INSTITUT DE RECHERCHE EN GEOPOLITIQUE ET D'ETUDES STRATEGIQUES

Revue

Intelligence Stratégique

Vol. 008, Numéro 021, Avril-Juin 2025
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 82 006 1696 ; 81 86 19 121; 89 7175 074
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 8, numéro 21
Avril-Juin 2025
p-ISSN : 3006-547X ; e-ISSN : 3006-5488
https://doi.org/10.62912/ROEI5393
www.revue-is.org

GUERRE HYBRIDE ET ANTICIPATION STRATEGIQUE EN AFRIQUE CENTRALE : APPROCHES MULTIDIMENSIONNELLES DE LA RESILIENCE FACE AUX MENACES EMERGENTES

Donat-Soft MUKUNA MUYA
Docteur en médecine et Doctorant en stratégie, sécurité et défense au Collège des Hautes Études de Stratégie et de Défense (CHESD)/Kinshasa-RDC

RESUME

Cet article scientifique explore la nature et les dynamiques contemporaines de la guerre hybride, avec un accent particulier sur l'Afrique centrale, notamment la République démocratique du Congo (RDC). Elle analyse les formes que prend cette guerre dans les domaines militaire, numérique, informationnel et idéologique. En s'appuyant sur une approche prospective, le document présente des scénarios stratégiques pour les États confrontés à l'ingérence de sociétés militaires privées (SMP), à la montée du djihadisme et aux vulnérabilités systémiques. Il propose des mesures concrètes de résilience étatique, de veille stratégique et de gouvernance anticipative, tant au niveau des institutions publiques que du secteur privé extractif. La note intègre également un plan de résilience sanitaire post-pandémie sévère (cas du Covid-19) et une matrice d'évaluation des risques. Elle appelle enfin à une réforme des systèmes de sécurité, à une coopération inter-agences et à l'internalisation de la culture de l'anticipation stratégique.

Mots-clés : *guerre hybride, Afrique centrale, anticipation stratégique, menaces émergentes RDC.*

ABSTRACT

This scientific paper explores the nature and contemporary dynamics of hybrid warfare, with a particular focus on Central Africa, especially the Democratic Republic of Congo (DRC). It analyzes the forms this war takes in the military, digital, informational and ideological domains. Using a forward-looking approach, the document presents strategic scenarios for states faced with the interference of

private military companies (PMCs), the rise of jihadism and systemic vulnerabilities. It proposes concrete measures for state resilience, strategic intelligence and anticipatory governance, both at the level of public institutions and the extractive private sector. The note also includes a severe post-pandemic health resilience plan (case of Covid-19) and a risk assessment matrix. Finally, it calls for a reform of security systems, inter-agency cooperation and the internalization of a culture of strategic anticipation.

Keywords : hybrid warfare, Central Africa, strategic anticipation, emerging threats DRC.

INTRODUCTION

Au cours des dernières décennies, l'art de la guerre a considérablement évolué avec l'émergence de menaces dites « hybrides ». Celles-ci combinent des modes d'action conventionnels et non conventionnels, brouillant la distinction entre temps de paix et conflit ouvert. Dans le contexte africain, et en particulier en Afrique centrale, ces menaces hybrides se manifestent de plus en plus fréquemment. Des puissances étrangères recourent à des sociétés militaires privées (SMP) pour projeter leur influence de manière déniable; d'autres soutiennent en sous-main des rébellions locales pour déstabiliser leurs voisins (ainsi le M23 en RDC bénéficie d'appuis extérieurs), tandis que des groupes djihadistes exploitent les fragilités locales pour étendre leur emprise. Parallèlement, la désinformation numérique attise les tensions communautaires existantes. Les États d'Afrique centrale se retrouvent ainsi confrontés à des ingérences multiformes qui défient les approches de défense classiques. Comme l'affirme l'Union africaine, l'analyse des conflits modernes suppose « une compréhension systémique des dynamiques régionales[1] » afin de ne pas être pris de court par ces nouvelles menaces.

Comment les pays d'Afrique centrale peuvent-ils anticiper et contrer efficacement les stratégies de guerre hybride qui menacent leur stabilité ? Face à la complexité de ces menaces, mêlant acteurs étatiques et non étatiques, champ militaire et civil, dimension locale et internationale, une approche traditionnelle de sécurité semble insuffisante.

[1] MUSILA C., « L'insécurité transfrontalière au Cameroun et dans le bassin du lac Tchad », dans *Ifri*, 2012, p. 4.

L'hypothèse directrice de cette note est qu'une approche multidimensionnelle et anticipative de la résilience est nécessaire pour faire face aux guerres hybrides. En d'autres termes, seule l'internalisation d'une culture d'anticipation stratégique au sein des États, couplée à un renforcement global de la résilience (militaire, sociétale, numérique, sanitaire, etc.), permettrait de relever efficacement ce défi.

Cette étude vise d'abord à clarifier le concept de guerre hybride et à en dresser les caractéristiques essentielles, afin de bien cerner la nature du problème. Ensuite, elle examine comment la guerre hybride se manifeste concrètement dans différents secteurs (militaire, numérique, informationnel…). Sur cette base, l'étude se focalise sur les enjeux spécifiques à l'Afrique centrale, région où la présence de SMP, la radicalisation djihadiste et la faiblesse de certains Etats (à l'instar de la RDC) créent un terreau propice à de telles menaces.

A partir d'une méthode de prospective (anticipation stratégique), plusieurs scénarios d'évolution sont proposés pour illustrer les futurs possibles d'un État de la région confronté à ces défis. Enfin, la note formule des mesures de riposte stratégiques et met en avant des outils d'anticipation (cellule de veille, analyse de risques, plan de résilience post-pandémie), sans oublier d'aborder la contribution du secteur privé, en particulier des industries extractives, à cette dynamique d'anticipation.

La démarche est à la fois analytique et prospective. Elle s'appuie sur une revue de la littérature existante (ouvrages de stratégie, rapports d'organisations internationales, travaux académiques) ainsi que sur l'analyse de cas concrets récents (ingérence du groupe Wagner en Centrafrique, expansions djihadistes au Sahel, désinformation lors des opérations Barkhane, résurgence du mouvement M23 à l'est de la RDC, etc.). L'approche prospective se traduit par l'élaboration de scénarios à moyen terme, nourris par l'identification de signaux faibles et de tendances lourdes dans la région. Ces scénarios permettent d'explorer de manière systématique les différentes trajectoires possibles afin d'en déduire des options stratégiques de réponse. Par ailleurs, une matrice d'analyse de risques (impact/probabilité) et un ensemble d'indicateurs de résilience ont été développés pour hiérarchiser les menaces et mesurer la préparation des États face à ces menaces hybrides. L'ensemble de ces outils vise à offrir aux décideurs une grille de lecture proactive, afin de passer d'une posture réactive à une posture anticipative en matière de sécurité nationale.

Scientifiquement, ce travail enrichit le débat sur la guerre hybride en l'appliquant au contexte peu étudié de l'Afrique centrale, confrontant les théories globales aux réalités locales. Il met en lumière l'intersection entre études stratégiques, études sécuritaires africaines et études de prospective. D'un point de vue pratique, cette note se veut un outil d'aide à la décision pour les responsables politiques et les institutions de la région. Les recommandations formulées qu'il s'agisse de créer des cellules de veille, d'investir dans la cybersécurité ou d'encadrer les SMP sont destinées à orienter des actions concrètes. In fine, le propos est de montrer qu'une meilleure anticipation des menaces hybrides, doublée d'une amélioration de la résilience systémique, peut permettre aux États d'Afrique centrale de prévenir les crises au lieu de les subir, contribuant ainsi à la stabilité et au développement durable de la région.

I. CLARIFICATION ET CARACTERISTIQUES DE LA GUERRE HYBRIDE

La guerre hybride désigne un type de conflit qui combine simultanément des moyens conventionnels et non conventionnels. Autrement dit, elle mêle des opérations militaires classiques à des tactiques asymétriques (guérilla, terrorisme) et à la guerre de l'information et du cyberespace. Il n'existe pas de définition universellement acceptée du concept, mais on s'accorde à dire qu'une guerre hybride brouille la frontière entre guerre régulière et irrégulière, entre temps de paix et temps de conflit. L'adversaire exploite les vulnérabilités de sa cible en utilisant de façon synchronisée divers instruments de puissance (forces armées, milices, cyberattaques, propagande, coercition économique) pour atteindre des effets synergiques. Ce mode d'action indirect cherche à déstabiliser l'ennemi sans déclencher nécessairement une confrontation militaire ouverte, s'inscrivant ainsi dans une logique stratégique d'évitement frontal[2].

La guerre hybride se caractérise par la multiplicité d'acteurs, la combinaison de tactiques, un usage intensif de la propagande et de la désinformation, l'ambiguïté et le déni.

Sur la multiplicité d'acteurs, il sied de noter que l'agresseur hybride peut mêler des forces étatiques et non étatiques agissant de concert. Par exemple, une puissance peut nier son implication directe tout en soutenant discrètement des

[2] LUTTWAK E. N., *Strategy: The Logic of War and Peace,* Harvard University Press, 1990.

milices locales dans un conflit il s'agit alors d'une guerre par procuration masquant son action. L'acteur hybride profite ainsi de la dénégation plausible : il instrumentalise des tiers (groupes rebelles, SMP, hacktivistes) pour brouiller les pistes et diluer ses responsabilités.

La combinaison de tactiques fait allusion à l'emploi simultané de modes d'action conventionnels (chars, missiles, armée régulière) et irréguliers (attentats, insurrection), couplés à des opérations dans le cyberespace et l'informationnel. Par exemple, lors du conflit israélo-libanais de 2006, le Hezbollah acteur non étatique a utilisé à la fois des missiles antichars avancés, des drones de reconnaissance et des tactiques de guérilla classique, illustrant cette hybridation des moyens. De même, au Sahel de nos jours, des insurgés djihadistes combinent la guérilla terrestre à des campagnes de propagande en ligne, tout en bénéficiant de l'appui occulte de mercenaires étrangers.

L'usage intensif de la propagande et de la désinformation fait référence aux offensives hybrides incluent presque toujours un volet informationnel. L'adversaire mène de front une guerre cognitive visant à influencer les populations et à brouiller la perception de la réalité. Via les réseaux sociaux et les médias, il propage de fausses nouvelles (fake news), amplifie des discours polarisants et cherche à saper la confiance du public dans les institutions. Ce pilier informationnel, intégré à la manœuvre militaire, peut affaiblir la cohésion interne de l'ennemi avant même l'engagement physique.

Dans l'ambiguïté et le déni, l'agresseur hybride opère souvent dans la zone grise du droit international. Ses actions sont conçues pour créer une incertitude sur l'identité de l'attaquant. Des soldats sans insignes les fameux « petits hommes verts » apparus en Crimée en 2014 peuvent occuper un territoire tout en permettant à l'État qui les emploie de nier son implication directe. Cette ambiguïté complique énormément la réponse juridique et militaire : qui sanctionner ou combattre quand l'adversaire ne se déclare pas comme tel ?

En somme, la guerre hybride est une forme de conflictualité multi-dimensionnelle. Elle se déroule sur le champ de bataille classique, mais aussi parmi les populations civiles et dans l'arène globale de l'information. Comme le souligne l'OTAN, « la guerre hybride implique une fusion de moyens conventionnels et d'outils de subversion », l'objectif étant de porter des coups à l'adversaire sans

jamais franchir le seuil d'un conflit armé déclaré. On peut considérer que certains conflits récents illustrent bien ce modèle « sous le seuil » : en Ukraine en 2014, par exemple, l'intervention de forces spéciales russes non identifiables, couplée à une intense guerre de l'information, a montré la puissance de cette approche hybride. La stratégie indirecte prônée par Luttwak frapper l'ennemi de manière imprévue et diffuse trouve ici un terrain d'application privilégié[3].

En Afrique Centrale et de l'Ouest, plusieurs crises actuelles comportent également des dimensions hybrides : au Sahel, les Etats font face simultanément à des insurrections djihadistes, à la désinformation en ligne et à l'ingérence de mercenaires, ce qui met à l'épreuve leurs modèles de défense traditionnels.

II. MANIFESTATIONS SECTORIELLES DE LA GUERRE HYBRIDE

Afin de mieux comprendre la portée concrète d'une guerre hybride, il convient d'en examiner les manifestations dans différents secteurs ou champs d'opération, ainsi qu'à travers des cas pratiques. Les attaques hybrides ne se limitent pas au domaine strictement militaire : elles visent aussi bien le cyberespace, l'information, l'économie, etc., de manière coordonnée. Les exemples mondiaux et régionaux abondent, illustrant comment la conflictualité hybride s'insère tant dans les armées que dans les sociétés civiles. Ci-dessous comment un conflit hybride peut se déployer sur le plan militaire et dans le domaine numérique et informationnel deux sphères particulièrement pertinentes dans le contexte actuel ; et la guerre hybride en République démocratique du Congo.

II. 1. Sur le plan militaire

Sur le terrain militaire, la guerre hybride se manifeste par l'intégration de méthodes de combat non conventionnelles aux opérations classiques. Concrètement, l'adversaire va au-delà du face-à-face entre armées régulières en recourant à des forces irrégulières et à la dissimulation.

Quelques formes clés de manifestations militaires hybrides sont notamment l'infiltration par des forces spéciales "niées", l'appui occulte à des milices locales et mercenaires, la guerre conventionnelle camouflée, et l'armement sophistiqué aux mains de groupes irréguliers, la tactiques de terreur imbriquées à la guérilla.

[3] LUTTWAK, E. N., *Strategy: The Logic of War and Peace,* Harvard University Press, 1990.

L'infiltration par des forces spéciales "niées", c'est l'emploi de commandos ou de soldats sans insignes opérant clandestinement en territoire adverse. Cette tactique a été observée lors de l'intervention russe en Crimée et au Donbass, où des hommes en tenue militaire sans marque nationale ont pris position, brouillant la distinction entre une rébellion locale spontanée et l'action d'une puissance étatique. De telles troupes « furtives » permettent de conquérir du terrain tout en maintenant le déni plausible au niveau politique.

L'appui occulte à des milices locales et mercenaires (SMP) fait qu'au lieu d'engager ouvertement ses propres troupes, un État peut soutenir des groupes armés non étatiques pour faire le sale boulot. Cela inclut le recours à des sociétés militaires privées. Ces combattants privés, motivés par l'argent, interviennent sans engager officiellement la responsabilité de l'État qui les emploie. En Afrique, par exemple, la présence de la SMP russe Wagner aux côtés des armées nationales en République centrafricaine et au Mali illustre cette dimension hybride, où la frontière entre soldats réguliers et contractuels privés s'estompe. Ces acteurs agissent dans l'opacité, échappant souvent au droit international et peuvent déstabiliser des régions entières tout en offrant à leur sponsor une couverture politique.

Dans la guerre conventionnelle camouflée, un belligérant hybride peut mener des actions militaires classiques (déploiement de blindés, d'artillerie, de missiles) tout en les dissimulant derrière le paravent d'une insurrection locale. Comme l'explique le chercheur Élie Tenenbaum, ce mode opératoire « fait de la composante irrégulière la force principale[4] tandis que la puissance régulière fournit un soutien logistique et financier » . L'exemple du conflit dans l'est de l'Ukraine (Donbass) est parlant : la Russie, acteur étatique, a soutenu militairement des séparatistes locaux, combinant ainsi une offensive conventionnelle non déclarée et une guerre civile artificielle.

Pour l'armement sophistiqué aux mains de groupes irréguliers, la guerre hybride dote des acteurs non étatiques de capacités militaires avancées autrefois réservées aux armées régulières. Par exemple, on a vu des mouvements rebelles utiliser des drones de reconnaissance ou même armés sur le champ de bataille (cas observés en Libye ou en Éthiopie ces dernières années). Cette montée en

[4] TENENBAUM E., *Partisans et centurions : Une histoire de la guerre irrégulière au XXe siècle,* Perrin, Paris, 2019.

gamme des moyens irréguliers accroît la létalité et la portée de ces groupes le Hezbollah libanais, dès 2006, a pu tirer un missile de croisière anti-navire contre une frégate israélienne, exploit autrefois inimaginable pour une milice.

Les tactiques de terreur imbriquées à la guérilla font que l'adversaire hybride combine volontiers des actes de terrorisme (attentats à l'explosif, massacres ciblés de civils pour terroriser la population) avec des manœuvres de guérilla classique contre les forces militaires. Par exemple, un groupe djihadiste peut lancer une attaque surprise sur une base isolée (tactique de guérilla), puis diffuser des images effroyables de victimes civiles pour semer la panique (terrorisme psychologique). Ce mélange décuple l'impact psychologique et rend la réponse des autorités délicate, car il faut à la fois traquer des combattants irréguliers et protéger les populations locales visées.

En résumé, sur le plan militaire, la guerre hybride se traduit par une hybridation des forces et des modes d'action. L'ennemi cherche constamment l'asymétrie : il utilise « tout ce qui n'est pas conventionnel » pour contourner la puissance de feu classique de son adversaire.

Cette approche exploite les angles morts des armées régulières. Face à une armée nationale classique, un acteur hybride peut ainsi simultanément financer des milices locales, mener des embuscades insurrectionnelles, employer des mercenaires étrangers et lancer des cyberattaques contre les communications militaires. En étirant les forces de défense sur plusieurs fronts à la fois, il les submerge. Les États africains font de plus en plus face à ce défi : par exemple au Mali, les Forces armées maliennes appuyées discrètement par des « instructeurs » russes de Wagner affrontent des katibas djihadistes adeptes de la guérilla, illustrant un schéma hybride (État + SMP vs insurrection + terrorisme) désormais bien réel sur le continent.

II. 2. Dans le domaine numérique et informationnel

Le cyberespace est un pilier central de la guerre hybride moderne. L'adversaire y déploie des attaques et des manipulations visant à désorganiser son ennemi sans confrontation directe. Par ailleurs, le champ informationnel et idéologique, souvent couplé au cyber, sert à affaiblir la volonté de résistance de la cible.

La guerre hybride prend plusieurs formes notamment : la cyberguerre et sabotage informatique, la désinformation et propagande en ligne, la radicalisation et le recrutement via l'internet, l'ingérence électorale et l'espionnage numérique, et la perturbation des communications.

La cyberguerre et sabotage informatique fait référence aux attaques cybernétiques massives qui peuvent paralyser des infrastructures vitales d'un pays sans tirer un seul coup de feu. Par exemple, un assaillant peut déployer un virus destructeur ou un ransomware sur le réseau électrique, les systèmes bancaires ou les hôpitaux d'un État, plongeant celui-ci dans le chaos. En Afrique, même si les capacités cyber offensives des groupes hostiles restent limitées, la menace est bien réelle : des attaques par cryptovirus ont touché des hôpitaux en Afrique du Sud, des entreprises au Nigeria, etc. On peut imaginer le scénario noir d'une cyberattaque réussie contre un réseau électrique national, causant une panne généralisée c'est un cas de menace hybride pris très au sérieux désormais par les services de sécurité.

La désinformation et la propagande en ligne font de la guerre de l'information une arme privilégiée de l'espace numérique. L'adversaire conduit des campagnes de désinformation via les réseaux sociaux, les sites web et les messageries, pour semer la discorde et saper la légitimité des autorités. L'objectif est de créer un narratif favorable à l'agresseur tout en divisant le camp adverse. Par exemple, de fausses images ou rumeurs peuvent accuser une armée régulière de crimes imaginaires afin de la discréditer, ou au contraire présenter des insurgés comme des « libérateurs ». Au Mali, en avril 2022, une campagne en ligne coordonnée a diffusé de prétendues photos de charniers de civils attribués aux forces françaises, alors qu'il s'agissait d'une mise en scène orchestrée par des mercenaires de Wagner. Cet épisode du faux charnier de Gossi illustre le pouvoir de la manipulation informationnelle : en quelques heures, la perception de l'intervention française a pu être altérée par une fake news habile, créant un scandale international avant même que la vérité ne soit rétablie.

La radicalisation et le recrutement via l'internet sont une aubaine pour les groupes extrémistes exploitent largement Internet pour diffuser leur idéologie et recruter des partisans. Des messages de radicalisation circulant sur YouTube, WhatsApp ou Facebook peuvent constituer des signaux faibles annonciateurs d'une menace terroriste émergente. Par exemple, l'apparition soudaine de prêches

djihadistes en langue locale sur les réseaux sociaux d'une région jusqu'alors paisible peut indiquer que des agents du chaos cherchent à y gagner des soutiens. Le domaine numérique sert ainsi de terreau à l'émergence d'une « cinquième colonne » idéologique prête à soutenir une action armée ultérieure.

L'ingérence électorale et espionnage numérique : un Etat hostile peut recourir au piratage informatique pour voler des données sensibles (listes électorales, communications internes compromettantes) et les divulguer au moment opportun afin d'influencer des processus politiques. Des campagnes d'ingérence numérique peuvent aussi consister à financer des trolls locaux pour orienter les débats en ligne, ou à déployer des bots sur Twitter et Facebook qui inondent l'espace médiatique de propagande et de discours polarisants. Le but est de fausser les mécanismes démocratiques de l'ennemi de façon invisible. On se souvient de l'ingérence russe dans les élections américaines de 2016 via le piratage de courriels et l'activisme de fermes à trolls ; ce type de méthode peut être adapté contre des pays africains, par exemple pour attiser des conflits électoraux à dimension ethnique.

La perturbation des communications est une stratégie pour l'adversaire hybride. Il peut chercher à couper les moyens de communication de sa cible, soit par des attaques informatiques de grande ampleur, soit par des sabotages physiques. Par exemple, des attaques DDoS (déni de service) peuvent rendre indisponibles les sites web gouvernementaux ou des médias pendant une crise majeure, privant l'État de ses canaux d'information officiels. Des câbles Internet sous-marins ou des antennes satellitaires peuvent également être sabotés pour plonger une région dans un black-out numérique. Une telle perturbation isole la population, propage la panique et entrave la coordination de la défense du pays visé.

En résumé, le champ numérique et informationnel est devenu incontournable dans les guerres hybrides. Un rapport de l'Assemblée parlementaire du Conseil de l'Europe[5] note que les États font face à « des campagnes de désinformation massive, y compris sous forme de fausses nouvelles sur les réseaux sociaux, des

[5] Conseil de l'Europe, Menaces hybrides et sécurité démocratique en Europe, Rapport de l'Assemblée parlementaire, Strasbourg, 2021.

ingérences dans les processus électoraux, la perturbation des communications, etc., pouvant déstabiliser et saper l'ensemble d'une société ».

L'Afrique n'est pas épargnée : la pénétration rapide des smartphones et des réseaux sociaux, même dans des zones rurales, offre un vecteur par lequel des puissances étrangères ou des groupes armés peuvent influencer l'opinion publique. Combiner ces attaques numériques avec des actions militaires ou économiques amplifie l'efficacité de la guerre hybride, en prenant l'adversaire à revers là où il est souvent le moins préparé c'est-à-dire sur le terrain virtuel. Notons que des technologies émergentes, comme l'intelligence artificielle, pourraient encore accentuer ces menaces en permettant des opérations de guerre invisible automatisée (ex. création de faux contenus ultraciblés, cyberattaques pilotées par IA[6]).

II. 3. La guerre hybride en République démocratique du Congo

Au-delà des considérations sectorielles, la République démocratique du Congo constitue une illustration paradigmatique des dynamiques de la guerre hybride en Afrique centrale. Son histoire contemporaine, marquée par des conflits multiformes et persistants, met en évidence la complexité des menaces qui échappent aux classifications classiques de la guerre. En particulier dans la partie orientale du pays, les épisodes de violence armée ont impliqué une diversité d'acteurs, étatiques, non étatiques, communautaires, transnationaux, évoluant dans une zone grise entre guerre conventionnelle, insurrection interne et ingérence étrangère.

Ces conflits hybrides se caractérisent par l'interconnexion de plusieurs dimensions : opérations militaires asymétriques, campagnes de désinformation, exploitation des ressources naturelles, mobilisation identitaire ou religieuse, et parfois l'usage cynique de la négociation politique comme levier tactique. La RDC incarne à ce titre un théâtre d'opérations où se déploient, souvent simultanément, des logiques militaires, économiques, sociales et diplomatiques.

Qu'il s'agisse de rébellions structurées bénéficiant du soutien de puissances voisines, de milices communautaires enracinées dans des griefs historiques locaux, ou de groupes politico-militaires se construisant sur les failles de l'État, les cas

[6] CLAPPER J. R., *Facts and Fears: Hard Truths from a Life in Intelligence,* Viking Press, 2017.

congolais révèlent à quel point la porosité entre conflit intérieur et agression extérieure est un élément central de la guerre hybride contemporaine.

Nous analysons ici plusieurs cas emblématiques, le Mouvement du 23 Mars (M23), le Rassemblement Congolais pour la Démocratie (RCD), le Congrès National pour la Défense du Peuple (CNDP), l'insurrection Kamuina Nsapu, ainsi que la milice Mobondo, afin d'illustrer les différentes formes, logiques et impacts d'une guerre hybride appliquée au contexte congolais

II. 3. 1. Mouvement du 23 mars (M23)

Le Mouvement du 23 Mars (M23) est une rébellion armée apparue en 2012 dans l'est de la République démocratique du Congo, plus précisément dans la province du Nord-Kivu, avant d'être réactivée en 2021 après plusieurs années d'accalmie. Le groupe trouve son origine dans les désaccords sur l'application de l'accord de paix du 23 mars 2009, signé entre le gouvernement congolais et le Congrès national pour la défense du peuple (CNDP), lui-même héritier du Rassemblement congolais pour la démocratie (RCD), d'où le nom M23.

La composition du M23 reflète la continuité stratégique de la guerre hybride dans la région. Il regroupe d'anciens membres du RCD intégrés au sein du CNDP, puis incorporés dans les FARDC avant d'entrer en dissidence, des éléments issus de l'ex-Armée patriotique rwandaise (APR), et des groupes tutsis congolais anciennement enrôlés de force ou marginalisés par les structures sécuritaires nationales.

Rapidement, le M23 bénéficie d'un soutien extérieur important, en particulier du Rwanda, comme le confirment de nombreux rapports onusiens et d'ONG. Son retour sur la scène militaire a plongé l'est du Congo dans une crise sécuritaire et humanitaire d'une ampleur exceptionnelle : massacres de civils, violences sexuelles utilisées comme arme de guerre, destruction de villages, et plus de 6,9 millions de personnes déplacées à l'intérieur du pays.

Il ne s'agit pas d'une simple rébellion locale : le M23 représente une ingérence étrangère dissimulée derrière un habillage congolais, Kigali poursuivant ses intérêts économiques, sécuritaires et géopolitiques tout en niant toute implication directe. Les FARDC se retrouvent confrontées à un ennemi hybride, combinant tactiques de guérilla, actions militaires quasi-conventionnelles, armement moderne et appui logistique transfrontalier.

Parallèlement à l'action militaire, le M23 s'inscrit dans une stratégie globale de guerre hybride, mêlant propagande informationnelle, justifications diplomatiques et exploitation économique des zones conquises. Le Rwanda orchestre ainsi une guerre par procuration, justifiant ses interventions par la menace persistante des FDLR ou la nécessité de protéger les populations tutsies du Congo, tout en promouvant sa position sur la scène internationale. Sur les réseaux sociaux, les porte-parole du M23 tentent de façonner le récit du conflit, tandis que le pillage systématique des ressources minières dans les zones sous contrôle rebelle accentue la dimension économique de la guerre.

Comme l'a souligné un observateur international, « il ne s'agit plus d'un conflit traditionnel mais bien d'une guerre hybride, alimentée par des intérêts économiques, miniers et stratégiques, qui dépasse les logiques classiques d'affrontement entre États ». Le gouvernement congolais partage cette analyse : le ministre de la Communication, Patrick Muyaya, a récemment qualifié la guerre à l'Est d'« affrontement combinant agression militaire, manipulation informationnelle et pression économique », appelant à une riposte nationale tout aussi multidimensionnelle.

En définitive, le M23 constitue un cas d'école de la guerre hybride en Afrique centrale : un groupe armé aux racines locales, mais aux ramifications régionales, utilisé comme vecteur indirect d'ingérence par un État voisin, au service d'objectifs stratégiques multiples.

II. 3. 2. Rassemblement Congolais pour la Démocratie (RCD)

Parmi les précédents les plus marquants en matière de guerre hybride en République démocratique du Congo, le cas du Rassemblement congolais pour la démocratie (RCD) occupe une place centrale. Ce mouvement rebelle est apparu en 1998, dans le contexte du déclenchement de la Deuxième guerre du Congo, avec le soutien militaire, politique et logistique massif du Rwanda et de l'Ouganda. Il a servi de vecteur d'intervention indirecte pour ces deux puissances régionales, leur permettant de projeter leurs forces armées sur le territoire congolais tout en prétendant soutenir une rébellion interne.

En réalité, le RCD a constitué un habillage politico-militaire d'une intervention étrangère planifiée, brouillant les frontières entre guerre civile et invasion régionale. Appuyé par des troupes régulières rwandaises et ougandaises, le

mouvement a rapidement pris le contrôle de vastes portions de l'est de la RDC, notamment dans les provinces du Nord-Kivu, Sud-Kivu, et de la Province Orientale. Dans ces zones, il a mis en place des structures administratives parallèles, instaurant une forme de gouvernance de substitution à l'État central congolais. Ce pouvoir de facto s'est accompagné d'un discours politique justificateur, présentant le RCD comme un mouvement de libération nationale, soucieux de restaurer la démocratie et de mettre fin à la mauvaise gouvernance.

Le caractère hybride du RCD se manifeste dans sa triple nature : militaire, avec des opérations offensives menées conjointement par des unités rebelles et des soldats réguliers étrangers, utilisant parfois des moyens lourds (blindés, artillerie) ; politique, à travers une rhétorique nationaliste et une tentative de légitimation diplomatique sur la scène régionale et économique, avec une stratégie de prédation des ressources naturelles (coltan, or, bois, etc.) dans les zones occupées, au profit de réseaux transfrontaliers d'enrichissement.

Le mouvement a également joué sur plusieurs fronts diplomatiques, ses parrains régionaux se présentant comme médiateurs du conflit qu'ils alimentaient en coulisses. Ce double jeu a renforcé la confusion stratégique, et permis au Rwanda et à l'Ouganda de maintenir une négation plausible de leur implication directe dans la guerre, en déléguant à un acteur congolais l'expression visible de leurs intérêts.

L'aboutissement de cette guerre hybride s'est opéré en 2003 avec les Accords de Sun City, dans le cadre de la formule de transition dite « 1 + 4 » (un président et quatre vice-présidents). Le RCD a alors été converti en parti politique légal, dont plusieurs cadres ont intégré les institutions nationales, y compris au sein de l'armée et du gouvernement. Ce passage du statut de mouvement armé à celui d'acteur institutionnel illustre une facette cruciale de la guerre hybride : la transformation d'une force rebelle en interlocuteur politique, permettant une recomposition stratégique sans véritable rupture de continuité.

Ainsi, le cas du RCD démontre de manière exemplaire comment une rébellion armée peut être instrumentalisée par des puissances étrangères pour atteindre des objectifs stratégiques tels que : le contrôle territorial, le pillage économique, l'influence politique, tout en s'ancrant dans des logiques de guerre prolongée, négociée et réadaptée.

II. 3. 3. Insurrection Kamuina Nsapu (2016-2017)

Tous les conflits hybrides en République démocratique du Congo ne relèvent pas nécessairement d'une ingérence étrangère. L'insurrection de Kamuina Nsapu, qui a embrasé la région du Grand Kasaï entre 2016 et 2017, constitue une illustration emblématique d'un conflit hybride à dominante interne, révélateur des tensions structurelles au sein de l'État congolais.

À l'origine, il s'agit d'un conflit localisé : l'assassinat de Jean-Prince Mpandi, chef coutumier de Kamuina Nsapu, entré en dissidence contre l'autorité de l'État central, déclenche un soulèvement de ses partisans. Ce soulèvement mobilise essentiellement des jeunes ruraux marginalisés, armés d'armes artisanales et galvanisés par des rituels magico-religieux censés leur conférer l'invulnérabilité face aux forces de l'ordre.

Très vite, l'insurrection dépasse le cadre local pour s'étendre à plusieurs provinces du Kasaï, transformant une région historiquement paisible en foyer de violences généralisées. Les symboles de l'État : administrations, forces de l'ordre, représentants de l'autorité, deviennent des cibles privilégiées, tandis que la milice Kamuina Nsapu, à l'organisation floue mais très mobile, mêle croyances mystiques, discours de révolte politique et exactions brutales. Des enfants-soldats sont enrôlés, et des massacres ciblés sont perpétrés contre des civils, notamment ceux perçus comme liés à l'État ou appartenant à d'autres communautés.

Face à cette menace, l'armée congolaise réagit avec une répression brutale, déclenchant une spirale de violences. Les combats donnent lieu à l'incendie de villages entiers, à la découverte de fosses communes, et à une détérioration rapide de la situation humanitaire. Le bilan humain est lourd : plus de 3 300 morts selon l'Église catholique à la mi-2017, et jusqu'à 5 000 morts selon les estimations des Nations unies en 2018. Environ 1 million de personnes sont déplacées à l'intérieur du pays, et des dizaines de milliers de réfugiés fuient vers l'Angola.

Sur le plan analytique, cette insurrection présente toutes les caractéristiques d'un conflit hybride interne. Elle combine des formes classiques d'affrontement armé avec des éléments de résistance irrégulière, décentralisée et mystico-

idéologique. Elle utilise des modes d'action insaisissables, comme la guérilla rurale sans commandement unifié. Elle joue sur les représentations symboliques, exacerbant l'opposition entre pouvoir coutumier et autorité centrale.

Le rôle de l'information et de la perception est ici central. La diffusion virale de vidéos montrant des atrocités, notamment des exécutions sommaires de jeunes adeptes par les forces armées congolaises, ou encore celle des deux experts des Nations unies en mission d'enquête, a suscité un choc international et mis le gouvernement sous une pression diplomatique forte.

La résolution partielle de cette crise a nécessité une approche combinée : d'une part, une répression militaire pour démanteler les bastions de la milice ; d'autre part, des démarches politiques et coutumières, notamment à travers la réinstallation d'un chef traditionnel reconnu et des négociations locales avec les communautés encore mobilisées.

Le phénomène Kamuina Nsapu démontre que, même en l'absence d'un acteur étranger, un conflit interne peut basculer dans une logique hybride, mêlant insurrection armée, soulèvement populaire, guerre psychologique et mystique, manipulation des récits, et crise humanitaire de grande ampleur.

Il révèle surtout comment la fragilité de l'Etat congolais, l'absence de services publics de proximité et les frustrations socioéconomiques chroniques peuvent être exploitées pour produire une menace sécuritaire difficilement maîtrisable par les seules méthodes conventionnelles. Ce cas met en lumière l'importance d'une stratégie d'anticipation fondée sur la gouvernance locale, la veille communautaire et la réponse rapide aux signaux faibles de contestation.

II. 3. 4. Milice Mobondo (2022 à ce jour)

Un autre visage de la guerre hybride en République démocratique du Congo se manifeste à travers les violences communautaires de l'ouest du pays, particulièrement avec le phénomène dit des « Mobondo ». Cette appellation désigne une milice d'autodéfense apparue à partir de 2022 dans la province du Maï-Ndombe et les zones adjacentes (notamment le territoire de Kwamouth), sur fond de conflit foncier, identitaire et coutumier entre les communautés Teke (autochtone) et Yaka (présentés comme allochtones).

À l'origine limitées à des affrontements villageois autour du contrôle des terres et de la légitimité des chefs traditionnels, ces violences ont rapidement

dégénéré en une insurrection rurale structurée, dirigée contre les civils Teke et l'autorité de l'État central. La milice Mobondo, composée majoritairement de jeunes issus de la communauté Yaka, a mené des attaques systématiques et coordonnées non seulement contre des villages mais aussi contre des éléments de l'appareil sécuritaire congolais (policiers, militaires, agents administratifs).

En quelques mois, l'activisme de cette milice a provoqué une crise sécuritaire et humanitaire de grande ampleur dans l'ouest du pays : plus de 3 000 morts selon les estimations d'organisations locales ; environ 550 000 personnes déplacées internes ; et un climat de peur généralisée, aggravé par l'impossibilité pour l'État de restaurer son autorité dans les zones concernées.

Les méthodes de la milice Mobondo illustrent parfaitement les logiques de guerre hybride : brutalité extrême : massacres à la machette, incendies de villages, viols collectifs, enlèvements ciblés ; mobilité stratégique : les miliciens se fondent dans la population ou se réfugient dans les forêts pour échapper aux opérations de l'armée ; et utilisation des symboles coutumiers et communautaires pour justifier leur insurrection et recruter localement.

Le caractère hybride de cette insurrection se manifeste également dans l'impact stratégique disproportionné qu'elle engendre. Alors que l'attention nationale et internationale est centrée sur la guerre contre le M23 à l'est, la montée en puissance de la milice Mobondo à l'ouest a pris l'Etat congolais de court. A tel point que les Forces armées de la RDC (FARDC) ont été contraintes de rediriger des troupes déployées à l'est vers le front occidental, exposant ainsi un déséquilibre dans la gestion stratégique des menaces internes. Le fait que cette crise ait atteint les abords de la capitale, notamment dans la commune rurale de Maluku, constitue un signal d'alarme majeur.

Comme le note un rapport de la Commission Justice et Paix de Kinshasa : « C'est une situation oubliée. La plupart des habitants de Kinshasa ignorent que cette crise est arrivée jusqu'à Maluku, à la porte de la capitale… Il y a de nombreuses victimes, tant civiles que militaires, alors que ces derniers sont nécessaires à l'Est. Ils meurent gratuitement ici à l'Ouest, faute de stratégies efficaces pour mettre fin à cette aventure. »

Au-delà de sa brutalité, la milice Mobondo représente un acteur hybride au sens plein du terme : elle mêle des motivations initialement locales (disputes

coutumières, frustrations foncières) à des conséquences politico-sécuritaires nationales. Certains observateurs évoquent même une possible instrumentalisation politique, notamment par des acteurs intéressés à affaiblir le pouvoir central, en exploitant des tensions communautaires persistantes.

Face à une telle menace, les réponses purement militaires apparaissent insuffisantes. La solution envisagée par les acteurs locaux et internationaux s'inscrit dans une approche pluridimensionnelle, intégrant : des opérations militaires ciblées (ratissage, démantèlement des bastions miliciens) ; un dialogue intercommunautaire structuré (notamment entre chefs coutumiers et autorités provinciales) ; des poursuites judiciaires exemplaires pour les instigateurs et recruteurs de la violence ; et une politique de réconciliation territoriale à travers une meilleure gouvernance foncière et la reconnaissance des droits coutumiers.

La milice Mobondo met en évidence les nouveaux visages de la menace hybride en RDC : décentralisée, communautaire, mobile, symbolique et potentiellement manipulée, elle complique la tâche des planificateurs sécuritaires congolais. Elle rappelle aussi qu'un État qui néglige la gestion de ses périphéries peut se retrouver submergé par des foyers de crise inattendus, capables d'ébranler son équilibre national.

II. 3. 5. Congrès national pour la défense du peuple (CNDP)

Entre 2006 et 2009, le Congrès national pour la défense du peuple (CNDP), dirigé par le général déchu Laurent Nkunda, un officier tutsi congolais, ancien cadre du RCD/Goma ayant combattu lors de la deuxième guerre du Congo sous la bannière rwandaise, a incarné une nouvelle phase de la guerre hybride dans l'est de la RDC. Ce mouvement est issu d'une scission non organique de l'armée congolaise, consécutive aux défaillances du processus d'intégration post-Transition (2003-2006), marquant l'échec partiel de la réunification des forces armées après les accords de paix.

Le CNDP a été principalement composé d'ex-rebelles rwandophones, en majorité issus des rangs de l'ex-Armée patriotique rwandaise (APR) ; d'anciens du RCD/Goma intégrés dans les FARDC mais ayant fait dissidence entre 2004 et 2006 ; de groupes tutsis congolais mobilisés dans les territoires de Masisi, Rutshuru, et Nyiragongo ; ainsi que de jeunes recrues locales, principalement issues de la communauté tutsie.

Sous couvert d'un discours identitaire revendiquant la protection des populations tutsies congolaises, souvent présentées comme marginalisées ou menacées par d'autres groupes ou par l'État, le CNDP a structuré un véritable système parallèle de pouvoir dans le Nord-Kivu : mise en place d'une administration locale autonome ; prélèvement de taxes illégales sur les routes commerciales ; encadrement militaire des zones occupées ; et établissement de canaux diplomatiques informels, souvent appuyés en sous-main par Kigali.

Comme dans les cas du RCD et du M23, le Rwanda a été fortement soupçonné de soutenir activement le CNDP, tant sur le plan logistique que dans la planification stratégique. Plusieurs rapports des Nations unies et d'ONG indépendantes ont documenté la présence d'éléments rwandais dans les rangs ou dans l'encadrement du CNDP, bien que Kigali ait toujours nié formellement toute implication directe.

Le caractère hybride du CNDP se manifeste à plusieurs niveaux : par sa double identité de mouvement armé rebelle et acteur politique en quête de reconnaissance ; par sa capacité à alterner diplomatie, négociation, et action militaire ; et par son usage simultané de la guérilla, de l'intimidation politique, et de la manipulation communautaire.

Le CNDP a exploité les leviers médiatiques pour présenter ses actions comme une défense communautaire légitime, tout en multipliant les attaques asymétriques contre les FARDC, perturbant l'ordre public dans des zones stratégiques proches de Goma. Parallèlement, il a su tirer parti des mécanismes régionaux de paix, notamment à travers les négociations de Nairobi (2008,2009), où il a obtenu des engagements partiels du gouvernement en échange d'un cessez-le-feu temporaire. Cette capacité à instrumentaliser le processus de paix tout en poursuivant des actions armées sur le terrain est une des marques typiques des acteurs hybrides.

L'arrestation surprise de Laurent Nkunda par le Rwanda en 2009, suivie d'une tentative d'intégration de ses troupes dans les FARDC, n'a pas mis fin à la logique du CNDP. Bien au contraire, une frange importante des ex-combattants du CNDP a refusé l'intégration ou a été mal encadrée, formant plus tard l'embryon du Mouvement du 23 mars (M23). Cette continuité organique et stratégique entre les deux mouvements démontre que le CNDP n'était pas une simple rébellion

conjoncturelle, mais bien un vecteur d'influence géostratégique à long terme, mobilisé au service d'objectifs transfrontaliers.

En somme, le cas du CNDP illustre une stratégie hybride prolongée, combinant : ingérence étrangère indirecte, rébellion armée à fondement communautaire, contrôle territorial et fiscal parallèle, et exploitation politique du dialogue de paix. Il montre comment un acteur militaire irrégulier peut évoluer simultanément comme belligérant, négociateur et relais d'intérêts extérieurs, dans une région riche en ressources minières et hautement stratégique.

Le cas de la République Démocratique du Congo illustre de manière exemplaire la complexité multidimensionnelle des guerres hybrides en contexte africain. On y observe à la fois des ingérences étatiques extérieures à travers des rébellions proxies telles que le RCD, le CNDP ou, plus récemment, le M23, soutenues en sous-main par des puissances voisines ; des conflits internes multiformes exploitant les failles de la gouvernance nationale, qu'il s'agisse d'insurrections coutumières (Kamuina Nsapu) ou de milices communautaires violentes (Mobondo) ; des stratégies ambiguës de contrôle du pouvoir, où certaines forces irrégulières tolérées ou instrumentalisées par les autorités contribuent à une instabilité persistante.

Cette superposition de menaces asymétriques contraint l'État congolais à une adaptation permanente de ses modes d'action. Il lui faut à la fois conduire une guerre conventionnelle contre des forces dotées de logistiques et de soutiens transfrontaliers ; mener des opérations de contre-insurrection dans les provinces ; engager une réforme en profondeur de son appareil politico-sécuritaire, afin de restaurer la légitimité de l'État et d'éviter d'alimenter lui-même les cycles de violence.

C'est précisément ce niveau de complexité stratégique, articulant différents registres de conflictualité, que recouvre le concept de guerre hybride : un enchevêtrement de conflits de nature distincte, souvent synchronisés ou instrumentalisés, qui se renforcent mutuellement et rendent obsolètes les approches classiques et unidimensionnelles en matière de défense et de sécurité.

III. ENJEUX HYBRIDES EN AFRIQUE CENTRALE : SCENARIOS PROSPECTIFS

Les pays d'Afrique centrale se trouvent aujourd'hui à la convergence de plusieurs dynamiques propices à la guerre hybride : implication de SMP étrangères

dans les conflits locaux souvent autour de ressources naturelles, circulation régionale de groupes armés, exacerbation de tensions identitaires locales par des discours extrémistes, et vulnérabilités économiques post-pandémie, résurgences d'insurrections djihadistes, fragilités économiques et institutionnelles internes.

Pour explorer ces enjeux de manière structurée, nous esquissons ci-après plusieurs scénarios prospectifs allant du pire au meilleur concernant l'évolution possible d'un État fictif de la région confronté à des menaces hybrides. Ces scénarios, fondés sur des tendances réelles, visent à anticiper les défis et à éclairer les choix stratégiques. Le pays imaginé cumule des traits de plusieurs États d'Afrique centrale afin de servir de cas d'école ; toute ressemblance avec un pays existant comme par exemple la RDC ou la Centrafrique, n'est pas fortuite, mais le scénario ne se limite pas à un cas particulier).

L'anticipation stratégique repose en effet sur la lecture croisée des signaux faibles[7] et des tendances lourdes c'est ce que nous appliquons ici en construisant trois scénarios contrastés sur un horizon de cinq ans.

III. 1. Scénario pessimiste (embrasement généralisé)

Imaginons un Etat d'Afrique centrale présentant les facteurs suivants : de fortes tensions intercommunautaires internes, l'ingérence de mercenaires d'une SMP autour de zones minières stratégiques, et la propagation de messages djihadistes sur les réseaux sociaux locaux. Cette situation, qui rappelle des contextes réels récents, dégénère progressivement.

Les affrontements interethniques initiaux fournissent un terreau au recrutement par un groupe insurgé local, tandis que la SMP étrangère arme discrètement une faction rebelle sous couvert de « protection des investissements ». Parallèlement, une campagne de désinformation en ligne attise la haine entre communautés et discrédite le gouvernement légitime. En quelques mois, l'État perd le contrôle de plusieurs territoires : une coalition de milices locales et de combattants étrangers s'empare d'une province minière clé, proclamant un mouvement de libération. Le pouvoir central, débordé, fait appel à des partenaires internationaux, mais la situation sur le terrain est chaotique. Des exactions

[7] ADANGA S., « Gouvernance anticipative et sécurité en Afrique centrale », dans *Revue africaine de stratégie,* 2023.

massives contre les civils sont rapportées. Le conflit prend également une tournure régionale : des flux de réfugiés affluent vers les pays voisins, certains combattants franchissent les frontières pour établir des bases arrière, provoquant l'inquiétude des capitales voisines.

Sous la pression, l'armée nationale s'effondre partiellement, certains soldats faisant défection pour rejoindre des groupes armés rémunérés par la SMP. Ce scénario catastrophe verrait ainsi la quasi-balkanisation du pays, avec l'établissement de zones de non-droit contrôlées par des seigneurs de guerre. Pour la communauté internationale, le dilemme serait grand : intervenir militairement pour éviter un effondrement total (au risque d'une guerre ouverte avec les puissances soutenant en sous-main les belligérants) ou tenter de contenir le conflit aux frontières.

Du point de vue national, le gouvernement serait confronté à des choix cornéliens : soit composer avec la SMP et les milices pour faire cesser leurs abus, soit mettre fin à ces collusions au risque d'aggraver temporairement le vide sécuritaire. On peut voir dans la crise centrafricaine de 2013-2014 un exemple d'une dérive similaire, où la rupture entre ex-Séléka et anti-Balaka, attisée par des influences extérieures, a plongé le pays dans la guerre civile , il a fallu l'intervention de l'ONU et de la France pour éviter un génocide. Le Sahel[8] constitue également un précédent inquiétant pour la sécurité en Afrique centrale (UNDP, 2022), montrant comment l'embrasement d'un conflit hybride peut déborder sur des États fragiles voisins.

Ce scénario pessimiste met en lumière les enchaînements qu'il faut absolument chercher à éviter : escalade de la violence interethnique, laissez-faire vis-à-vis de mercenaires incontrôlés, vide de gouvernance exploité par des djihadistes. Il souligne l'impératif d'agir en amont pour ne pas laisser la situation se détériorer à ce point.

III. 2. Scénario intermédiaire (dégradation contenue)

Dans ce scénario, les mêmes menaces hybrides émergent mais l'État parvient partiellement à les contenir sans toutefois les résoudre. Les violences intercommunautaires éclatent, mais l'armée, bien que débordée au début, réussit à sécuriser les principales villes. La SMP continue d'opérer dans la zone minière,

[8] International Crisis Group, Avoiding the Perfect Storm in the Sahel, Africa Report n°293, 2021.

sous le regard impuissant du gouvernement qui craint qu'une rupture du contrat n'aggrave la situation.

Les groupes armés locaux, eux, ne sont pas éradiqués mais limités à des zones rurales périphériques. La campagne de désinformation en ligne sème la confusion parmi la population urbaine, alimentant méfiance et théories du complot, ce qui fragilise le soutien au gouvernement.

Cependant, grâce à la médiation de partenaires régionaux, un semblant de dialogue s'instaure avec certains chefs miliciens, aboutissant à des cessez-le-feu localisés. L'État accepte tacitement la présence de la SMP pour éviter un front supplémentaire, mais négocie un encadrement de ses activités (par exemple en l'intégrant à une « coalition » de stabilisation sous mandat de l'Union africaine, bien que cela reste de façade).

Le pays évite le pire, il n'y a pas d'effondrement général ni de massacres à grande échelle, mais il s'installe dans une crise prolongée à basse intensité. Sur le plan économique, les investissements fuient, à l'exception du secteur minier contrôlé par des intérêts privés étrangers. Les déplacés internes s'entassent autour des villes sous contrôle gouvernemental, constituant un foyer de misère et de ressentiment.

La situation n'est ni guerre ouverte généralisée, ni paix réelle : elle rappelle celle de la RDC dans les années 2000 après les accords de Sun City, où le pays, officiellement réunifié, restait en proie à des milices à l'Est et à une prédation continue de ses ressources. Le gouvernement, fragilisé, dépend largement de l'aide internationale pour éviter l'effondrement économique, tandis que politiquement il navigue entre des exigences contradictoires, montrer une souveraineté intacte et, en même temps, accepter des arrangements de sécurité non conventionnels.

Ce scénario de dégradation contenue souligne la difficulté de restaurer pleinement l'autorité de l'État une fois que le ver est dans le fruit. Il met en garde contre le risque de « normalisation » d'une certaine instabilité : le danger est qu'un État s'habitue à tolérer sur son sol la présence de forces armées étrangères ou de groupes rebelles résiduels, au prix d'une souveraineté amoindrie et d'une population vivant dans l'insécurité chronique. Éviter ce piège requiert une volonté

politique de reprendre progressivement le contrôle de chaque parcelle du territoire et de ne pas institutionnaliser des zones grises de gouvernance.

III. 3. Scénario optimiste (stabilisation proactive)

Dans ce dernier scénario, grâce à des mesures intelligentes et à un sursaut de volonté politique, le pays parvient à désamorcer les tensions et à inverser progressivement les tendances négatives. Le gouvernement initie un ambitieux programme de réconciliation nationale et de développement local, ce qui réduit les frustrations identitaires. Des accords de partage du pouvoir au niveau local apaisent les rivalités entre communautés.

Concernant la SMP, les autorités, sous pression populaire et internationale, décident de mettre fin au contrat avec les mercenaires ; l'armée nationale, mieux formée, reprend elle-même le contrôle de la sécurité des sites miniers, éventuellement avec l'aide de conseillers de l'Union africaine plutôt que de contractants privés. Sur le front idéologique, l'État, en partenariat avec les chefs religieux et la société civile, mène une campagne efficace contre l'extrémisme : les prêcheurs de haine sont arrêtés ou discrédités, tandis que des programmes sociaux (éducation, emploi des jeunes) viennent tarir le vivier de recrutement djihadiste.

Parallèlement, de gros efforts sont faits pour contrer la désinformation : le gouvernement communique de manière transparente, s'appuie sur des journalistes et blogueurs crédibles pour relayer les faits vérifiés, et investit dans la cybersécurité pour contrer les fake news provenant de l'étranger. Au bout de cinq ans, la sécurité intérieure et la cohésion sociale se sont sensiblement améliorées.

Les anciens miliciens ont été en grande partie désarmés et intégrés soit dans un programme de DDR (désarmement, démobilisation, réintégration), soit dans les forces régulières pour les plus disciplinés. Les investissements internationaux reprennent, encouragés par la stabilisation de la situation. Le pays sert même de modèle de résilience pour ses voisins : les leçons tirées de cette sortie de crise profitent aux États de la sous-région confrontés à des défis similaires.

Ce scénario optimiste montre qu'avec de la volonté politique et une approche globale, il est possible de défaire le piège de la guerre hybride. Il insiste sur l'importance d'initiatives locales (réconciliation, développement) conjuguées à des décisions stratégiques au plus haut niveau (exclure les acteurs déstabilisateurs comme les SMP, investir dans la jeunesse). Bien entendu, ce scénario reste l'idéal

et nécessite la conjonction de nombreux facteurs favorables, mais son intérêt est de tracer une feuille de route possible pour les dirigeants qui voudraient réellement neutraliser les menaces hybrides avant qu'elles ne deviennent ingérables.

Variables à surveiller la volonté politique réelle du gouvernement de mettre en œuvre des réformes de gouvernance et de lutter contre la corruption (sans cet engagement au sommet, le scénario optimiste ne peut se concrétiser) ; l'évolution de la perception publique, mesurée via des sondages ou des consultations citoyennes, pour vérifier la baisse du sentiment d'injustice ou d'insécurité dans la population ; le soutien des partenaires internationaux : aide financière au développement, sanctions dissuasives contre les acteurs perturbateurs (par ex. sanctions contre une SMP étrangère) et assistance dans la mise en place des mesures de stabilisation ; des indicateurs de déradicalisation : par exemple la diminution de la diffusion de propagande extrémiste en ligne, ou le nombre de repentis quittant le mouvement djihadiste.

En termes des options stratégiques, il s'agit de consolider ces avancées. Institutionnaliser durablement l'anticipation stratégique au sein de l'appareil d'État , par exemple en créant une cellule de prospective rattachée à la Présidence, chargée de surveiller en continu les facteurs de risque , permettra d'éviter de retomber dans la surprise stratégique. De même, la professionnalisation des forces de sécurité devra s'accompagner d'un ancrage de la culture du renseignement et de la proactivité.

Enfin, le gouvernement devra maintenir un dialogue constant avec la population pour détecter rapidement tout retour de flamme des tensions latentes, et impliquer la société civile dans la consolidation de la paix (mécanismes locaux d'alerte précoce, comités intercommunautaires, etc.). L'ensemble de ces mesures vise à inscrire la stabilisation dans la durée et à immuniser autant que possible le pays contre de futures tentatives de déstabilisation hybride.

IV. MESURES STRATEGIQUES DE RIPOSTE

Face à la palette étendue de menaces hybrides identifiées, il est nécessaire de déployer une riposte tout aussi multidimensionnelle. Les axes d'action stratégiques doivent combiner le renforcement des capacités de défense classique avec des approches innovantes touchant à la société, à l'économie et à la gouvernance.

Ce point propose des mesures concrètes que les Etats d'Afrique centrale, en particulier la RDC et ses voisins, pourraient adopter pour accroître leur résilience et leur capacité de réaction.

Renforcer le renseignement et la coopération inter-agences par l'amélioration du partage d'informations et la synergie entre les différents services de l'État (armée, renseignement intérieur, police, diplomatie). Les attaques hybrides étant multiformes, la création d'une cellule fusionnée de renseignement réunissant analystes de plusieurs agences permet de détecter plus vite les schémas d'agression. Par exemple, l'Union européenne et l'OTAN ont mis en place des centres de fusion pour suivre les menaces hybrides et échanger les bonnes pratiques entre pays. En Afrique centrale, on pourrait s'en inspirer via une coopération renforcée de l'Union africaine et des communautés régional[9], afin d'identifier précocement les campagnes de déstabilisation transnationales (financements occultes de milices, réseaux de désinformation traversant les frontières, etc.). L'OTAN recommande d'ailleurs une réponse résolument coordonnée face à ce type de menaces complexes[10] .

Il y a lieu de muscler la cyberdéfense et la lutte contre les infox. Puisque le cyberespace est un champ privilégié de la guerre hybride, il faut investir dans la sécurité informatique (équipes d'intervention d'urgence cyber CERT, protection des infrastructures critiques, formations spécialisées) et dans la contre-propagande en ligne. Il s'agit d'être capable de réagir vite aux fausses nouvelles massives et aux offensives informationnelles. Un exemple significatif a eu lieu au Mali : lorsque des mercenaires russes ont fabriqué le faux charnier de Gossi pour accuser l'opération Barkhane, l'état-major français a répliqué rapidement en publiant les preuves vidéo du montage, coupant court à la désinformation. Cette réactivité doit devenir la norme. La France, de son côté, a inscrit dans sa loi de programmation militaire le renforcement de ses moyens cyber et d'influence pour faire face à l'hybridité des menaces. Les Etats d'Afrique centrale gagneraient également à mettre en place des cellules de veille médiatique capables de détecter les rumeurs malveillantes circulant sur les réseaux sociaux et d'y répondre par du fact-checking public et des contre-discours officiels, afin de vacciner la population contre les manipulations.

[9] Hybrid CoE, Hybrid Threats: Scenarios and Responses, Helsinki, 2023.
[10] OTAN, Countering Hybrid Threats: NATO's Approach, Publication de l'OTAN, Bruxelles, 2016.

Pour sensibiliser la population et bâtir une résilience sociétale, le grand public doit être conscient de l'existence des menaces hybrides pour ne pas en être victime ou vecteur malgré lui. Une mesure importante est d'éduquer et informer l'opinion sur les techniques de désinformation et de division utilisées par des acteurs hostiles. Par exemple, intégrer dans les programmes scolaires et les campagnes médiatiques des modules d'éducation aux médias et de lutte contre les fake news. Une population vigilante, capable d'identifier une propagande extérieure, sera moins susceptible de se laisser manipuler. De même, renforcer la cohésion interne par exemple en impliquant davantage les communautés locales dans la prévention des conflits et en répondant aux griefs légitimes augmente la résilience face aux ingérences qui cherchent souvent à exploiter les fractures sociales existantes. Comme le note l'OTAN, la confiance et l'unité au sein de la nation sont le meilleur antidote contre ces menaces diffuses.

L'encadrement des SMP et autres acteurs armés non étatiques requiert d'établir un cadre juridique national et international pour contrôler les sociétés militaires privées et autres intervenants armés privés. Beaucoup de conflits hybrides actuels, notamment en Afrique, sont aggravés par l'implication de mercenaires échappant à tout cadre légal[11].

Il convient donc d'adopter des lois ou règlements imposant par exemple l'enregistrement officiel des SMP opérant sur le sol national, la signature de codes de conduite conformes au droit humanitaire, et de prévoir des sanctions contre les États qui les emploient illégalement. L'Assemblée parlementaire du Conseil de l'Europe invite d'ailleurs les États à « s'abstenir de recourir à des sociétés militaires privées dans leurs actions de guerre hybride » et à respecter la souveraineté des autres pays.

En Afrique centrale et de l'Ouest, on pourrait traduire cela par des accords régionaux interdisant le recrutement de mercenaires, et par une vigilance accrue sur les compagnies de sécurité opérant autour des mines ou dans les zones de conflit. Ces mesures réduiraient l'espace de manœuvre des SMP déstabilisatrices.

Il y a lieu d'adopter une approche « globale » de la sécurité (whole-of-government). La lutte contre une menace hybride nécessite de décloisonner

[11] SMAÏL D., *Les sociétés militaires privées en Afrique : acteurs hybrides, enjeux politiques,* L'Harmattan, Paris, 2020.

l'action de l'État et de mobiliser l'ensemble des moyens de la nation. Concrètement, il est préconisé de mettre en place des cellules de crise hybrides rassemblant, sous un pilotage unifié au plus haut niveau, des compétences variées : diplomates, militaires, experts cyber, spécialistes de la communication, etc.

Face à une offensive hybride majeure, la réponse doit en effet être orchestrée sur tous les fronts : par exemple, en cas d'ingérence étrangère combinant émeutes locales et désinformation internationale, l'État pourrait simultanément mener une action policière sur le terrain, une campagne médiatique à l'étranger pour rétablir la vérité, des poursuites judiciaires contre les instigateurs externes et un renforcement des défenses techniques sur ses réseaux. Une telle orchestration n'est possible qu'en brisant les silos bureaucratiques. Il faut également impliquer les alliés et partenaires : aucune nation ne pouvant affronter seule ce type de menace, la coopération régionale est primordiale (partage de renseignements, exercices conjoints simulant des attaques hybrides, etc.). A cet égard, des centres d'excellence spécialisés comme le Centre européen d'Helsinki sur les menaces hybrides ou les mécanismes de l'Union africaine, pourraient être mis à contribution des pays africains pour améliorer leurs capacités de détection et de réaction.

En résumé, combattre la guerre hybride exige tout autant de renforcer les défenses (militaires, cyber, renseignement) que d'accroître la résilience de la société (cohésion sociale, éducation, robustesse du cadre légal). Comme le souligne l'OTAN, « la confiance et l'unité interne sont le meilleur antidote face à ces menaces diffuses ». Enfin, la prévention est cruciale : détecter tôt les signaux d'une attaque hybride imminente permet de la contrer avant qu'elle ne cause des dommages irréversibles. Chaque État devrait ainsi élaborer un plan national de réponse aux menaces hybrides, incluant des exercices réguliers, afin de n'être ni surpris ni démuni le jour où il en sera la cible.

V. CELLULE DE VEILLE STRATEGIQUE ET SIGNAUX FAIBLES

Pour anticiper une guerre hybride, il est indispensable de détecter précocement les signaux faibles annonciateurs des crises à venir. Cela peut être la diffusion de nouveaux messages de propagande, l'arrivée de personnel paramilitaire étranger, ou tout autre indice inhabituel. La mise en place d'une cellule de veille stratégique dédiée, au sein par exemple du Ministère de la Défense

ou du Conseil national de sécurité, constitue une réponse appropriée. Cette cellule serait chargée de collecter, d'analyser et d'alerter sur les indicateurs précoces de menaces hybrides. En pratique, son fonctionnement obéirait aux principes suivants :

- La collecte multisources : la cellule doit recueillir l'information de manière large et diversifiée. Elle agrège des renseignements de sources ouvertes (OSINT) suivi des médias locaux, des réseaux sociaux, rapports d'ONG mais aussi des remontées du terrain via les forces de sécurité (comptes rendus des unités déployées, rapports des chefs locaux, attaches de défense dans les ambassades, etc.). Il est crucial d'intégrer également des sources non conventionnelles : par exemple, les ONG humanitaires ou missions religieuses présentes sur le terrain peuvent observer des signaux faibles avant les autorités. Une ONG médicale qui signale un afflux inhabituel de blessés par balle dans une zone minière isolée fournit potentiellement un indice d'accrochages impliquant une milice ou une SMP, alerte qui doit remonter à la cellule de veille.
- L'analyse et la fusion : au sein de la cellule, une équipe pluridisciplinaire d'analystes (officiers de renseignement, sociologues, data scientists, linguistes, etc.) traite et recoupe ces informations brutes. Elle utilise des outils analytiques modernes : logiciels de data mining pour détecter des tendances sur les réseaux sociaux (mots-clés djihadistes émergents, pics d'activité suspects) et SIG (systèmes d'information géographique) pour cartographier incidents et signaux sur le territoire. Le but est de distinguer le signal faible significatif du bruit de fond. Par exemple, vérifier si des incidents isolés de recrutement armé dans différentes provinces ne seraient pas liés ce qui pourrait révéler l'existence d'un réseau commun. Cette phase demande des protocoles rigoureux pour évaluer la fiabilité des sources et procéder à des validations croisées avant de conclure.
- La veille continue et réactive : la cellule doit idéalement opérer en mode 24/7 ou, à défaut, de façon très régulière. La veille stratégique n'est pas un exercice ponctuel mais un processus continu, vivant, mis à jour en permanence. Il s'agit de briser le cloisonnement sectoriel : la cellule doit pouvoir collaborer avec d'autres ministères si nécessaire (Intérieur, Affaires étrangères, Santé…) pour partager l'information pertinente sur des menaces hybrides qui, par essence, dépassent les silos institutionnels. Une

veille efficace implique aussi des réunions hebdomadaires pour faire le point sur les signaux collectés et ajuster le focus des recherches (par exemple, si un nouveau groupe Facebook extrémiste apparaît, décider de le surveiller de près).

- La diffusion et alerte : le travail de la cellule de veille aboutit à deux types de produits. D'une part, des bulletins périodiques (par exemple des notes stratégiques mensuelles) synthétisant les tendances émergentes et signaux faibles observés, à destination des décideurs (ministres, états-majors). D'autre part, la capacité de déclencher des alertes immédiates si un signal faible critique semble annoncer une crise imminente. Par exemple, si la veille détecte une coordination soudaine entre une milice locale et un groupe jihadiste voisin, elle doit émettre un bulletin d'alerte vers les autorités compétentes (armée, police) pour initier une action préventive sans délai. L'art de la diffusion consiste à sensibiliser sans affoler : communiquer le risque avec son degré d'incertitude, aux bonnes instances, afin qu'une réaction proportionnée soit engagée.
- L'organisation et partenariats : la cellule de veille pourrait être rattachée au Centre de renseignement de l'État, tout en travaillant en lien étroit avec le Centre de gestion des crises du gouvernement. Elle doit entretenir des canaux de partage avec des partenaires extérieurs : par exemple, l'Union Africaine dispose d'un Système continental d'alerte précoce (Continental Early Warning System, CEWS) pour prévenir les conflits la cellule nationale pourrait lui faire remonter ses informations et recevoir en retour des analyses régionales[12]. De même, des échanges avec le Centre d'excellence européen pour la lutte contre les menaces hybrides (Hybrid CoE à Helsinki) pourraient apporter une expertise internationale. Enfin, la cellule doit s'inscrire dans les réseaux d'échange d'information sécuritaire de la sous-région (conférences de renseignement de la CEEAC, etc.).

Malgré ces mécanismes, certains outils existants restent sous-utilisés. Par exemple, le CEWS de l'Union Africaine n'est pas pleinement exploité dans plusieurs contextes critiques[13]. Il importe donc que la cellule de veille nationale s'interface activement avec ces systèmes d'alerte régionaux ou internationaux, afin d'en tirer

[12] African Union, Continental Early Warning System (CEWS) Annual Report. Addis-Abeba, 2020.
[13] ADANGA S., Signaux faibles et veille stratégique : anticiper les menaces hybrides, Note pédagogique, CHESD-Kinshasa, 2023.

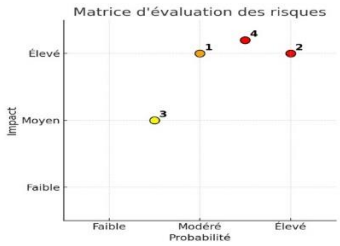
tout le potentiel. In fine, l'instauration d'une telle cellule de veille stratégique aidera à institutionnaliser l'anticipation : l'État passera d'une posture réactive à une posture proactive vis-à-vis des menaces hybrides émergentes.

VI. ANALYSE DE RISQUES STRATÉGIQUES : MATRICE IMPACT/PROBABILITÉ

Anticiper signifie aussi hiérarchiser les menaces pour concentrer l'effort là où le risque est le plus critique. Pour ce faire, on peut utiliser une matrice Impact vs. Probabilité : chaque scénario de menace est évalué en termes de gravité de son impact et de vraisemblance de son occurrence. Le positionnement dans la matrice permet de dégager un niveau de risque (par exemple, risque critique si impact et probabilité sont élevés, risque modéré si un des deux est faible, etc.) et oriente la priorité d'action. La matrice ci-dessous illustre cet exercice avec quatre événements stratégiques potentiels pour un pays d'Afrique centrale, classés de façon qualitative en probabilité et impact, accompagnés de la priorité d'action suggérée pour chacun :

Événement stratégique	Probabilité	Impact	Niveau de risque (qualitatif)
1. Cyberattaque contre des infrastructures énergétiques	Modérée (éventualité occasionnelle)	Élevé (paralysie possible)	Risque élevé Impact critique malgré probabilité moyenne
2. Expansion d'un groupe djihadiste en zone épargnée	Élevée (tendance régionale avérée)	Élevé (déstabilisation sécuritaire)	Risque critique Probabilité et impact très élevés
3. Intervention clandestine d'une SMP dans une crise locale	Faible à modérée (cas rares et ciblés)	Moyen (dégradation locale limitée)	Risque modéré Menace circonscrite géographiquement
4. Sécheresse prolongée avec crises migratoires	Élevée (choc récurrent attendu)	Élevé (crise humanitaire majeure)	Risque critique Probabilité et impact très élevés

Source : Conception de l'auteur.



VI. 1. Cyberattaque contre les infrastructures énergétiques

Ce risque est évalué à probabilité modérée les attaques cyber sophistiquées existent dans le monde, mais visent surtout les pays très connectés ; toutefois la vulnérabilité augmente avec la numérisation des réseaux électriques, y compris en Afrique centrale. L'impact, lui, serait élevé : une cyberattaque réussie plongerait des régions entières dans le noir, perturbant gravement l'économie et mettant potentiellement des vies en danger (pannes d'électricité dans les hôpitaux, etc.). La priorité d'action face à ce risque est jugée élevée. Il faut renforcer dès maintenant la cybersécurité des infrastructures critiques : mise en place d'équipes de réponse aux incidents (CERT), audits de sécurité réguliers des systèmes de contrôle industriel (SCADA), formation du personnel à l'hygiène cyber.

Il convient également de prévoir des plans de continuité d'activité (générateurs de secours, procédures manuelles de repli) pour pouvoir réagir en cas d'attaque réussie. Ce risque a une portée nationale et un impact potentiellement catastrophique, mais il est un peu moins fréquent qu'une attaque terroriste classique ; la priorité réside donc surtout dans la prévention : investir préventivement dans la résilience cyber avant qu'une catastrophe ne survienne.

VI. 2. Expansion d'un groupe djihadiste dans une région jusque-là épargnée

La probabilité de cet événement est jugée très élevée, car l'expérience récente montre la dynamique d'essaimage rapide du djihadisme. Le Sahel en fournit un exemple éloquent : partis du nord du Mali, des groupes affiliés à Al-Qaïda ou à Daech ont essaimé au Burkina Faso et menacent maintenant des pays du golfe de Guinée où le djihadisme était jusqu'alors absent. De même, l'apparition de filiales djihadistes en RDC (les ADF dans le Nord Kivu) illustre la capacité de ces mouvements à s'étendre géographiquement. L'impact d'une telle expansion serait très élevé : voir une nouvelle région basculer dans le terrorisme ouvrirait un front

de conflit supplémentaire, provoquerait une crise humanitaire et ferait reculer le développement local.

Ce type d'essaimage peut ébranler même des États jusqu'ici stables. La priorité d'action est donc critique (maximale). Il faut prévenir l'implantation djihadiste avant qu'elle n'atteigne un point de non-retour. Concrètement : renforcer le renseignement aux frontières et la surveillance des zones limitrophes pour détecter l'infiltration de prédicateurs ou de combattants ; mettre en place des programmes de contre-radicalisation (impliquer les chefs religieux locaux, mener des campagnes d'information) dès les premiers signes de propagation idéologique ; et coordonner régionalement la réponse sécuritaire (patrouilles conjointes aux frontières, échanges d'informations sur les mouvements de groupes armés). Si malgré tout un groupe commence à s'implanter, une réaction militaire rapide est nécessaire avant qu'il ne se fortifie, de préférence avec l'appui d'organisations régionales ou de l'ONU.

L'histoire des dernières décennies montre qu'à chaque fois qu'un sanctuaire terroriste se crée dans une nouvelle zone (Somalie, nord du Mali, nord-est du Nigéria…), il devient très coûteux à éliminer par la suite. D'où l'impératif d'une action anticipative énergique.

VI. 3. Intervention clandestine d'une SMP dans une crise politique locale

La probabilité globale est estimée faible à modérée ce genre d'ingérence requiert des conditions spécifiques (intérêt d'une grande puissance pour un pays donné, accord tacite d'une partie prenante locale). Néanmoins, on a vu des cas récents : la présence de mercenaires étrangers au Mozambique pour combattre les insurgés au Cabo Delgado, ou le déploiement du groupe Wagner en Centrafrique lors de la crise de 2017-2018. L'impact d'une SMP clandestine est en général moyen et souvent limité à la zone de conflit où elle opère : elle peut exacerber la violence locale et prolonger le conflit, mais son effet reste moindre qu'une insurrection nationale bien implantée.

Cependant, si la SMP soutient un régime impopulaire, elle peut envenimer la guerre civile et accroître le ressentiment populaire. La priorité d'action est modérée. Il s'agit avant tout de surveiller et encadrer ce risque. Les autorités nationales doivent détecter en amont les signes d'arrivée d'une SMP

(renseignement sur les vols entrants d'étrangers, surveillance des contrats de sécurité passés, etc.) et diplomatiquement décourager toute ingérence de ce type.

Sur le plan interne, il convient de renforcer les capacités locales (armée, police) afin de réduire l'attrait pour une aide militaire extérieure. Si malgré tout une SMP agit clandestinement, la réponse peut être diplomatique (exposer son rôle sur la scène internationale pour faire pression sur l'État qui la sponsorise) et juridique (interdire son accès aux zones de conflit, menacer de poursuites pour mercenariat selon les lois nationales ou internationales applicables). Un défi majeur est celui de l'attribution : réunir les preuves de l'implication de la SMP afin de légitimer la réponse de l'État, à l'image de la démarche de la France au Mali vis-à-vis de Wagner. Adanga souligne qu'il faut absolument intégrer le suivi des SMP dans l'analyse stratégique actuelle. En anticipant ce risque par exemple en élaborant des scénarios du type « SMP soutenant un coup d'État » et en planifiant les réactions adéquates on peut le contenir avant qu'il ne mine gravement la souveraineté nationale.

VI. 4. Sécheresse prolongée avec conséquences migratoires

Dans de nombreuses régions d'Afrique centrale (et de l'Est), ce risque est malheureusement très probable à moyen terme en raison du changement climatique. Des épisodes de sécheresse de plus en plus fréquents et intenses poussent des millions de personnes vers la famine et le déplacement forcé la Corne de l'Afrique connaît actuellement une sécheresse historique qui illustre cette menace.

L'impact est élevé : d'abord humanitaire (pénuries alimentaires, malnutrition, mortalité), mais aussi socio-politique (migration massive de populations rurales vers les villes ou vers d'autres pays, créant des tensions et potentiellement alimentant des conflits pour les ressources). Des migrations désespérées dues à la faim peuvent déstabiliser les régions d'accueil, voire servir de terreau à l'extrémisme les groupes terroristes exploitant souvent le désarroi des déplacés climatiques pour recruter. La priorité d'action est critique. Ce type de menace, à la fois lente et inexorable, exige une stratégie de résilience et d'adaptation plutôt qu'une solution ponctuelle.

Il faut mettre en œuvre des politiques d'adaptation climatique : irrigation et agriculture résistante à la sécheresse, gestion durable de l'eau, pour atténuer

l'impact sur les communautés rurales. Renforcer les mécanismes d'alerte précoce en matière de sécurité alimentaire permettra de déclencher à temps des plans d'urgence (constitution de stocks stratégiques de céréales, programmes du PAM).

Il convient aussi de développer des filets sociaux pour les populations affectées (transferts monétaires, travaux publics locaux rémunérés) afin d'éviter les migrations forcées. En parallèle, sur le plan diplomatique, préparer des accords de gestion des flux migratoires avec les pays voisins en cas de crise majeure pourrait prévenir des tensions ultérieures. Ce risque montre que la guerre hybride peut exploiter des chocs a priori naturels : une crise climatique mal gérée offre une opportunité à des acteurs malveillants (groupes armés, propagandistes) pour aggraver l'instabilité. La réponse doit donc lier étroitement sécurité et développement durable.

L'analyse ci-dessus permet de prioriser l'action stratégique. Manifestement, le risque d'expansion djihadiste et celui de sécheresse conflictuelle sont les plus critiques à la fois très probables et ravageurs et appellent des efforts prioritaires multiples (sécuritaires mais aussi socio-économiques). Le risque cyber est potentiellement très grave mais d'une occurrence un peu moindre en Afrique centrale : il appelle une priorité intermédiaire, centrée sur la prévention technologique.

Le risque SMP clandestine est plus localisé et d'ordre politico-diplomatique : il doit être surveillé, sans mobiliser autant de ressources que les menaces précédentes. Cette hiérarchisation doit aider les décideurs à orienter l'allocation des ressources et l'attention stratégique : par exemple, intensifier dès maintenant la coopération antiterroriste et les programmes anti-sécheresse, sans pour autant négliger de renforcer la cybersécurité ni de surveiller l'activité des SMP dans la région.

VII. PLAN DE RESILIENCE SANITAIRE POST-PANDEMIQUE : ENSEIGNEMENTS DU COVID-19

La pandémie de COVID-19 a mis en lumière la nécessité pour les systèmes de santé de disposer d'une résilience stratégique forte, c'est-à-dire de la capacité non seulement de résister au choc, mais aussi de s'adapter et de se transformer pour mieux faire face aux crises futures.

Un plan d'anticipation post-COVID doit donc intégrer ces trois dimensions résister, s'adapter, se transformer chacune étant assortie d'actions concrètes et d'indicateurs de suivi permettant de mesurer les progrès accomplis. Nous présentons ci-après un cadre d'actions inspiré des leçons de COVID-19, articulé autour de ces trois volets complémentaires (courant terme, moyen terme et long terme) pour renforcer la résilience sanitaire.

VII. 1. Résister (capacité d'absorption du choc immédiat)

Il s'agit de renforcer les défenses du système de santé afin qu'il puisse encaisser une nouvelle crise sanitaire soudaine (épidémie, afflux massif de malades) sans s'effondrer. Les a*ctions "résister" :*

- Renforcement des stocks stratégiques : constituer des réserves nationales suffisantes d'équipements de protection individuelle (masques, gants), de médicaments essentiels et de matériel critique (respirateurs, bouteilles d'oxygène). Par exemple, prévoir l'équivalent de 6 mois de consommation en masques FFP2 pour les soignants, et mettre en place des entrepôts régionaux permettant un déploiement rapide de ces ressources en cas d'urgence.
- Capacité hospitalière d'urgence : augmenter le nombre de lits de réanimation disponibles et préparer des plans de surge capacity (par exemple, pouvoir doubler le nombre de lits critiques en 15 jours). Former à l'avance un vivier de personnel de réserve (médecins retraités volontaires, étudiants en dernière année mobilisables) pour renforcer les équipes en cas de pic sanitaire. Prévoir le déploiement d'hôpitaux de campagne modulaires dans les foyers d'épidémie pour absorber le surplus de patients.
- Systèmes d'alerte précoce : améliorer la détection rapide des menaces sanitaires via un réseau de surveillance épidémiologique jusqu'au niveau local (par exemple, désigner des centres de santé sentinelles chargés de signaler toute hausse inhabituelle de cas de syndrome grippal). Connecter ce réseau aux systèmes d'alerte internationaux (OMS, CDC Afrique) pour recevoir en temps réel les alertes mondiales et déclencher rapidement la réponse nationale appropriée.

Sur les indicateurs de résistance, il se dégage ce qui suit : Taille des stocks d'urgence (ex. nombre de masques en réserve, doses d'antiviraux disponibles) et

taux de rotation de ces stocks (pour éviter la péremption des produits) ; Taux d'occupation des lits critiques en temps normal contre en période de pic (pour mesurer la marge de capacité disponible). L'objectif pourrait être de <80% d'occupation en période de pic, afin de conserver une marge de manœuvre ; Délai de réaction aux alertes : temps entre la détection d'un signal épidémique et l'activation du plan d'urgence. Par exemple, viser <48h pour enclencher la cellule de crise et déployer les premières mesures suite à une alerte locale ; et ratio de personnel de réserve par rapport au personnel actif : indicateur de la ressource humaine mobilisable en cas de crise (par ex., un ratio de 0,2 signifierait 20 réservistes pour 100 soignants actifs).

VII. 2. S'adapter (capacité d'ajustement en cours de crise et à moyen terme)

C'est la faculté du système de santé à ajuster son fonctionnement en cours de crise et à tirer des leçons de la crise pour améliorer ses procédures dans le moyen terme. Les Actions "s'adapter" :

- Flexibilité organisationnelle : instituer des plans de continuité des soins pour que, en cas de pandémie, l'offre de santé courante (pour les autres maladies) soit maintenue autant que possible. Par exemple, développer la télémédecine pour le suivi des patients chroniques quand les déplacements sont limités, afin d'éviter les interruptions de traitement. Former les soignants à pouvoir adapter leurs rôles : un infirmier de bloc opératoire pourrait être redéployé en réanimation si les chirurgies non urgentes sont déprogrammées.
- Adaptation des protocoles : mettre à jour régulièrement les protocoles cliniques de prise en charge des maladies émergentes, en s'appuyant sur l'expérience Covid-19. Par exemple, élaborer à l'avance des guides thérapeutiques pour une possible prochaine pandémie de grippe sévère. Institutionnaliser des exercices de simulation de crise sanitaire chaque année afin de tester et améliorer les protocoles (par ex. exercice de distribution de vaccins de masse, exercice de confinement localisé).
- Apprentissage et feedback : créer un comité post-crise chargé d'analyser la gestion de la pandémie de COVID-19 (ce qui a fonctionné ou non) et de recommander des changements. Intégrer ces retours d'expérience dans la formation continue des cadres de santé et des gestionnaires. Par exemple, si un manque de coordination entre hôpitaux a été constaté, mettre en

place une plateforme numérique de pilotage centralisé des lits disponibles accessible à tous les établissements.

- Renforcement communautaire : impliquer la communauté et la santé de base dans l'adaptation. Former des agents de santé communautaires capables de relayer les campagnes de prévention et d'effectuer un premier tri des cas dans les villages en cas de nouvelle épidémie. Cette capillarité jusqu'au niveau local permet d'ajuster la riposte aux réalités du terrain (langues locales, pratiques culturelles) et d'éviter d'engorger inutilement les hôpitaux de niveau supérieur.

Sur les indicateurs d'adaptation, on note :

- Temps de mise à jour des protocoles après l'émergence d'une nouvelle menace : délai pour produire des directives officielles temporaires (objectif indicatif : <1 semaine pour des recommandations provisoires, quitte à affiner par la suite).
- Taux de continuité des services essentiels en période de crise : par exemple, nombre de consultations prénatales réalisées pendant la pandémie comparé à la normale, afin de mesurer dans quelle mesure les soins de base ont été maintenus.
- Nombre d'exercices de simulation réalisés par an et existence de leurs rapports d'évaluation (viser au moins un exercice national et plusieurs exercices régionaux par an).
- Couverture de la télémédecine : proportion des structures de santé équipées pour la téléconsultation et l'échange de dossiers à distance (un taux élevé indique une meilleure adaptabilité en cas de confinement) .
- Satisfaction du personnel après la crise : mesurer via des enquêtes si les soignants estiment avoir eu les outils et informations nécessaires pour s'adapter (une amélioration de ce ressenti dans le temps indiquerait une meilleure préparation).

VII. 3. Se transformer

Il s'agit ici de tirer parti de la crise pour effectuer des réformes profondes, en « rebâtissant en mieux » le système de santé afin qu'il soit plus performant en temps normal et plus robuste face aux futures crises. Les actions "se transformer" :

- Investissement soutenable et local : accroître de manière pérenne la part du budget national allouée à la santé afin d'atteindre les normes internationales (par ex. viser l'objectif de 15% du budget national dédié à la santé, conformément à la Déclaration d'Abuja). Cet effort financier doit servir à améliorer les infrastructures (hôpitaux, laboratoires) et à former/embaucher du personnel, pour résorber la pénurie critique de médecins et d'infirmiers. La transformation passe aussi par le développement de la production locale d'intrants stratégiques : encourager la fabrication nationale de certains produits de santé essentiels (masques, médicaments génériques, vaccins). Par exemple, l'Institut Pasteur de Dakar a lancé une initiative de production de vaccins COVID en Afrique ; ce genre de projet doit être démultiplié pour réduire la dépendance extérieure[14].
- Renforcement de la santé publique et de la prévention : réorienter le système en passant d'un modèle centré sur le curatif hospitalier à un modèle plus préventif et holistique. Après COVID, investir davantage dans les programmes de santé publique : vaccination systématique, lutte contre les maladies non transmissibles (obésité, diabète…) qui alourdissent le bilan des pandémies. Intégrer la santé dans toutes les politiques (approche One Health liant santé humaine, animale et environnementale). Par exemple, créer une cellule permanente One Health chargée de surveiller les zoonoses (afin de détecter un nouveau virus avant qu'il ne se propage à l'homme).
- Transformation digitale du système de santé : la crise COVID a montré l'importance cruciale des données et du numérique. Il faut accélérer la numérisation des systèmes de santé : dossiers médicaux électroniques interopérables, systèmes d'information reliés du centre aux périphéries, utilisation de l'IA pour détecter rapidement l'apparition de foyers épidémiques (par exemple en analysant en temps réel les requêtes Internet de symptômes). La mise en place d'une plateforme nationale de données de santé permettrait un suivi épidémiologique plus fin et une meilleure coordination en temps de crise.
- Gouvernance anticipative en santé : instituer au ministère de la Santé une cellule d'anticipation stratégique dédiée aux risques sanitaires. Celle-ci

[14] Institut Pasteur de Dakar, Vers une production locale de vaccins en Afrique, Rapport stratégique, Dakar, 2021.

élaborerait régulièrement des scénarios de crises (pandémie de grippe, flambée Ebola, bioterrorisme, etc.) et testerait la résilience du système face à chacun. Chaque année, elle pourrait publier un rapport de préparation avec des recommandations aux hôpitaux et aux autres ministères concernés (car la résilience sanitaire dépend aussi de l'énergie, des transports, etc.). Il s'agit d'une transformation culturelle : passer d'une attitude purement réactive à une attitude proactive et planificatrice face aux risques sanitaires.

En ce qui concerne les indicateurs de transformation, on décompte :

- Pourcentage du PIB ou du budget national alloué à la santé, pour mesurer l'effort financier soutenu. Objectif : augmentation régulière jusqu'à atteindre le seuil cible (ex. 15%).
- Capacité locale de production de produits de santé stratégiques : nombre de vaccins ou % de médicaments essentiels produits localement. Par exemple, viser 50% de médicaments génériques produits dans le pays d'ici 5 ans.
- Taux de couverture vaccinale annuelle et capacité de vaccination en cas de nouvel agent pathogène : un système transformé devrait être capable de vacciner >80% de sa population contre une nouvelle maladie en moins d'un an, indicateur clé de performance post-crise.
- Indice de sécurité sanitaire globale pour le pays (tels que le Global Health Security Index), avant et après mise en œuvre du plan, afin de mesurer l'amélioration de ses capacités de détection, de réponse rapide, de chaîne logistique, etc. (La République Démocratique du Congo, par exemple, présentait encore récemment de faibles scores de préparation sanitaire selon l'indice GHSI de 2021 d'où l'urgence d'améliorer ces indicateurs[15].
- Existence et activité de la cellule prospective sanitaire : nombre de scénarios élaborés, nombre de recommandations adoptées par le gouvernement suite à ces travaux. On peut par exemple viser que 80% des hôpitaux du pays réalisent un audit de résilience dans l'année suivant un exercice national de crise.

[15] Global Health Security Index, Global Preparedness for Health Emergencies Country Profile and Index Scores, Johns Hopkins University / Nuclear Threat Initiative, 2022.

En combinant ces trois volets (résister, s'adapter, se transformer), le plan post-pandémique assure une amélioration à court, moyen et long terme de la résilience sanitaire nationale. Par exemple, résister signifie être capable d'absorber une troisième vague épidémique sans confinement généralisé ; s'adapter signifie maintenir la prise en charge du paludisme et de la maternité pendant cette vague grâce à la télésanté et à la reconfiguration des services ; se transformer signifie qu'à l'issue de la crise, le pays dispose d'hôpitaux plus nombreux et mieux équipés, d'un réseau de cliniques mobiles et d'une capacité de produire localement des tests ou vaccins diagnostiques. La clé est d'assurer un suivi serré via les indicateurs mentionnés : un tableau de bord de la résilience sanitaire doit être suivi trimestriellement par le ministère de la Santé. Ainsi, on pourra vérifier que les leçons de COVID-19 ont bien été retenues et traduites en progrès concrets, et que le pays est désormais activement préparé aux menaces sanitaires de demain plutôt que de les subir passivement.

VIII. GOUVERNANCE ANTICIPATIVE DANS LES ENTREPRISES MINIÈRES EN ZONE FRAGILE

Une entreprise minière opérant dans une zone fragile (marquée par des conflits locaux, la présence de groupes armés, une instabilité politique) doit adopter une gouvernance anticipative. Cela signifie intégrer systématiquement l'anticipation stratégique dans sa gestion afin de prévenir les crises et d'assurer la pérennité de ses activités.

Concrètement, cela implique plusieurs axes d'actions, la mobilisation d'acteurs variés, et une prise en compte spécifique des risques liés aux SMP et au djihadisme. L'objectif est que l'entreprise ne soit plus un simple spectateur ou une victime collatérale des troubles environnants, mais qu'elle devienne un acteur stratégique conscient de l'écosystème conflictuel où elle opère, capable d'en atténuer les dangers par l'anticipation. Les actions pour mettre en place une gouvernance anticipative sont entre autre :

- Institutionnaliser la veille et la prospective : la compagnie devrait se doter en interne d'une unité de veille stratégique (ou désigner un Chief Risk Officer dédié) chargée de surveiller en permanence l'environnement socio-politique et sécuritaire. Cette unité collecte des informations sur les tensions communautaires autour du site minier, les évolutions politiques du

pays, l'activité des groupes armés dans la région, etc. Elle élabore régulièrement des scénarios d'évolution (coup d'État, conflit local, nouvelles réglementations) et conçoit des plans de contingence correspondants. Par exemple, imaginer ce qui se passerait si un groupe djihadiste s'implantait à 100 km de la mine, ou si l'État faisait appel à une SMP étrangère pour une opération à proximité puis prévoir les mesures à prendre dans ces cas de figure. Ces scénarios internes permettront à l'entreprise d'avoir préparé des réponses (évacuation du personnel, sécurisation du site, etc.) plutôt que de subir les événements ;

- Planification et gestion intégrée des risques : sur la base de cette veille, intégrer les risques identifiés dans la planification stratégique de l'entreprise. Cela signifie inclure des plans d'urgence dans le business plan : plan d'évacuation du personnel expatrié en cas de menace grave, diversification des routes d'exportation du minerai si la route principale devient dangereuse, constitution de fonds d'urgence pour financer un éventuel arrêt temporaire de l'activité, etc. La gouvernance anticipative incite à allouer des ressources avant la crise. Par exemple, investir dans une piste d'atterrissage privée pour l'évacuation sanitaire/sécuritaire peut sembler coûteux, mais pourrait sauver l'activité en cas de routes terrestres bloquées ou minées. En résumé, intégrer les risques majeurs (sécurité, instabilité politique) dans la stratégie d'entreprise permet de prendre à l'avance les mesures qui préserveront la continuité des opérations le moment venu ;
- Engagement proactif avec les communautés et les autorités : une entreprise anticipative n'attend pas que la situation dégénère pour agir localement. Elle met en place des programmes de développement communautaire (santé, éducation, accès à l'eau) profitant aux populations avoisinantes, afin de réduire les frustrations et de renforcer l'acceptation sociale du projet minier. Cela diminue les risques de sabotage ou de collusion entre habitants et groupes armés hostiles. Par ailleurs, l'entreprise établit dès que possible un dialogue structuré avec les autorités locales et nationales et les forces de sécurité. Par exemple, signer un protocole d'accord avec l'armée ou la police locale pour l'alerte mutuelle en cas de menace, offrir un soutien (équipements, renseignements) en échange d'une protection officielle du site. Cet engagement multi-acteurs

correspond à l'idée d'associer le secteur privé à la gestion préventive des risques, approche d'ores et déjà recommandée par le Pr Adanga[16] ;

- Adaptation continue et flexibilité : la gouvernance anticipative suppose une mise à jour régulière des stratégies. L'entreprise doit instaurer une revue périodique des risques (par exemple trimestrielle) où elle évalue si de nouveaux signaux faibles nécessitent d'ajuster ses mesures. Par exemple, si l'actualité montre une montée de l'insécurité dans la province, peut-être faut-il renforcer temporairement la sécurité du site, retarder une phase de projet, ou au contraire accélérer l'extraction de stock minier tant que c'est possible, pour réduire l'exposition future. Cette agilité décisionnelle, appuyée par des données prospectives, permet à l'entreprise de devancer les crises plutôt que d'y réagir en panique lorsque celles-ci éclatent.

Les acteurs internes et externes à associer sont les suivants :

- Interne : la direction générale de l'entreprise doit impulser la démarche anticipative et la considérer comme stratégique (et non comme un simple coût). Les responsables HSE (Hygiène-Sécurité-Environnement), qui gèrent déjà des risques opérationnels, peuvent élargir leur périmètre à la géopolitique et travailler étroitement avec l'équipe de veille stratégique. Le responsable sûreté du site minier sera en première ligne pour déployer les mesures de protection et doit être intégré dans ce dispositif. Les représentants du personnel doivent également être partie prenante, via par exemple des formations du personnel aux protocoles d'urgence et des comités locaux permettant aux employés de faire remonter leurs préoccupations. Enfin, les actionnaires ou le conseil d'administration doivent être sensibilisés et impliqués, pour soutenir les investissements préventifs décidés il faut parfois convaincre la maison-mère qu'investir maintenant dans la sécurité évitera des pertes bien plus grandes plus tard.
- Externe : les autorités locales et nationales (préfet, gouverneur, ministères de tutelle) leur appui est crucial pour légitimer les actions de l'entreprise et les coordonner avec les forces de l'ordre. Les communautés locales et chefs traditionnels en zone fragile, ignorer la population serait une erreur fatale. Inclure des représentants des villages voisins dans un comité de

[16] ADANGA S., « Gouvernance anticipative et sécurité en Afrique centrale », dans *Revue africaine de stratégie,* 2023.

liaison permet de recevoir tôt les doléances, de désamorcer les conflits sociaux, et même d'obtenir des renseignements informels sur ce qui se trame (rumeurs de bandes armées, etc.). Les organisations internationales et ONG par exemple, collaborer avec des ONG spécialisées en médiation de conflit ou développement peut aider à apaiser les tensions autour de la mine. De même, si l'ONU ou l'UA ont des missions de paix sur place (type MONUSCO en RDC), elles peuvent être des partenaires pour partager analyses et alertes. Les autres entreprises de la région via un réseau ou une association professionnelle : une gouvernance anticipative peut être en partie mutualisée. Plusieurs sociétés minières dans un même pays pourraient cofinancer ensemble une cellule d'analyse des risques pays, ou partager des informations de sécurité pertinentes. Enfin, faire appel périodiquement à des experts extérieurs (anciens diplomates, cabinets de conseil en risques) peut offrir un regard neuf et indépendant sur les vulnérabilités et les plans d'action.

- Intégration des risques liés aux SMP et au djihadisme : ces risques spécifiques doivent être explicitement inclus dans l'analyse stratégique de l'entreprise, car ils peuvent impacter directement ses opérations.

Sur les SMP, l'entreprise doit décider si elle-même recourt à une SMP pour sa sécurité, et si oui sous quelles conditions (choisir une société réputée, respectueuse des droits, et s'assurer d'une coordination étroite avec l'État). D'autre part, elle doit surveiller l'éventuelle présence de SMP tierces dans son environnement. Par exemple, si le gouvernement engage une SMP étrangère pour opérer dans la région, cela peut entraîner des interactions avec le site minier (positives ou négatives).

Il faut alors établir un protocole de coopération avec cette SMP, ou au minimum la contacter pour clarifier les rôles et éviter les incidents. Si à l'inverse une SMP opère au service d'un acteur illégal (ex. mercenaires soutenant une milice locale), l'entreprise doit redoubler de prudence c'est un signal d'alerte majeur. Des scénarios du type « SMP impliquée dans un coup d'État » doivent être envisagés : que faire si demain une SMP prend le contrôle de la capitale et que le cadre légal change ?

L'entreprise doit prévoir comment réagir (mise en sécurité du personnel expatrié, gel de certaines opérations jusqu'à clarification, etc.). Le cours du Pr

Adanga mentionne que l'instabilité politique liée à la présence de SMP dans les zones minières est un risque à examiner sérieusement. En RDC par exemple, des tentatives de déploiement de SMP aux abords de sites miniers ont été rapportées ; une compagnie minière anticipative s'en montrera attentive et informera les autorités si elle constate de telles ingérences. En résumé, intégrer ce risque signifie surveiller activement l'activité des SMP dans l'environnement de l'entreprise et définir des lignes rouges claires (par ex. cesser temporairement l'exploitation si le périmètre passe sous le contrôle d'une SMP hors cadre légal, afin de ne pas cautionner l'illégalité).

Sur le djihadisme, l'entreprise doit cartographier la menace terroriste dans son évaluation des risques. Cela inclut l'idéologie (y a-t-il des discours hostiles aux intérêts de l'entreprise rhétorique anti-occidentale par exemple susceptibles de la désigner comme cible ?) et l'activité opérationnelle (groupes armés djihadistes opérant à distance raisonnable du site, modes opératoires connus comme l'enlèvement d'employés, le sabotage d'infrastructures, l'attaque de convois). Elle devra intégrer ces données dans ses plans de sécurité : former ses gardes aux scénarios d'attaque armée, fortifier certains points névralgiques, et éventuellement contribuer au développement local (emplois pour les jeunes, soutien aux écoles coraniques officielles) afin de réduire l'attrait des populations locales pour les groupes extrémistes.

Un volet important est la coordination avec les forces antiterroristes nationales : l'entreprise peut fournir un appui logistique (par exemple, autoriser l'installation d'un poste militaire à un coin de sa concession pour surveiller la zone) ou des renseignements, en échange d'une protection accrue du site. Il faut noter que les groupes djihadistes ont déjà ciblé des sites miniers en Afrique : au Burkina Faso, l'attaque du convoi de la mine de Boungou (opérée par Semafo) en 2019 a fait 37 morts, montrant que ces groupes voient dans les entreprises minières des cibles à haute valeur (pour les rançons, le matériel saisi, ou l'impact médiatique). Ce type d'événement doit donc faire partie des scénarios envisagés. Ainsi, des exercices de crise internes pourraient simuler une attaque terroriste ou un kidnapping pour tester la réaction de l'entreprise et corriger les failles à l'avance.

En plus de ces points, la gouvernance anticipative implique une communication soignée autour de ces enjeux. L'entreprise doit entretenir sa légitimité locale : montrer qu'elle agit pour le bien-être de la région et qu'elle n'est

pas un acteur prédateur uniquement intéressé par le profit. Cela peut la protéger en partie des narratifs djihadistes ou anti-étrangers. Par exemple, si une entreprise minière communique régulièrement sur ses projets communautaires et ses efforts environnementaux, il sera plus difficile pour des propagandistes de la dépeindre comme "l'ennemi à chasser".

Sur le plan international, si elle subit l'impact d'une SMP ou d'un groupe terroriste, elle doit avoir documenté la situation pour pouvoir mobiliser ses soutiens extérieurs (ambassades, chambres de commerce) et faire pression sur les gouvernements compétents le cas échéant (ex. demander des sanctions contre un État qui enverrait des mercenaires, ou une aide militaire contre un groupe terroriste menaçant l'économie locale).

En synthèse, une entreprise minière en zone fragile doit se comporter non plus en simple exploitant passif, mais en acteur stratégique conscient de son écosystème conflictuel. Anticiper lui permettra d'éviter d'être prise de court par les événements. Comme le dit le Pr Adanga : « celui qui ne surveille pas les SMP dans son analyse stratégique se prive d'un facteur clé d'explication de nombreuses crises » cela vaut également pour le terrorisme.

En associant de manière proactive tous les acteurs (État, communautés, experts) et en intégrant ces menaces dans sa gouvernance quotidienne, l'entreprise accroîtra sa résilience. Elle sera capable de prévenir certaines crises (en désamorçant les tensions sociales naissantes), de réagir efficacement à celles qu'elle ne peut éviter (plan d'urgence opérationnel en cas d'attaque d'un de ses convois, par exemple) et même de contribuer positivement à la stabilité de la zone par son influence économique et sociale.

Cette approche de gouvernance anticipative, encore nouvelle, deviendra sans doute un standard pour les industries extractives opérant dans des zones à hauts risques. En effet, les exemples passés montrent que lorsqu'un investisseur privé agit isolément sans vision à long terme, il finit soit par quitter précipitamment le pays en perdant son investissement, soit involontairement par nourrir le conflit. À l'inverse, une entreprise qui planifie sur 10-20 ans en intégrant l'anticipation stratégique peut devenir un acteur résilient et stabilisateur, au bénéfice mutuel de son activité et du développement local.

En synthèse, l'exploitation minière en zones à faible gouvernance est un talon d'Achille pour la stabilité de l'Afrique centrale. Cette section examine comment promouvoir une « gouvernance anticipative » dans les entreprises extractives opérant en zone fragile (comme l'est de la RDC, riche en minerais stratégiques). On y discute du rôle que peuvent jouer les compagnies minières pour réduire les risques de conflit : programmes de développement communautaire pour éviter les frustrations locales, partenariats avec les forces de sécurité pour une protection des sites qui n'alimente pas les tensions (ex : éviter de recourir à des gardes privés non contrôlés), mécanismes de traçabilité des minerais pour couper la finance des groupes armés, etc. L'exemple de certaines initiatives en RDC (comme la certification ITSCI pour l'étain, ou les zones "vertes" sans conflit au Sud-Kivu) est évoqué.

L'idée directrice est que le secteur privé a aussi sa part de responsabilité et d'intérêt dans l'anticipation stratégique : une entreprise minière proactive peut agir en vigie (détecter des signes de montée d'insécurité), en acteur de paix (investir dans le social local) et en relais d'alerte auprès de l'État. Cette approche whole-of-society est présentée comme complémentaire à l'approche étatique.

CONCLUSION

Les menaces hybrides constituent aujourd'hui un défi majeur pour la stabilité des États d'Afrique centrale. Ces menaces, en combinant habilement actions militaires, ingérence indirecte, subversion informationnelle et exploitation des faiblesses systémiques, mettent à l'épreuve la capacité de réaction de ces États.

Face à un adversaire diffus, souvent non déclaré, et à des attaques qui visent simultanément le champ militaire, le cyberespace et le tissu social, une approche classique de la sécurité nationale ne suffit plus. La situation actuelle dans l'est de la RDC en est l'illustration tragique : un mélange d'acteurs externes et internes y mène une agression multiforme qui dépasse les schémas traditionnels de la guerre. Il faut donc innover dans la façon de penser et d'organiser la défense et la résilience.

Cette étude a mis en évidence plusieurs axes d'amélioration. D'une part, il est crucial de réformer le système de sécurité pour le rendre plus intégré et adaptable : décloisonner les agences, renforcer le renseignement et le piloter de manière unifiée, développer des unités spécialisées (cyberdéfense, communication

stratégique) et anticiper les menaces plutôt que de simplement y réagir. D'autre part, la réponse aux guerres hybrides ne peut pas reposer sur le seul secteur de la défense : c'est l'ensemble de la société qu'il convient de rendre plus résiliente et plus consciente.

L'éducation aux médias, le renforcement de l'unité nationale, la réduction des vulnérabilités socio-économiques qui alimentent les conflits sont autant de chantiers à mener de front. Par exemple, comme le souligne le PNUD[17], le développement inclusif et la réduction des inégalités diminuent les frustrations sur lesquelles capitalise l'extrémisme violent (UNDP, 2022)[18]. Autrement dit, investir dans l'éducation, la santé et la cohésion sociale est une composante à part entière de la lutte contre les menaces hybrides.

En matière d'anticipation stratégique, nous avons préconisé plusieurs outils concrets : cellules de veille pour détecter les signaux faibles, scénarios prospectifs pour guider l'action, matrices de risques pour hiérarchiser les priorités, etc. Ces dispositifs doivent maintenant être institutionnalisés. Il importe que les gouvernements (et même les grandes entreprises, comme illustré dans le cas du secteur minier) adoptent une culture de l'anticipation. Cela passe par la création d'unités dédiées à la prospective, la formation de spécialistes, l'intégration de la planification d'urgence dans toutes les politiques publiques. Par exemple, au ministère de la Santé, mettre en place une cellule de prospective sanitaire permettra de suivre les indicateurs de préparation et d'éviter qu'une crise comme le Covid-19 ne surprenne de nouveau le pays sans plan d'action. De même, au niveau de la Présidence ou du Conseil de sécurité national, la nomination de conseillers en stratégie prospective garantirait que chaque décision majeure soit éclairée à l'aune des menaces futures possibles.

Sur le plan de la coopération régionale et internationale, l'Afrique centrale gagnerait à mutualiser les efforts avec ses voisins et partenaires. Les menaces hybrides ignorent les frontières : un groupe armé chassé d'un pays peut se réfugier dans le pays voisin (comme on l'a vu entre la RDC et ses voisins), une campagne

[17] UNDP, Preventing Violent Extremism through Inclusive Development and the Promotion of Tolerance, 2022.

[18] UNDP, Prevention of Violent Extremism in Africa. United Nations Development Programme, 2022.

de désinformation en ligne visant un État peut avoir des répercussions chez ses alliés, etc.

Il est donc indispensable de renforcer les mécanismes d'échange de renseignements au niveau régional (par exemple via l'Initiative d'analyse des menaces de la CEEAC), d'organiser des exercices conjoints de réponse aux crises hybrides, et de parler d'une voix unie sur la scène diplomatique pour condamner les ingérences (mercenaires, interférences étrangères) qui affectent la région. Au besoin, les pays d'Afrique centrale doivent solliciter l'appui d'organisations plus larges, Union africaine, Nations Unies, Union Européenne, pour bénéficier d'expertise, de formation et de soutien technique. La solidarité internationale est un atout que la région doit mobiliser intelligemment contre un adversaire souvent soutenu, lui, par des puissances extérieures.

En définitive, relever le défi de la guerre hybride en Afrique centrale implique un changement de paradigme : passer d'une posture réactive à une posture anticipative, et d'une approche sectorielle à une approche holistique de la sécurité. Ainsi donc, les recommandations suivantes peuvent être formulées :

- Réformer et adapter les systèmes de sécurité nationale : moderniser les armées et services de renseignement en incorporant les dimensions cyber et influence; améliorer la coordination inter-agences par des cellules de crise intégrées; développer des doctrines et entraînements spécifiques à la menace hybride (par exemple, entraînements conjoints armée-communication pour scénariser des ripostes à des campagnes de désinformation couplées à des attaques militaires).
- Renforcer la coopération inter-États et la réponse multilatérale : mettre en place au niveau régional des centres de fusion du renseignement sur les menaces hybrides; conclure des accords contre l'emploi de mercenaires, le trafic d'armes et la contrebande des ressources naturelles ; solliciter l'appui des mécanismes internationaux (par ex. appliquer les recommandations du Centre européen de lutte contre les menaces hybrides , Hybrid CoE, dans le contexte africain19; adopter une posture diplomatique ferme, incluant

[19] Hybrid CoE, Hybrid Threats: A Strategic Communications Perspective, European Centre of Excellence for Countering Hybrid Threats, 2020.

d'éventuelles sanctions ciblées, envers les acteurs étatiques ou non étatiques qui soutiennent ces ingérences.

- Institutionnaliser la culture d'anticipation : créer au sommet de l'État des unités de veille stratégique (rattachées aux présidences ou aux conseils nationaux de sécurité) chargées de la prospective et de l'alerte précoce; intégrer systématiquement des analyses de scénarios et de risques dans l'élaboration des politiques publiques; développer des programmes de formation en anticipation stratégique pour les cadres civils et militaires, de manière à diffuser les outils et réflexes d'anticipation à tous les échelons.
- Accroître la résilience globale des sociétés : investir dans le développement inclusif et la réduction des inégalités pour tarir le terreau des conflits (éducation, emploi, santé); renforcer l'éducation aux médias afin de réduire la vulnérabilité aux fake news et aux discours de haine; impliquer la société civile, le secteur privé et les communautés locales dans la prévention des crises (approche Whole-of-Society); promouvoir la cohésion nationale et le dialogue intercommunautaire, car une société unie est bien moins vulnérable aux manipulations externes et aux divisions internes.

En suivant ces axes, les pays d'Afrique centrale, au premier rang desquels la RDC compte tenu de l'ampleur des défis qu'elle affronte, seront mieux équipés pour voir venir les menaces hybrides et y faire face de manière coordonnée et efficace. L'enjeu dépasse la simple sécurité : il s'agit de protéger les acquis de développement, la souveraineté et la stabilité de la région tout entière.

A l'ère de la guerre hybride, l'anticipation est la meilleure des défenses. En prenant dès maintenant les mesures appropriées, l'Afrique centrale peut transformer cette menace diffuse en une opportunité de renforcement structurel, et montrer qu'elle est prête à déjouer les stratégies de déstabilisation du XXIe siècle.

REFERENCES BIBLIOGRAPHIQUES

- ADANGA S., « Gouvernance anticipative et sécurité en Afrique centrale », dans *Revue africaine de stratégie,* 2023.
- ADANGA S., Signaux faibles et veille stratégique : anticiper les menaces hybrides, Note pédagogique, CHESD-Kinshasa, 2023.

- African Union, Continental Early Warning System (CEWS) Annual Report. Addis-Abeba, 2020.
- CLAPPER J. R., *Facts and Fears: Hard Truths from a Life in Intelligence,* Viking Press, 2017.
- Conseil de l'Europe, Menaces hybrides et sécurité démocratique en Europe, Rapport de l'Assemblée parlementaire, Strasbourg, 2021.
- Global Health Security Index, Global Preparedness for Health Emergencies Country Profile and Index Scores, Johns Hopkins University / Nuclear Threat Initiative, 2022.
- Hybrid CoE, Hybrid Threats: A Strategic Communications Perspective, European Centre of Excellence for Countering Hybrid Threats, 2020.
- Hybrid CoE, Hybrid Threats: Scenarios and Responses, Helsinki, 2023.
- Institut Pasteur de Dakar, Vers une production locale de vaccins en Afrique, Rapport stratégique, Dakar, 2021.
- International Crisis Group, Avoiding the Perfect Storm in the Sahel, Africa Report n°293, 2021.
- LUTTWAK, E. N., *Strategy: The Logic of War and Peace,* Harvard University Press, 1990.
- MUSILA C., « L'insécurité transfrontalière au Cameroun et dans le bassin du lac Tchad », dans *Ifri*, 2012.
- OTAN, Countering Hybrid Threats: NATO's Approach, Publication de l'OTAN, Bruxelles, 2016.
- SMAÏL D., *Les sociétés militaires privées en Afrique : acteurs hybrides, enjeux politiques,* L'Harmattan, Paris, 2020.
- TENENBAUM E., *Partisans et centurions : Une histoire de la guerre irrégulière au XXe siècle,* Perrin, Paris, 2019.
- UNDP, Preventing Violent Extremism through Inclusive Development and the Promotion of Tolerance, 2022.
- UNDP, Prevention of Violent Extremism in Africa, United Nations Development Programme, 2022.