée d'incidents internationaux de référence, retenus pour leur valeur illustrative et leur documentation publique, permet de dégager des régularités et de mesurer la diffusion des modes d'action. Le troisième est une matrice analytique à sept dimensions, adaptée d'un cadre récent et appliquée à la région des Grands Lacs, qui sert de grille de lecture systématique pour décomposer une menace composite en ses vecteurs constitutifs.

L'étude de cas centrale, la séquence d'événements de mai 2026 autour de l'épidémie d'Ebola Bundibugyo, relève de la méthode du cas paradigmatique : une étude n'est pas retenue parce qu'elle serait représentative au sens statistique, mais parce qu'elle rend visible, sous une forme condensée, une logique générale autrement diffuse. Les sources mobilisées sont de nature documentaire : publications académiques, rapports d'organisations internationales et techniques, déclarations officielles et chronologies publiques. Trois limites doivent être assumées d'emblée.

D'une part, l'attribution des actions hybrides demeure, par construction, incertaine ; l'analyse se garde donc d'affirmer des intentions qu'elle ne peut prouver et raisonne en termes de capacités, d'opportunités et d'effets. D'autre part, la proximité temporelle de certains événements en limite le recul critique ; ils sont traités comme des indices convergents plutôt que comme des preuves définitives. Enfin, la concomitance d'événements n'équivaut pas à une coordination : la « compression temporelle » examinée plus loin est proposée comme cadre d'interprétation heuristique, et non comme démonstration d'un dessein concerté.

II. L'ANATOMIE DE LA VULNÉRABILITÉ ET LA JURISPRUDENCE DES INCIDENTS

II. 1. Deux principes qui fragilisent tout le système

Deux propriétés systémiques expliquent pourquoi des sociétés techniquement avancées peuvent être mises à genoux par des moyens limités. La première est l'effet de cascade. Les infrastructures critiques ne sont pas des silos indépendants : elles forment un réseau d'interdépendances serrées. L'électricité alimente les télécommunications ; celles-ci conditionnent le fonctionnement des banques ; les banques irriguent l'approvisionnement et la logistique. Une attaque sur un seul point peut donc déclencher une réaction en chaîne qui se propage à l'ensemble. L'agresseur n'a pas besoin de frapper partout : il lui suffit d'identifier le maillon dont la rupture entraîne tous les autres.

La seconde propriété est la convergence des technologies de l'information et des technologies opérationnelles (IT/OT). Autrefois isolées et pilotées par des leviers mécaniques, les technologies opérationnelles — celles qui commandent les barrages, les postes électriques, les stations de pompage — sont désormais connectées aux réseaux informatiques pour des raisons d'efficacité et de télégestion. Cette intégration a un revers : on peut aujourd'hui saboter une centrale depuis un clavier, à distance, sans jamais s'approcher physiquement de l'installation. La frontière entre le monde numérique et le monde physique, qui protégeait jadis les infrastructures lourdes, s'est effacée.

Les chiffres traduisent l'ampleur du phénomène : une large majorité d'organisations d'infrastructures critiques déclarent une hausse des cyberattaques. La panne ibérique d'avril 2025, qui a plongé l'Espagne et le Portugal dans le noir en quelques secondes, a illustré de manière spectaculaire — quelle qu'en soit la cause technique exacte — la fragilité systémique des sociétés hyperconnectées. Lorsque l'électricité tombe, tout le reste suit, des paiements aux transports en passant par les communications.

II. 2. Pourquoi l'infrastructure est la cible idéale

Si les infrastructures critiques sont devenues le terrain de prédilection de la conflictualité contemporaine, c'est qu'elles réunissent une combinaison de propriétés qui en font une cible quasi parfaite. Elles sont coûteuses à protéger : chaque kilomètre de câble, chaque poste de transformation, chaque hôpital constitue une surface d'exposition qu'il faudrait défendre en permanence. Elles sont faciles à perturber : un point de défaillance unique suffit souvent à interrompre un service. Elles sont indispensables au quotidien, pour que leur atteinte se ressente immédiatement par toute la population et produise un effet politique disproportionné. Elles sont enfin difficiles à attribuer : il est toujours possible d'invoquer l'accident, l'acteur privé ou la simple défaillance technique.

Cette équation explique la rationalité de l'agresseur. Frapper une infrastructure, c'est frapper la nation entière sans tirer un coup de feu. Ces attaques sont rentables, un investissement modeste produit un effet majeur, discrètes et difficiles à attribuer. Réunies, ces trois qualités forment un incitatif puissant : voilà pourquoi de telles attaques se multiplient, et pourquoi elles continueront de le faire tant que le rapport entre le coût de l'agression et celui de la protection restera aussi favorable à l'assaillant.

II. 3. Cartographier la menace : les sept dimensions

Pour analyser une menace hybride sans la réduire à l'un de ses vecteurs, il est utile de la décomposer selon une matrice à sept dimensions, adaptée d'un cadre récent et appliquée ici à la région des Grands Lacs. La dimension sanitaire renvoie aux épidémies et à la perturbation des services de santé. La dimension cyber recouvre les rançongiciels, les intrusions et le sabotage des systèmes de contrôle.

La dimension physique vise le sabotage matériel des câbles, pipelines, pylônes et voies ferrées. La dimension informationnelle concerne la désinformation, la diffusion de la panique et l'érosion de la confiance dans les institutions. La dimension économique englobe la coercition, l'entretien de la dépendance et l'augmentation de la prime de risque-pays. La dimension sécuritaire mobilise des groupes armés par procuration et des stratégies de déni d'accès. La dimension biosécuritaire, enfin, recouvre l'extraction d'expertise et de valeur biomédicale au détriment du pays touché.

L'intérêt de cette grille n'est pas taxinomique mais opérationnel : elle permet de reconnaître qu'une même séquence d'événements peut simultanément activer plusieurs dimensions, et que c'est leur convergence, et non chacune prise isolément, qui produit l'effet stratégique. Elle servira de fil conducteur à l'analyse du cas Bundibugyo. Sa leçon générale tient en une formule : frapper l'infrastructure, c'est frapper la nation entière, sans tirer un coup de feu.

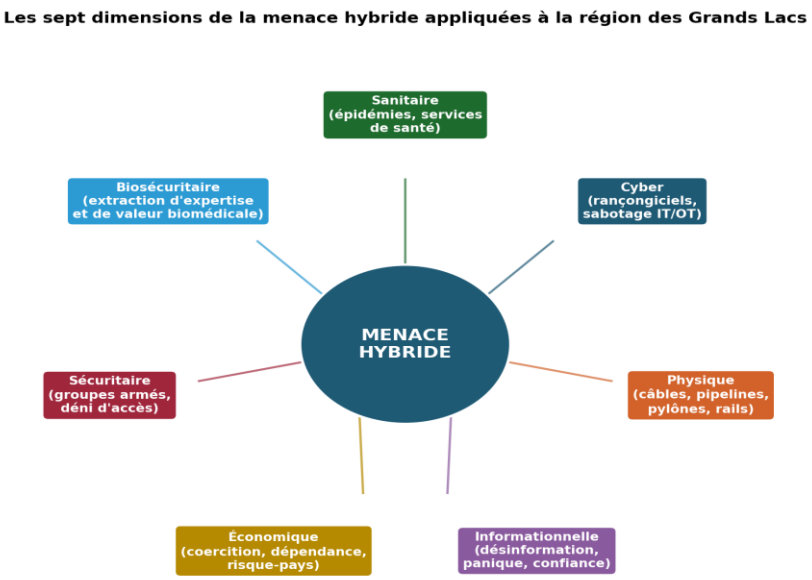

Fig. 1 — Les sept dimensions de la menace hybride appliquées à la région des Grands Lacs (élaboration de l'auteur).

II. 4. Une jurisprudence mondiale des incidents

La diffusion des modes d'action hybrides n'est plus une hypothèse : elle est documentée par une série d'incidents devenus des références mondiales. En 2010, le ver informatique Stuxnet a saboté physiquement les centrifugeuses du programme nucléaire iranien : pour la première fois, une arme numérique produisait des destructions matérielles, et la frontière entre le cyber et le physique disparaissait.

En 2015 et 2016, des cyberattaques ont coupé l'électricité à des centaines de milliers de foyers ukrainiens en plein hiver, première mondiale d'une coupure de réseau électrique provoquée à distance. En 2021, le rançongiciel qui a paralysé le Colonial Pipeline, principal oléoduc de la côte est des États-Unis, a provoqué des pénuries de carburant et la déclaration de l'état d'urgence. Cet évènement a démontré qu'une attaque sur un système de gestion pouvait suffire à arrêter une artère énergétique.

La séquence s'est ensuite déplacée vers les infrastructures sous-marines et les nœuds logistiques. En 2022, le sabotage des gazoducs Nord Stream en mer Baltique a conduit l'OTAN et l'Union européenne à mettre sur pied une task force

dédiée. En 2024 et début 2025, plusieurs câbles ont été sectionnés en Baltique et autour de Taïwan par des navires « civils » au comportement suspect, amenant l'OTAN à lancer, le 14 janvier 2025, la mission Baltic Sentry de protection des infrastructures sous-marines. En avril 2025, l'effondrement quasi instantané du réseau électrique ibérique a rappelé que l'électricité conditionne tout le reste.

L'année 2025 a confirmé que le secteur des transports aériens — nœud par excellence de la mobilité, du commerce et de la confiance — était devenu une cible de premier plan. À la fin de septembre 2025, une cyberattaque par rançongiciel a visé la société Collins Aerospace et, à travers elle, la plateforme MUSE (Multi-User System Environment) qui gère l'enregistrement et l'embarquement des passagers dans de nombreux aéroports. Les conséquences ont été immédiates et spectaculaires : à Londres-Heathrow, Bruxelles et Berlin, les systèmes d'enregistrement et de traitement des bagages sont tombés, contraignant le personnel à revenir aux procédures manuelles, ordinateurs portables, tablettes et cartes d'embarquement papier.

À Bruxelles, une partie significative des vols au départ a dû être annulée, et les perturbations se sont prolongées plusieurs jours. L'Agence de l'Union européenne pour la cybersécurité (ENISA) a confirmé qu'il s'agissait d'une attaque par rançongiciel. L'épisode illustre une vulnérabilité structurelle. En effet, la dépendance d'un grand nombre d'aéroports à l'égard d'un même fournisseur de services crée un point de défaillance unique dont la compromission se propage instantanément, par effet de cascade, à des dizaines de hubs simultanément.

À cette agression numérique s'est ajoutée, à l'automne 2025, une vague d'incursions de drones au-dessus d'aéroports européens, qui a matérialisé la dimension physique et psychologique de la menace hybride. Le 22 septembre 2025, des survols de drones ont entraîné la suspension du trafic à l'aéroport de Copenhague pendant environ quatre heures, provoquant de nombreuses annulations et déroutements, tandis que des perturbations affectaient simultanément l'aéroport d'Oslo.

Début octobre 2025, l'aéroport de Munich a dû interrompre ses opérations à deux reprises en moins de vingt-quatre heures à la suite de signalements de drones près de ses pistes. Plusieurs dirigeants européens ont publiquement évoqué une possible implication russe, la Première ministre danoise déclarant qu'une telle implication « ne pouvait être exclue », Moscou démentant pour sa part toute responsabilité. Les autorités danoises ont qualifié ces activités d'opération vraisemblablement hybride, destinée à inquiéter la population et à perturber des

infrastructures critiques. Il convient toutefois de noter qu'à ce jour aucune de ces incursions n'a fait l'objet d'une attribution judiciairement établie.

L'enseignement de cette double séquence aérienne de 2025 dépasse le cas européen. Elle démontre, d'une part, qu'une perturbation majeure peut être obtenue sans destruction, il a suffi de la simple présence de drones, ou de la compromission d'un logiciel d'enregistrement, pour figer des hubs entiers ; et, d'autre part, que l'ambiguïté demeure le ressort central, puisque ni les drones ni le rançongiciel n'ont été en mesure d'être attribués avec une certitude juridique suffisante pour déclencher une riposte coalisée. C'est exactement la grammaire hybride à l'œuvre : un effet maximal, un coût minimal, une attribution impossible.

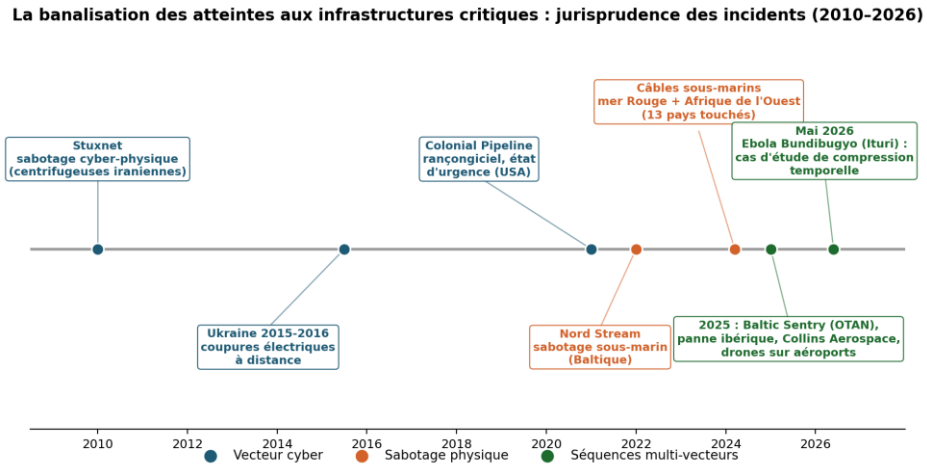

Fig. 2 — La banalisation des atteintes aux infrastructures critiques : chronologie des incidents de référence, 2010–2026 (élaboration à partir des sources citées).

II. 5. Notre réalité : l'exposition de l'Afrique et de la RDC

Ces dynamiques cessent d'être abstraites dès lors qu'on les rapporte à l'architecture numérique du continent africain. La très grande majorité des flux de données intercontinentaux transitent par les câbles sous-marins ; la connectivité de l'Afrique repose donc sur un petit nombre d'artères physiques dont la rupture a des effets immédiats et massifs. Le 14 mars 2024, la rupture quasi simultanée de quatre câbles majeurs, WACS, ACE, SAT-3 et MainOne, a coupé ou dégradé l'accès à Internet dans treize pays africains, la Côte d'Ivoire se retrouvant quasi totalement à l'arrêt. Quelques semaines plus tôt, début 2024, en mer Rouge, l'ancre d'un navire endommagé dans le contexte des attaques houthies avait sectionné les

câbles Seacom, AAE-1 et EIG, perturbant la connectivité entre l'Afrique de l'Est et l'Asie. (Ces ruptures ont été majoritairement attribuées à des causes accidentelles ou environnementales ; elles sont mobilisées ici comme démonstration de vulnérabilité systémique, non comme preuve de sabotage.)

La RDC n'est pas un spectateur extérieur de ces phénomènes. Selon les informations publiques disponibles, une intrusion détectée dans les réseaux de la Société congolaise des postes et télécommunications (SCPT) a déjà créé des procédures : la menace cyber a touché le sol national. Cette exposition est aggravée par la faible redondance des points d'entrée internet, la concentration des dépendances et l'absence, à ce stade, d'un cadre juridique et institutionnel dédié à la protection des installations vitales. Autrement dit, la RDC réunit aujourd'hui les conditions de vulnérabilité que les incidents internationaux ont précisément appris à exploiter.

II. 6. Le cas paradigmatique : Ebola Bundibugyo, mai 2026

Avertissement méthodologique. La séquence reconstituée ci-dessous est établie à partir de déclarations officielles et de chronologies publiques disponibles au moment de la rédaction. Les dates et faits précis demeurent sujets à confirmation par les sources primaires (communiqués de l'OMS, du ministère de la Santé de la RDC et des autorités concernées). L'analyse qui en est tirée a une valeur heuristique : elle propose une lecture, non une preuve d'intentionnalité.

C'est sur ce terrain de vulnérabilité que prend tout son sens la séquence d'événements observée en mai 2026 autour de l'épidémie d'Ebola Bundibugyo (BDBV) en Ituri. Plusieurs événements se sont enchaînés en l'espace de quelques jours, et cette compression temporelle offre, à titre d'illustration et non de démonstration, une lecture en temps réel de ce que peut être une menace hybride à sept dimensions.

Autour du 15 mai, la RDC et l'Ouganda confirment l'épidémie de virus Ebola Bundibugyo en Ituri. Le lendemain, l'Organisation mondiale de la santé déclare l'urgence de santé publique de portée internationale. Dans les jours qui suivent, les États-Unis instaurent une restriction d'entrée temporaire visant les voyageurs en provenance de la RDC, de l'Ouganda et du Soudan du Sud. À la même période, à Kigali, les États-Unis et le Rwanda signent un mémorandum d'entente sur le nucléaire civil, assorti d'un projet portant sur des réacteurs modulaires compacts (SMR). Un vol commercial est par ailleurs dérouté et un médecin américain est évacué vers l'Allemagne. La létalité estimée du BDBV se situe, selon les données épidémiologiques disponibles, dans une fourchette élevée : la dimension sanitaire est donc bien réelle, et tragique.

Comment une crise sanitaire authentique peut-elle se muer en avantage stratégique pour des tiers ? Le mécanisme proposé ici, à titre d'hypothèse, repose sur trois engrenages. Le premier est une réduction de l'attention et de la vérification indépendantes : une restriction des vols et des déplacements diminue la présence physique d'observateurs extérieurs, journalistes, personnels humanitaires, rotations internationales, et concentre l'attention institutionnelle sur l'urgence sanitaire, au détriment d'autres dynamiques régionales. (Précisons que cette opacité est partielle et porte sur la présence humaine et l'attention médiatique : l'observation satellitaire, qui ne dépend pas du trafic aérien civil, demeure quant à elle disponible.). Le deuxième engrenage est l'exploitation éventuelle de ce déficit d'attention : pendant une telle période, des groupes armés actifs dans l'Est pourraient consolider leurs positions avec une moindre publicité internationale. Le troisième engrenage est une asymétrie de souveraineté : le médecin américain est exfiltré vers un site à haut niveau de confinement, tandis que les populations locales d'Ituri demeurent sans accès à des capacités équivalentes. À ces engrenages s'ajoute un récit international, résumé par le raccourci « Rwanda = modernité, RDC = risque », dont chaque fragment, pris isolément, peut être factuel, mais dont l'assemblage compose un cadre interprétatif orienté.

Le point cardinal de l'analyse doit ici être énoncé sans ambiguïté : aucune fabrication n'est alléguée, et la coordination est non prouvée. Rien ne permet de suggérer que l'épidémie aurait été conçue ou manipulée ; il s'agit d'une épidémie naturelle, réelle et mortelle. De même, la concomitance des décisions diplomatiques et sécuritaires évoquées ne saurait être tenue, en l'état des sources, pour la preuve d'un dessein concerté. C'est précisément ce qui rend le cas instructif. La menace ne naît pas du virus, mais de la rencontre possible entre une épidémie naturelle et des asymétries préexistantes, de surveillance, d'expertise, de narratif et de dépendance.

De cette rencontre peut résulter un multiplicateur stratégique au bénéfice de l'acteur le plus doté. Un État qui maîtriserait sa biosécurité, ses hôpitaux, ses capacités diagnostiques, son autorité épidémiologique, verrait son épidémie beaucoup moins susceptible de se transformer en arène stratégique pour d'autres. La vulnérabilité, et non nécessairement la malveillance, demeure la variable explicative la plus robuste.

II. 7. Une grammaire commune : ce que les cas enseignent ensemble

Replacés les uns à côté des autres, ces incidents ne forment pas une panoplie d'anecdotes alarmantes ; ils révèlent une grammaire commune. Première régularité : la cible n'est presque jamais l'armée, mais le service. De l'électricité

ukrainienne au carburant américain, des bagages européens à la connectivité ouest-africaine, ce que l'on vise est toujours la prestation quotidienne dont dépend la vie ordinaire, car c'est là que le dommage devient politiquement insupportable et immédiatement perceptible par tous. Deuxième régularité : l'effet recherché est psychologique autant que matériel. Couper un service, c'est ébranler la confiance des citoyens dans la capacité de l'État à les protéger, et cette érosion de confiance est un gain stratégique en soi, qui survit longtemps à la réparation technique de la panne. Troisième régularité : l'attribution est systématiquement diluée, qu'il s'agisse de navires « civils », d'acteurs criminels agissant à des fins apparemment lucratives, ou de drones sans pavillon.

De ces régularités découle un renversement méthodologique décisif. Tant que l'on raisonne en termes d'agresseur, on reste paralysé par l'exigence de preuve : il faut établir qui, et avec quelle intention, avant d'agir. Mais, si l'on raisonne en termes de vulnérabilité, l'action redevient possible immédiatement, car réduire un point de défaillance unique protège la nation indépendamment de l'identité de celui qui aurait pu l'exploiter. C'est pourquoi la posture défendue dans cet article n'est pas accusatoire mais préventive : elle déplace la question de « qui nous attaque ? » vers « où sommes-nous exposés ? ». Cette dernière question, à la différence de la première, admet des réponses et appelle des actes.

III. DISCUSSION : DE L'EXPLOITATION DES CRISES AUX ENJEUX DE SOUVERAINETÉ

III. 1. Ce que révèle Bundibugyo

Le cas Bundibugyo confirme et précise la thèse avancée en introduction — à condition de la maintenir au rang d'hypothèse interprétative. Il suggère d'abord que la frontière entre crise naturelle et conflit stratégique est poreuse : il n'est pas nécessaire qu'un adversaire crée l'événement déclencheur pour qu'il en tire un avantage. La distinction classique entre l'accidentel et l'intentionnel, sur laquelle repose une part substantielle du droit international et des doctrines de défense, se trouve ainsi mise en tension. En effet, l'exploitation d'une crise peut produire des effets comparables à ceux d'une agression sans en présenter les signatures attribuables.

Il rappelle ensuite que la dimension biosécuritaire mérite d'être pleinement intégrée à la réflexion sur les infrastructures critiques. La santé n'est qu'un secteur vital parmi d'autres ; la capacité d'un État à diagnostiquer, à confiner et à raconter ses propres crises sanitaires constitue une infrastructure souveraine à part entière. Lorsque l'expertise, les échantillons biologiques et l'autorité épidémiologique

migrent systématiquement vers l'extérieur, c'est une forme de dépendance structurelle qui s'installe et qui peut, en situation de crise, se convertir en levier stratégique.

Il souligne enfin le rôle décisif de la dimension informationnelle. Un récit n'a pas besoin d'être mensonger pour être stratégique : il suffit qu'il sélectionne et agence des faits exacts pour produire une hiérarchie implicite entre les nations. La lutte pour la résilience est donc aussi une lutte pour la maîtrise du récit que l'on tient sur soi-même.

Cette triple leçon invite enfin à élargir la notion même de défense. Pendant des siècles, défendre une nation a signifié protéger ses frontières et concentrer ses forces face à une armée adverse. La conflictualité hybride exige d'y ajouter une logique de profondeur. La sécurité ne se joue plus seulement à la frontière, mais en chaque point où un service vital peut être interrompu : un centre de données à Kinshasa, un point d'atterrissement de câble sur la côte atlantique, un laboratoire en Ituri. Défendre devient alors un acte distribué, qui mobilise autant l'ingénieur réseau et l'épidémiologiste que le soldat. C'est un changement de culture : stratégique avant d'être un changement d'équipement.

III. 2. Le partenariat USA-RDC : trois enjeux articulés

C'est à la lumière de cette analyse que doivent être appréciés les enjeux du partenariat stratégique conclu entre la RDC et les États-Unis, qui consacre explicitement la protection des infrastructures critiques. Trois enjeux y sont étroitement liés et méritent d'être pensés ensemble plutôt que séparément.

Le premier est celui du corridor. L'axe Sakania–Lobito, destiné à acheminer vers l'Atlantique les ressources et la valeur ajoutée congolaises, constitue tout à la fois la colonne vertébrale de l'ambition économique nationale et son talon d'Achille. Le sécuriser ne se limite pas à protéger une voie ferrée : il s'agit de le défendre physiquement, numériquement et juridiquement, car de sa robustesse dépend toute la stratégie d'exportation de produits transformés plutôt que de matières brutes. Les enjeux sociaux du corridor, notamment les risques de déplacement de populations documentés par la société civile, font partie intégrante de cette robustesse : une infrastructure contestée localement n'est jamais pleinement résiliente.

Le deuxième enjeu est énergétique. Il n'y a pas d'industrialisation sans montée en puissance énergétique, qu'il s'agisse du potentiel d'Inga, de Ruzizi III ou d'un mix renouvelable diversifié. Mais cette infrastructure énergétique doit être conçue résiliente et cybersécurisée dès l'origine, et non équipée de protections

ajoutées tardivement. La sécurité ne se greffe pas après coup sur un système conçu sans elle ; elle s'inscrit dans l'architecture initiale ou elle demeure illusoire.

Le troisième enjeu, le plus déterminant, est celui de la souveraineté. Tout partenariat asymétrique porte un risque : que les capacités critiques, données, expertise, contrôle, demeurent à l'extérieur du pays, faisant de la RDC un terrain d'opération plutôt qu'un acteur autonome. Le critère d'évaluation d'un partenariat efficace est dès lors simple : un partenariat réussi rapatrie les capacités, il ne les externalise pas. La coopération est souhaitable et nécessaire ; encore faut-il qu'elle construise de l'autonomie congolaise au lieu d'entretenir la dépendance.

III. 3. Portée et limites de l'analyse

La portée de cette analyse doit être mesurée avec rigueur. L'incertitude d'attribution, inhérente à la conflictualité hybride, interdit d'affirmer des intentions hostiles là où l'on ne peut établir que des opportunités et des effets. Le propos n'est pas de désigner des coupables, mais de cartographier des vulnérabilités. C'est d'ailleurs la force opérationnelle de cette posture : alors qu'une politique fondée sur l'attribution reste suspendue à des preuves souvent inaccessibles, une politique fondée sur la réduction des vulnérabilités peut être engagée immédiatement et produit des bénéfices quelle que soit l'origine de la menace. Réduire sa surface d'exposition protège aussi bien contre l'accident que contre l'agression. C'est sur cette logique que repose le cadre de résilience proposé.

IV. VERS UN CADRE NATIONAL DE RÉSILIENCE

Que faire ? La réponse ne saurait se limiter à une liste de mesures techniques : elle suppose une stratégie nationale cohérente, ordonnée du plus rapide au plus structurant, et portée au plus haut niveau de l'État. Cinq axes en constituent l'ossature.

Cartographier et classer. On ne protège que ce que l'on a identifié. La première marche consiste à adopter une loi sur les infrastructures critiques, instituant un inventaire national et une classification des installations vitales selon leur criticité. Cet acte fondateur, à la fois juridique et cognitif, conditionne tout le reste : sans recensement officiel des points névralgiques, aucune politique de protection ne peut être ni ciblée ni évaluée.

Doter l'État d'un bouclier numérique. Il s'agit de créer ou de renforcer une agence nationale de cybersécurité et une équipe nationale de réponse aux incidents informatiques (CERT), dotées d'une capacité de détection en continu et d'une coordination interministérielle effective. Face à des attaques qui se jouent en

quelques secondes et traversent les frontières administratives, la résilience exige une vigilance permanente et une chaîne de décision capable de réagir sans délai.

Diversifier et créer de la redondance. Le principe directeur est l'élimination des points de défaillance uniques. Cela suppose de multiplier les points d'entrée internet en combinant câbles sous-marins, liaisons satellitaires et connexions terrestres, d'interconnecter le réseau national et d'exiger des opérateurs de véritables plans de continuité d'activité. La redondance a un coût ; mais ce coût est sans commune mesure avec celui d'une paralysie nationale.

Mutualiser à l'échelle régionale. Aucune nation ne sécurise seule des câbles partagés et des bassins fluviaux communs. Il convient de s'inspirer des dynamiques continentales, à l'image d'Africa CDC dans le champ sanitaire et des appels à une protection régionale des câbles, et de mobiliser les cadres d'intégration existants, de la Communauté économique des pays des Grands Lacs (CEPGL) à la Communauté de développement d'Afrique australe (SADC) et à l'Union africaine. La résilience régionale est un bien commun qui se construit collectivement ou ne se construit pas.

Bâtir la souveraineté technologique. L'axe le plus structurant consiste à lier tout transfert de technologie à la formation d'ingénieurs et d'experts en cybersécurité congolais, ainsi qu'au cofinancement de capacités locales, centres de données souverains, capacités nationales de maintenance des câbles, filières de compétences. C'est la traduction concrète du principe énoncé plus haut : un partenariat doit rapatrier les capacités. La souveraineté technologique n'est pas un slogan ; elle est la condition pour que la RDC cesse d'être l'objet des stratégies d'autrui et en devienne le sujet.

Ces cinq axes ne sont pas des mesures isolées mais les composantes d'un même système : la cartographie oriente le bouclier numérique, la redondance protège les actifs cartographiés, la mutualisation régionale démultiplie les capacités nationales, et la souveraineté technologique garantit la pérennité de l'ensemble. Leur valeur tient à leur cohérence.

CONCLUSION

Le cas Bundibugyo n'est pas une anomalie : c'est une photographie de la menace hybride du XXIe siècle. Une crise sanitaire authentique, couplée à des décisions diplomatiques et à des vides d'attention, a pu s'offrir comme fenêtre stratégique. Aucun combat n'a été livré pour cela ; aucun système n'a eu besoin d'être piraté. La nature a fourni le virus ; les asymétries préexistantes ont pu faire le reste. C'est là tout l'enseignement de cet article : la sécurité d'une nation ne se

mesure plus seulement à la force de ses armées, mais à la résilience de ses infrastructures et à la maîtrise de ses propres vulnérabilités.

Des centrifugeuses iraniennes de 2010 aux aéroports européens de 2025, des câbles de la Baltique à ceux des côtes africaines, une même logique se déploie : infliger un dommage maximal pour un coût minimal, sous le couvert d'une attribution impossible. La RDC n'échappe pas à cette logique ; elle en réunit même, par sa géographie stratégique et la fragilité de ses réseaux, plusieurs conditions d'application. Mais la vulnérabilité n'est pas une fatalité : elle est une variable sur laquelle un État peut agir.

Il appartient désormais à la RDC de choisir : rester dans un régime d'exploitation asymétrique de ses crises, ou devenir l'architecte de sa propre résilience. Ce choix n'est pas seulement technique ou budgétaire ; il est éminemment politique, car il engage l'idée même que la nation se fait de sa souveraineté. Protéger ses infrastructures, en définitive, c'est exercer sa souveraineté.

RÉFÉRENCES BIBLIOGRAPHIQUES

- ANDERSON, W. (2014). Making global health history: The postcolonial worldliness of biomedicine. *Social History of Medicine, 27*(2), 372–384. *https://doi.org/10.1093/shm/hkt126*.
- CULLEN, P. J., et REICHBORN-KJENNERUD, E. (2017). *Understanding hybrid warfare* [Note d'information]. Multinational Capability Development Campaign. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/717539/MCDC_CHW_Information_Note-Understanding_Hybrid_Warfare-Jan_2018.pdf*.
- HOFFMAN, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. *https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf*.
- MUKUNA MUYA, D.-S. (2025a). Conflits armés dans l'est de la RD Congo : Analyse stratégique des dynamiques régionales autour de l'activisme du M23/AFC et de l'armée rwandaise. *Revue Intelligence Stratégique, 8*(20), 55–70. *https://doi.org/10.62912/JYJX7512*.
- MUKUNA MUYA, D.-S. (2025b). Guerre hybride et anticipation stratégique en Afrique centrale : Approches multidimensionnelles de la résilience face aux menaces émergentes. *Revue Intelligence Stratégique, 8*(21), 79–131. *https://doi.org/10.62912/ROEI5393*.

- MUKUNA MUYA, D.-S. (2026). *Guerre hybride et souveraineté stratégique en Afrique centrale : Résilience systémique et riposte adaptative aux nouvelles conflictualités*. L'Harmattan.
- WIGELL, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs, 95*(2), 255–275. *https://doi.org/10.1093/ia/iiz018*.
- GLOBAL WITNESS. (2025, 4 décembre). *Thousands in DRC could face eviction from Lobito Corridor railway*. *https://globalwitness.org/en/campaigns/transition-minerals/thousands-in-drc-could-face-eviction-from-lobito-corridor-railway/*.
- INDUSTRIAL CYBER. (2025, 22 septembre). *ENISA confirms ransomware behind airport disruptions: Delays at Heathrow, Brussels and Berlin continue*. *https://industrialcyber.co/threats-attacks/enisa-confirms-ransomware-behind-airport-disruptions-delays-at-heathrow-brussels-berlin-continue/*.
- INTERNET SOCIETY. (2024). *2024 West Africa submarine cable outage report*. *https://www.internetsociety.org/resources/doc/2024/2024-west-africa-submarine-cable-outage-report/*.
- ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD, ALLIED MARITIME COMMAND. (2025, 14 janvier). *NATO's Baltic Sentry steps up patrols in the Baltic Sea to safeguard critical undersea infrastructure*. *https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure*.
- ORGANISATION MONDIALE DE LA SANTÉ. (2026, 17 juillet). *Ebola disease caused by Bundibugyo virus, Democratic Republic of the Congo and Uganda* [Disease outbreak news, DON613]. *https://www.who.int/emergencies/disease-outbreak-news/item/2026-DON613*.
- REUTERS. (2025, 22 septembre). *Drone sightings disrupt flights at Copenhagen and Oslo airports*. *https://www.reuters.com/business/aerospace-defense/copenhagen-airport-halts-traffic-due-drone-sightings-police-says-2025-09-22/*.
- REUTERS. (2025, 24 septembre). *Drones and systems hack test Europe's aviation security defences*. *https://www.reuters.com/business/aerospace-defense/drones-systems-hack-test-europes-aviation-security-defences-2025-09-24/*.
- REUTERS. (2025, 4 octobre). *Munich Airport to resume flight operations after drones in airspace caused delays*. *https://www.reuters.com/business/aerospace-defense/drone-sightings-delay-saturday-flight-operations-munich-airport-2025-10-04/*.