



**Université Peleforo
GON COULIBALY**

**DEPARTEMENT
D'HISTOIRE**

Août 2026



Revue électronique

E-ISSN : 3107-1651

P-ISSN : 3107-1643

REVUE D'HISTOIRE, D'ART ET D'ARCHEOLOGIE

TEFAL-PITYA

<https://www.revetefal-pitya.net>

soumission@tefal-pitya.net

revuetefal.pityaupgc@gmail.com

BP 1328 Korhogo

Revue d'Histoire, d'Art et d'Archéologie

TEFAL-PITYA



Vol.1, N°2, Août 2026

Site : <https://www.revuetefal-pitya.net>

Courriel : soumission@tefal-pitya.net
revuetefal.pityaupgc@gmail.com

Université Peleforo GON COULIBALY

**UFR Sciences Sociales
Département d'Histoire
BP 1328 Korhogo**

E -ISSN : 3107-1651/ P-ISSN : 3107-1643

COMITE EDITORIAL

DIRECTEUR SCIENTIFIQUE : Tanoh Raphael BEKOIN, Professeur Titulaire, Université Alassane Ouattara, Côte d'Ivoire.

DIRECTEUR DE PUBLICATION : KOUASSI Kouakou Siméon, Professeur Titulaire, Université Polytechnique de San-Pedro, Côte d'Ivoire.

DIRECTEUR DE REDACTION : KEWO Zana, Docteur en Histoire des Relations internationales, Université Peleforo GON COULIBALY, Côte d'Ivoire.

DIRECTEUR DE REDACTION ADJOINT : AGUIE Yhattey Hervé Thierry, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

SECRETARIAT DE REDACTION :

KOFFI Amani, Docteur en Histoire Ancienne, Université Peleforo GON COULIBALY, Côte d'Ivoire.

N'GORAN Kouadio Adolphe, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

SIGNAUX Affouminou Emmanuel, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

COORDONNATEURS DE PUBLICATION :

KONE Kiyali, Docteur en Histoire Moderne et Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire,

KOUAME N'founoum Parfait Sidoine, Docteur en Histoire Moderne et Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

TRESORIERE :

SORO Yéfounignigui Marie -Laure, Docteur en Histoire Moderne et Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

CHARGES DE DIFFUSION :

ABE Abé Laurent, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

ANGU Bleou Sylvain, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

ATCHIE Amon Guy Serge, Docteur en Histoire Médiévale, Université Peleforo GON COULIBALY BAKAYOKO Yaya, Docteur en Histoire Médiévale, Université Peleforo GON COULIBALY, Côte d'Ivoire.

DIOMANDÉ Vallet Samuel, Docteur en Histoire Moderne et Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

Fatoumata BAMBA, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

KOUADIO Yao Clément, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

LASME Yao Jean Terence Gauthier, Docteur en archeologie, Université Peleforo GON COULIBALY, Côte d'Ivoire.

OUATTARA Brahim, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

OUATTARA Issouf, Docteur en Histoire Médiévale, Université Peleforo GON COULIBALY, Côte d'Ivoire.

TUO Zie, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

WEBMASTER : COULIBALY Souleymane, Docteur en Histoire Contemporaine, Université Peleforo GON COULIBALY, Côte d'Ivoire.

ÉDITEUR : Département d'Histoire, Université Peleforo GON COULIBALY Website : <https://www.revuefefal-pitya.net>

COMITE SCIENTIFIQUE

Abass Souleymane SANGARE, Professeur Titulaire d'Histoire Médiévale, Université Alassane Ouattara, Côte d'Ivoire.

Aboulaye BATHILY, Professeur Titulaire d'Histoire, Université Cheick Anta Diop-Sénégal
Blesson Florent SOHI, Maître de Conférences en Histoire moderne, Université Felix Houphouët Boigny-Côte d'Ivoire.

Koffi Antoine GOLE, Professeur Titulaire d'Histoire, Université Alassane Ouattara- Côte d'Ivoire.

Moritié CAMARA, Professeur Titulaire d'Histoire des Relations Internationales, Université Alassane Ouattara- Côte d'Ivoire.

Nohadani Syrus AHMADI, Maître de Conférences en Géopolitique, Tarbiat Modares University- République Islamique d'Iran.

Odile GOERG, Professeure émérite d'Histoire de l'Afrique contemporaine, Université Paris Cité-CESSMA

Ouakoubo Gaston GNABRO, Professeur Titulaire d'Histoire des techniques, Université Peleforo GON COULIBALY, Côte d'Ivoire.

Siméon KOUAKOU, Professeur Titulaire d'archéologie, Université Felix Houphouët-Boigny Côte d'Ivoire.

Simon-Pierre M'BRA EKANZA, Professeur Titulaire d'Histoire, Professeur Émérites du Cameroun, Université Felix Houphouët-Boigny – Côte d'Ivoire

Tanoh Raphaël BEKON, Professeur Titulaire d'Histoire économique et sociale, Université Alassane Ouattara, Côte d'Ivoire.

Cho Julie Eunice BROU, Maître de Conférences en Histoire moderne et contemporaine, Université Felix Houphouët Boigny-Côte d'Ivoire.

Jean-Noël LOUCOU, Professeur Titulaire d'Histoire, Université Felix Houphouët-Boigny Côte d'Ivoire.

Théophile KOUI, Professeur Titulaire Études Ibériques et Civilisations Latino-Américaines, Université Felix Houphouët-Boigny- Côte d'Ivoire

Comlan Jérôme ALLADAYE, Professeur Titulaire d'Histoire, Université d'Abomey-Calavi Benin.

Ibrahim Muhammed SAADAOUI, Professeur d'Histoire Moderne et Contemporaine, Université de Tunisie. President de la Tunisian World Center for Studies, Research, and Development et de la Tunisian-Mediterranean Association for Historical, Social and Economic Studies. Tunisie)

Ousseynou FAYE, Professeur Titulaire d'Histoire, Université Cheick Anta Diop –Sénégal.

Kouamé René ALLOU, Professeur Titulaire d'Histoire, Université Felix Houphouët-Boigny - Côte d'Ivoire.

Mahomed N'GUESSAN, Professeur Titulaire d'Histoire politique, Université Felix Houphouët-Boigny -Côte d'Ivoire.

Tiona OUATTARA, Directeur de Recherche d'Histoire, Université Felix Houphouët-Boigny - Côte d'Ivoire.

COMITE DE REDACTION

ABE Abé Laurent,

AGUIE Yhattey Hervé Thierry,

ANGU Bleou Sylvain,

ATCHIE Amon Guy Serge,

BAKAYOKO Yaya,

COULIBALY Souleymane,

DIOMANDÉ Vallet Samuel,

Fatoumata BAMBA,

KEWO Zana,

KOFFI Amani,

KONE Kiyali,

KOUADIO Yao Clément,

KOUAME N'founoum Parfait Sidoine,

LASME Yao Jean Terence Gauthier,

N'GORAN Kouadio Adolphe,

OUATTARA Brahim,

OUATTARA Eugenie,

OUATTARA Issouf,

SIGNAUX Affouminou Emmanuel,

SORO Yéfounnigui Marie -Laure,

TUO Zie.

COMITE DE LECTURE

Djidjé Jacques KAZIO, Docteur en archéologie, Université de Bondoukou

Awa SOROGO, Docteur en Histoire Moderne et contemporaine, Université Alassane Ouattara

Antoine KRA, Maître Assistant d'Histoire économique et sociale, Université Alassane Ouattara -Côte d'Ivoire.

Tiantio SANOGO, Institut Nationale Supérieur des Arts et de l'Action Culturelle, Abidjan

Salif KINDREBEOGO, Maître de Conférences en Histoire des relations Internationales, Université Norbert Zongo de Koudougou.

Nohan SIDIBE, Docteur en Histoire du travail et Histoire économique, Université de San Pedro-Côte d'Ivoire.

Nahoua Karim SILUE, Docteur en Histoire des Relations Internationales, Université Alassane Ouattara.

N'Goran Gédéon BANGALI, Maître de Conférences d'Histoire des Relations Internationales, Université Jean Lorougnon Guede -Côte d'Ivoire.

N'dri Laurent KOUAKOU, Maître de Conférences d'Histoire des Relations Internationales, Université Alassane Ouattara -Côte d'Ivoire.

N'doua Etienne ETTIEN, Docteur en archéologie, Université Félix Houphouët Boigny, Abidjan.

Moutari Moussa MAMAN, Docteur en Histoire Sociopolitique, Université Djibo Hamani de Tahoua/Niger.

Mitanhantcha YEO, Docteur en archéologie, Université Alassane Ouattara- Côte d'Ivoire.

Mamadou Lamine DEMBELE, Professeur Titulaire du Mali / Maître de Conférences du CAMES en Histoire du droit et des institutions, Université des Sciences Juridiques et Politiques de Bamako (USJPB) –Mali.

Kpassigué Gilbert KONE, Docteur en Histoire Moderne et contemporaine, Université Alassane Ouattara

Kouakou Sylvain KOFFI, Docteur en archéologie, Université Félix Houphouët Boigny, Abidjan.

Kouakou Désiré M'BRA, Maître de Conférences en Histoire du peuplement, Université Alassane Ouattara Côte d'Ivoire.

Kouadio René BOUADI, Docteur en archéologie, Jean Lorougnon Guédé, Daloa Idrissa BA, Maître de Conférences d'Histoire Médiévale, Université Cheik Anta Diop- Sénégal.

Harouna YEO, Docteur en archéologie, Université Félix Houphouët Boigny, Abidjan. Guy-

Roland TIE BI GALLA, Docteur en archéologie, Université Félix Houphouët Boigny, Abidjan.

Gninin Aicha TOURE, Docteur en archéologie, Université Félix Houphouët Boigny, Abidjan.

Ernest YAOBI, Maître de Conférences d'Histoire des Religions, Université Félix Houphouët Boigny, Côte d'Ivoire

Dognima Lassina COULIBALY, Docteur en Histoire Moderne, Université Felix Houphouët Boigny, Côte d'Ivoire

Atché Michel AKA, Docteur en archéologie, Université de San Pedro

Abdoulaye BAMBA, Maître de Conférences d'Histoire des Relations Internationales, Université Felix Houphouët-Boigny -Côte d'Ivoire.

SOMMAIRE

1. Tiasvi Yao Raoul AGBAVON, Lecture du jeu des possibles jacobien à partir du déterminisme bernardien : une continuité épistémologique	1-11
2. El Hadji Malick DÈME & Younouss DIOP, Héliopolis, porte du ciel : Réception et Transmission des messages divins en Égypte ancienne	12-27
3. Maman Moutari MOUSSA IBRAH & Addo MAHAMANE & François WASSOUNI, Les savoir-faire techniques en Afrique au Sud du Sahara pendant la période précoloniale	28-43
4. Salif KIENDREBEOGO & Yaya SAWADOGO & Tiéwendé Jean BALIMA, Coopération, peuplement et mise en valeur du bassin de la Volta (1966-2002)	44-60
5. Ibrahima Khalilou & Khady Ndoye DIAGNE, Regard ethnographique sur l'activité céramique en milieu wolof au Sénégal : la caste des potières internes	61-80
6. Sébastien GUIPO, L'école burkinabé face au défi sécuritaire : situation des élèves déplacés dans la province du Zondoma (2015-2024)	81-96
7. Essou Koffi Benjamin MIEZAN & Bonzou Ella ESSEY épouse OHOUO, Service des grandes endémies en Côte d'Ivoire : instrument de lutte contre les maladies endémo-épidémiques (1959-1969)	97-109
8. Moussa Fadiala BOCOUM, L'implantation de la mine de lithium de Bougouni face à la vulnérabilité locale	110-124
9. Kossia Blandine KRA, Pathologies du personnel des forts de la Côte de l'Or (XVIIe-XIXe siècle)	125-138
10. Kouamé Koffi, Systèmes éducatifs en Afrique et problématique de l'employabilité : défis, enjeux et perspectives de transformation	139-154
11. Mitanhantcha YEO, La céramique dans la restauration à Gbèkèkro (Côte d'Ivoire)	155-167
12. Cédric-Aurel MANZENZA, La place du dieu Osiris dans les croyances égyptiennes (2778-1085 av. J-C)	168-180
13. Olive Pulchérie ITOUMBA & Eric Damien BIYOGHE BI ELLA, Longévité du pouvoir d'Omar Bongo Ondimba au Gabon : mécanismes de pérennisation et impacts politiques, économiques et sociaux (1967-2009)	181-202
14. N'founoum Parfait Sidoine KOUAME, Les Siti dans le Royaume de Bouna du XVIIe siècle au XIXe siècle	203-214

15. ABDOURHIMOU Hassane, Les enjeux des alliances politico-militaires entre le Ziguï (Dosso) et le Kebbi (Argungu) de 1831 à 1856	215-228
16. BIRBA Noaga, Approche ethnoarchéologique de l'art de la terre cuite chez les potières de Gaoua (Burkina Faso)	229-247
17. DEMBO YANGA, L'entreprenariat des Manjack en Casamance au temps de la colonie : 1850 – 1960	248-272
18. Jean-Max Pamphil BENIE & Massandjé FADIKA KANO, Violence politique et gouvernance impériale dans le Songhay au XVe XVIe siècles	273-287
19. Gaoussou KAGNASSY, Le conflit de 2026 entre l'Iran et l'axe israélo-américain : leçons technologiques pour l'Afrique	288-304
20. Awa SOROGO, Evolution de l'esclavage dans le Baoulé-faafoué 1721-1911	305-318
21. Adama SAWADOGO & Moctar SANFO, Authenticité et mutations du mariage des Mossé du Sandbontenga au Burkina Faso	319-336
22. DOGNON Elavagnon Dorothée, La réécriture poétique de la mémoire par l'esthétique d'archive dans le cinéma ouest-africain	337-357
23. ANIN PATRICIA-CLAIRE N'CHO Epouse NOGBOU, Mysticisme soufi, pouvoir urbain et identité savante en Afrique de l'Ouest du XVème au XVIème siècle	358-375
24. Richard Codjo AKODANDE HONMA, De la pénombre à la lumière : l'aménagement urbain comme vecteur de sécurité nocturne au Bénin 2016-2026 à travers les trajectoires de Cotonou, Porto-Novo et Parakou	376-392
25. Paul SALATOU, Le fondement de la réforme éducative du Réseau École et Développement (RED) : 1989-2011	393-408
26. MONGA Arthur Dénos & YRO Timbo Adler Vivien, Décryptage écocritique des mythes totémiques Wê de Côte d'Ivoire : les exemples des mythes de la poule et du poisson	409-423

Le conflit de 2026 entre l'Iran et l'axe israélo-américain : leçons technologiques pour l'Afrique

Gaoussou KAGNASSY

École normale supérieure de Bamako (Mali)

Kagnassy4@yahoo.fr

Résumé

L'article démontre que l'escalade technologique entre la coalition israélo-américaine et la République islamique d'Iran contraint le continent africain à réinventer la sécurité et la souveraineté numérique. La guerre, débutée en février 2026, est marquée par une rupture technologique majeure où s'imposent des armes ultra-rapides, telles que les technologies hypersoniques et l'intelligence artificielle. L'utilisation intensive bouleverse les stratégies militaires mondiales, marquant une transition vers ce que l'on nomme la « guerre à haute vitesse » ou la « cyberguerre ». De plus, l'emploi massif de la haute technologie, tels que les drones et la surveillance satellitaire en temps réel, rend caduques les tactiques de camouflage classiques. Le changement de paradigme fondamental dans la guerre moderne impose des défis critiques aux pays accusant un retard numérique, notamment en Afrique. Pour s'imposer durablement dans le numérique, les États africains doivent dépasser la simple logique d'achat d'équipements pour ancrer une culture de la cyberdéfense et développer le capital humain afin de bâtir des compétences stratégiques. La transition numérique de l'Afrique ne réussira qu'à condition de passer du statut de simple consommatrice de technologies à celui de productrice de solutions sécurisées. En misant sur les talents, le continent transformera la cyberdéfense en un véritable levier d'innovation, de confiance et de pérennité économique.

Mots-clés : Afrique, cyberattaque, cybersécurité, souveraineté numérique et Union africaine.

The 2026 Conflict between Iran and the Israeli-American Axis: Technological Lessons for Africa

Abstract

This article demonstrates that the technological escalation between the Israeli-American coalition and the Islamic Republic of Iran is forcing the African continent to rethink its security and digital sovereignty. The conflict, which began in February 2026, is characterized by a major technological breakthrough, with the growing deployment of ultra-high-speed weapons, including hypersonic technologies, as well as artificial intelligence. The intensive use of these technologies is reshaping global military strategies and marking a transition towards what has been described as “high-velocity warfare” and “cyberwarfare.” Furthermore, the widespread use of advanced technologies, particularly drones and real-time satellite surveillance, is rendering conventional camouflage tactics increasingly obsolete. This fundamental paradigm shift in modern warfare poses critical challenges to countries that lag behind in digital development, particularly in Africa. To establish a sustainable position in the digital domain, African states must move beyond simply purchasing equipment and instead foster a culture of cyber defence while developing human capital and building strategic capabilities. Africa's digital transformation will only succeed if the continent moves from being merely a consumer of technology to becoming a producer of secure technological solutions. By investing in its human talent, the continent can transform cyber defence into a genuine driver of innovation, trust, and economic sustainability.

Keywords: Africa, cyberattack, cybersecurity, digital sovereignty and African Union.

Introduction

Les tensions entre la coalition Israélo-américaine et l'Iran s'inscrivent dans une perspective historique de longue date. Mais l'escalade a débuté par des frappes aériennes massives lancées fin février 2026 par la coalition contre l'Iran. En réponse, l'Iran a frappé avec une haute précision des cibles dans les pays abritant des bases américaines tels que l'Arabie Saoudite, le Bahreïn, les Emirats Arabes Unis, l'Irak, la Jordanie, le Koweït et le Qatar. De ce fait, le conflit israélo-américain face à l'Iran se distingue par une combinaison de l'intelligence artificielle et des technologies hypersoniques. Les outils de guerre ne sont pas seulement des instruments de dissuasion, ils sont aussi des armes offensives ou d'attaque pour percer les systèmes de défense. L'ère hypersonique bouleverse l'équilibre stratégique, rendant caduque les systèmes de défense conventionnels. « La guerre en Iran constitue une rupture dans les conflits contemporains, avec une transformation radicale des stratégies militaires » (D. Diouf, 2026, p. 1).

En effet, la nouvelle donne souligne la vulnérabilité des États, notamment en Afrique, dont les dispositifs militaires restent ancrés dans des modèles classiques. Car, la plupart des États africains continuent à investir dans des systèmes de défense « sol-air » conventionnels qui demeurent obsolètes face aux menaces de haute technologie. De plus, le manque de capacités satellitaires de surveillances thermiques crée une fragilité stratégique majeure sur tout le continent. « Dans un contexte de numérisation accélérée, les pays africains sont de plus en plus exposés à des menaces numériques sophistiquées » (M. Lokossi, 2025, p. 1.). Une situation qui place l'Afrique dans une impasse sécuritaire assez critique. Une question reste en suspens : comment l'innovation technoscientifique dans la guerre entre la coalition israélo-américaine et l'Iran redéfinit-elle les normes de la guerre moderne et quelles leçons les pays africains peuvent-ils en tirer pour leur propre sécurité ?

Ainsi, l'objectif principal de l'article est de démontrer que l'escalade technologique entre la coalition israélo-américaine et la République islamique de l'Iran doit contraindre les États africains à réévaluer les systèmes de sécurité et la souveraineté numérique. Il s'agit pour les pays de repenser la sécurité à partir de la promotion de la cybersécurité. Enfin, l'étude adopte une démarche analytique pour dépasser la simple chronique factuelle et décrypter les dynamiques, les interactions ainsi que les rapports de cause à effet. Au-delà de l'inventaire des innovations technologiques employées dans le conflit, il s'agit d'évaluer l'impact de la cyberguerre sur la reconfiguration de la puissance mondiale. L'argumentation s'articule autour de deux axes principaux : d'une part, la guerre israélo-américaine en Iran comme guerre de la haute technologie ; d'autre part, l'examen des enseignements stratégiques que l'Afrique doit tirer du conflit entre la coalition israélo-américaine et l'Iran.

1. La guerre israélo-américaine en Iran comme guerre de la haute technologie

Le conflit entre l'Iran et le tandem israélo-américain ne se résume plus à de simples affrontements conventionnels sur un champ de bataille traditionnel. La guerre se métamorphose en une guerre de haute technologie, où l'innovation numérique et l'armement de pointe dictent le tempo des opérations. Des cyberattaques sophistiquées ciblant les infrastructures critiques aux frappes de précision guidées par l'intelligence artificielle, la frontière entre science-fiction et réalité militaire s'est totalement effacée. La mutation technologique redéfinit les doctrines de défense et la nature même de la dissuasion au Moyen-Orient. Analyser la guerre à travers le prisme permet ainsi de comprendre comment le renseignement électronique et la supériorité algorithmique priment désormais sur la force brute.

1.1. Le passage de la guerre de masse à la supériorité technologique dans le conflit en Iran

Le conflit entre la coalition israélo-américaine et l'Iran marque un tournant historique majeur. Il illustre une transition stratégique où la fulgurance des attaques dépasse désormais les capacités de réaction humaine. Comme le souligne le journal « Le Soleil » (2026) en ces termes :

Depuis, le conflit s'est étendu, mêlant frappes massives, attaques de drones, opérations cybernétiques et guerre indirecte, révélant une mutation profonde. La guerre contemporaine n'est plus seulement une confrontation d'armées régulières. Elle est devenue un système complexe, hybride et technologique. Le déclenchement de la guerre entre les États-Unis, Israël et l'Iran, en 2026, en est l'illustration la plus récente et la plus frappante. (D. Diouf, 2026, p. 1)

Il s'agit réellement d'une escalade combinant armes hypersoniques et intelligence artificielle, caractérisée par une vitesse extrême, une prise de décision automatisée et une précision chirurgicale. La supériorité technologique se mesure aussi à la capacité de traiter l'information et de frapper plus vite que la capacité de réflexion humaine. Le type de conflit comprime les temps de réaction à quelques secondes ou minutes, rendant les défenses traditionnelles largement caduques. De ce fait, V. Robert affirme ceci : « Aujourd'hui, la guerre de l'Iran, c'est une guerre du siècle dernier, alors que la guerre israélo-américaine, c'est la guerre de l'intelligence artificielle, de la haute technologie. Et la technologie a battu l'idéologie » (R. Virginie, 2026, p. 1.). Même si l'argument selon lequel la technologie iranienne est dépassée ne me paraît pas juste, car, selon C. Romano, « l'Iran a lancé le mardi 1er octobre un raid aérien contre Israël, utilisant pour la première fois un nouveau type de missile, hypersonique et balistique, baptisé Fattah » (C. Romano, 2024, p. 1.) ; mais il faut tenir que la guerre de 2026 se caractérise par une escalade technologique intense, où la supériorité sophistiquée de la coalition s'oppose à la stratégie iranienne basée sur le volume, les missiles balistiques et les drones.

En effet, le passage de la guerre de masse à la supériorité technologique se manifeste par une opposition entre deux doctrines fondamentalement différentes : la précision chirurgicale multi-domaine contre l'attrition asymétrique saturante. Selon Faucher Laure, « l'objectif de l'escalade pour la coalition n'est plus la conquête territoriale, mais la décapitation des centres de commandement tels que ceux des Gardiens de la révolution, et la destruction de la base industrielle de défense iranienne comme les missiles, le nucléaire » (L. Foucher, 2026, p. 5.). La coalition privilégie donc des frappes plus ou moins précises et l'intelligence artificielle pour démanteler les capacités iraniennes sans engagement terrestre massif, tandis que l'Iran répond par une saturation de drones et de missiles à bas coût. Le passage à la technologie permet à l'Iran de ne plus simplement compter sur le nombre de soldats, mais d'infliger des coûts élevés et de maintenir une capacité de nuisance stratégique malgré un déséquilibre des forces conventionnelles. Selon A. Azimi, « au cours de la dernière décennie, il a investi massivement dans des capacités balistiques à plusieurs niveaux, des drones à longue portée et un réseau de groupes armés alliés dans toute la région » (Azimi, 2026, paragr. 2.). Car la République islamique a compris que le territoire continental américain est hors de portée, mais les bases américaines dans la région, en particulier dans les pays arabes voisins, ne le sont pas. De plus, l'Israël se trouve également à portée des missiles et des drones iraniens. Dans le conflit, l'Iran a vite compris qu'il n'a pas besoin de remporter une victoire, mais de tenir. C'est pour cette raison, il mise sur une stratégie fondée sur la dissuasion, la durée et l'endurance. Selon l'analyse d'Amir Azimi pour la BBC Afrique, Téhéran ne cherche pas une victoire conventionnelle mais une dissuasion par l'endurance :

Le calcul de l'Iran repose en partie sur l'économie de guerre. Les intercepteurs utilisés par Israël et les États-Unis sont beaucoup plus coûteux que la plupart des drones et missiles à usage unique déployés par l'Iran. Un conflit prolongé oblige les États-Unis et Israël à utiliser des moyens coûteux pour intercepter des menaces relativement peu coûteuses. (Azimi, 2026, paragr. 2.).

Les attaques iraniennes par drones low-cost et missiles balistiques imposent l'usage d'intercepteurs sophistiqués, comme les systèmes Arrow, Patriot ou les équipements navals américains, qui se révèlent nettement plus coûteux. Par cette stratégie d'usure, l'Iran mise sur une asymétrie économique pour épuiser les budgets et les stocks de munitions de la coalition. Dès lors, la supériorité technologique de l'axe israélo-américain se heurte à la stratégie asymétrique d'usure de l'Iran.

1.2. La domination technologique de la coalition face à la stratégie asymétrique de l'Iran

La doctrine militaire américano-israélienne met l'accent sur la mobilisation rapide, la résilience et la supériorité technologique. Elle repose sur l'utilisation combinée de systèmes de défense antimissile multicouches, de guerre électronique et de réseaux de renseignement avancés. Cette supériorité s'est manifestée par des opérations de grande envergure, telles que « du côté américain, celle-ci est nommée Fureur épique (Epic Fury). Du côté israélien, elle est appelée Lion rugissant (Roaring Lion). Les deux armées auraient frappé plus de 2 000 cibles en Iran depuis le début des frappes » (M. Vaugoude, 2026, p. 1.). Ceci dit, l'escalade technologique et militaire au Moyen-Orient a amené la coalition israélo-américaine et partenaires régionaux à mobiliser un arsenal technologique de pointe pour neutraliser les capacités stratégiques de Téhéran, notamment les sites nucléaires, les centres de commandement et les infrastructures de missiles.

- **La domination technologique de la coalition israélo-américaine** : elle se matérialise d'abord par l'utilisation d'une aviation de chasse de pointe, de bombardiers stratégiques et de groupes aéronavals massifs. Ensuite, cette coalition israélo-américaine exprime sa supériorité technologique à travers le déploiement de systèmes d'interception sophistiqués et onéreux pour contrer les projectiles adverses. Enfin, rentre en ligne de compte sa supériorité dans la collecte de données, la surveillance satellite et les frappes de précision chirurgicale. Ainsi, face à la coalition Iran oppose, selon A. Azimi, « son système basé sur l'endurance, la saturation » (Azimi, 2026, paragr. 2.) et le relèvement des coûts économiques et énergétiques de la guerre.

- **La stratégie asymétrique de l'Iran** : Téhéran fait recours massif à des drones kamikazes (type Shahed) et à des missiles balistiques dont la production est peu coûteuse. De plus, elle multiplie les tirs pour saturer les radars de la coalition et épuiser ses stocks de missiles intercepteurs beaucoup plus chers. Par ailleurs, selon une enquête du New York Times qui souligne ceci :

L'Iran aurait réussi à préserver l'essentiel de ses stocks de missiles balistiques et de ses lanceurs, et disposerait encore d'importantes capacités dans ce domaine. Son arsenal de drones lui offre en outre un avantage net en matière de masse et un rapport coût-bénéfice largement favorable. L'Iran peut en effet fabriquer plusieurs milliers de drones par mois, quand la production américaine d'intercepteurs Patriot plafonne à environ 600 unités par an. (P. Simon, 2026, paragr. 7.).

L'Iran utilise aussi des usines et de sites de lancement souterrains que les experts appellent villes de missiles pour maintenir la production malgré les frappes. Enfin, la République islamique adopte une stratégie d'implication de milices régionales alliées pour

dispenser les théâtres d'opération et menacer les infrastructures économiques et énergétiques du Golfe.

- **Le choc des logiques stratégiques** : La coalition face à l'Iran mise sur l'intensité. Ses dispositifs sont taillés pour des campagnes courtes à haute technologie et à fort impact destructeur. Il s'agit d'une méthode dont le principe est de « frapper fort et vite ». Pour ce faire, la coalition utilise des armes plus avancées, une puissance de feu supérieure ou des innovations pour détruire l'ennemi avant qu'il ne puisse s'organiser. L'objectif est d'obtenir un résultat immédiat et limiter les pertes en évitant un conflit qui s'éternise. Par contre, la République Islamique vise la durée, une sorte de stratégie d'usure de longue haleine fondée sur le coût politique. En cela, l'Iran vise cet objectif d'augmenter continuellement le coût politique et économique du conflit pour pousser ses adversaires à la retenue ou au renoncement.

Ainsi, face à leurs vulnérabilités inhérentes et à des menaces asymétriques, la coalition israélo-américaine et l'Iran se tournent vers l'innovation militaire. Car la dynamique conflictuelle révèle une dépendance stratégique croissante envers l'innovation technologique. Face à des asymétries de puissance, chaque protagoniste déploie l'inventivité pour combler ses propres failles tactiques. D'un côté, Israël et les États-Unis perfectionnent leurs boucliers antimissiles et leur supériorité cybernétique. De l'autre, l'Iran compense son infériorité en investissant massivement dans les drones et les réseaux asymétriques. Cette course transforme le théâtre d'opérations en un laboratoire de doctrines militaires inédites. L'innovation devient ainsi le garant fondamental de la dissuasion et de la survie de chaque camp. Par conséquent, la guerre technologique entre l'Iran et l'axe israélo-américain engendre de lourdes répercussions directes et indirectes sur le continent africain.

1.3. Les conséquences de la guerre entre l'Iran et la coalition israélo-américaine sur l'Afrique

L'intensification des tensions entre Israël, l'Iran et les États-Unis entraîne des conséquences majeures à l'échelle internationale. Elle provoque de lourdes vagues de répercussions sur la sécurité et l'économie mondiales. Malgré une trêve encore incertaine, la communauté internationale craint une extension globale du conflit. La situation géopolitique actuelle au Moyen-Orient reste donc extrêmement volatile. Il s'agit d'un contexte de volatilité auquel les dirigeants africains doivent réagir. Les rivalités entre grandes puissances transforment régulièrement l'Afrique en champ de bataille malgré elle ; l'Histoire l'a toujours prouvé. Le continent africain a été et demeure un théâtre récurrent des rivalités géopolitiques mondiales à cause de sa position géographique stratégique et de ses immenses richesses en ressources naturelles. De nouveaux acteurs comme la Chine, la Russie, la Turquie et l'Iran aux

côtés des puissances traditionnelles, comme les États-Unis, la France et l'Union européenne, se disputent l'influence politique et l'accès aux minerais critiques indispensables aux technologies modernes. Cette compétition géopolitique en Afrique reflète une recomposition majeure des relations internationales autour du contrôle des ressources indispensables à la transition énergétique et numérique. En cela, l'Iran cherche à nouer des alliances stratégiques et économiques avec les pays africains. La République islamique renforce activement sa présence diplomatique, économique et sécuritaire en Afrique afin de diversifier ses partenariats et de contourner les sanctions occidentales. Dans ces dernières années, l'Iran a multiplié ses partenariats avec nombreux pays africains comme le Sénégal, le Burkina Faso, la Côte d'Ivoire, le Ghana et le Mali. Mais ses potentiels alliés africains seraient des pays tels que l'Afrique du Sud, l'Égypte et l'Éthiopie, qui siègent à ses côtés au sein du bloc des BRICS. Ainsi, la recherche de partenaires par l'Iran accentue la compétition diplomatique sur le continent.

Par ailleurs, même si le risque de basculement direct du conflit ouvert entre l'axe israélo-américain et l'Iran vers le territoire africain semble faible sur le plan strictement militaire, le continent subit les ondes de choc économiques, logistiques et les rivalités d'influence géopolitique. D'abord, l'instabilité régionale perturbe le trafic maritime proche du canal de Suez, une voie vitale pour les échanges entre l'Asie, l'Europe et l'Afrique de l'Est. Ensuite, les rivalités idéologiques ou l'action de réseaux d'influence peuvent exacerber des tensions locales préexistantes. Sur ce plan, la Corne de l'Afrique et les abords de la mer Rouge constituent un théâtre stratégique vulnérable face à une extension des représailles de l'Iran et de ses alliés régionaux. De plus, Téhéran et ses alliés instrumentalisent la rhétorique souverainiste et anti-occidentale pour chercher des soutiens diplomatiques auprès de certains États africains, accentuant les divisions face aux pressions des puissances occidentales. Dans des pays comme le Nigeria, l'influence de l'Iran sur les minorités chiites fait craindre aux services de sécurité des attaques de solidarité ou des troubles ciblés contre des intérêts américains ou israéliens. Comme le signale P. Martial, « au Nigeria, où la communauté chiite est importante, le Mouvement islamique du Nigeria a organisé des manifestations dans plusieurs grandes villes du Nord, mais aussi à Lagos et à Abuja », (P. Martial, 2026, p. 1.). Selon C. Assignon, les autorités nigérianes semblent vouloir jouer la carte de l'apaisement en appelant à la désescalade. Mais l'annonce de la disparition de plusieurs hauts responsables iraniens, dont le guide suprême Ali Khamenei a donné lieu à des protestations, notamment du Mouvement islamique du pays. « Nous sommes dans la rue pour présenter nos condoléances et témoigner de notre profonde tristesse et de notre douleur face à l'assassinat de Khamenei » (Assignon, 2026, paragr. 1.), assure Safiyya membre du mouvement islamique du Nigeria. Une partie de cette communauté pourrait se radicaliser,

d'autant que le gouvernement a autorisé une présence militaire des États-Unis sur le territoire. Enfin, les ressources militaires des États-Unis à Djibouti et en Somalie, ainsi que celles d'Israël en Érythrée, pourraient devenir la cible de représailles de l'Iran.

Ainsi, selon Voxafrica, pour éviter d'être impliqués dans cette crise au Moyen Orient, la majorité des dirigeants africains et les organisations régionales, telles que l'Union africaine et la CEDEAO, choisissent la neutralité et réclament une désescalade urgente. Face aux crises armées, l'Union africaine privilégie généralement la voie de la négociation et le respect des résolutions des Nations unies, (Voxafrica, 2026, paragr. 1 et 5.). Cependant, le conflit israélo-américain contre l'Iran agit comme un révélateur des enseignements stratégiques clés pour renforcer la sécurité et la résilience des pays africains.

2. Les leçons stratégiques de l'escalade technologique en Iran pour la souveraineté sécuritaire africaine

Le conflit entre l'Iran, Israël et les États-Unis dépasse le cadre strictement moyen-oriental pour résonner comme un cas d'école géopolitique mondial. Il met en lumière les mutations rapides de la guerre contemporaine. Pour les États africains, régulièrement confrontés à des crises sécuritaires internes et transfrontalières, ces événements constituent un cas d'étude stratégique majeur. Globalement, ils révèlent à l'Afrique les profondes vulnérabilités et lacunes technologiques face aux guerres modernes à haute intensité.

2.1. Le conflit en Iran comme révélateur des lacunes technologiques de l'Afrique

Le continent affronte une gamme de menaces non traditionnelles, notamment les cyberattaques, les drones et la guerre de l'information. Les professionnels de la sécurité doivent se préparer à affronter ces menaces hybrides, (Africa Defense Forum (adf), 2022, p. 1.). L'Afrique fait face à des cyberattaques et à une désinformation numérique majeures, dont la défense est freinée par le manque d'infrastructures adaptées et de moyens de coordination globale. Le Rapport INTERPOL de 2025 sur l'évaluation des cybermenaces en Afrique révèle que les actes de cybercriminalité sont en forte hausse sur l'ensemble du continent. Le Rapport souligne ceci :

La cybercriminalité prend actuellement de l'ampleur dans toute l'Afrique, menaçant la sécurité publique, les systèmes financiers et la confiance dans le numérique. Si de plus en plus de pays commencent à prendre des mesures face à ces cybermenaces, nombre d'entre eux connaissent encore de graves problèmes structurels qui entravent leur capacité à les déceler, à enquêter à leur sujet et à y mettre un terme, (INTERPOL, 2026, p. 3.).

L'analyse de la situation cybernétique du continent africain confirme une vulnérabilité prononcée face aux risques, en raison d'une forte dépendance envers les technologies

étrangères, d'un déficit de compétences techniques, de l'absence de cadres juridiques dans de nombreux pays et du manque d'une position commune de l'Union africaine.

- **La dépendance critique africaine envers des technologies étrangères** : Beaucoup d'infrastructures africaines dépendent de technologies et de serveurs étrangers. « La plupart des données consommées sur le continent proviennent de l'extérieur » (Soulé, 2023, paragr. 1.). L'Afrique dépend majoritairement de serveurs, de câbles sous-marins et de technologies hébergés à l'étranger, notamment en Europe, aux États-Unis et en Chine, pour faire fonctionner ses infrastructures numériques, ce qui fragilise la souveraineté et la sécurité des données. Par ce fait précis, O. Coelho affirme :

Plusieurs axes extracontinentaux majeurs se distinguent. À l'ouest, les flux numériques convergent vers l'Europe, où sont localisés de nombreux centres de données soutenant la numérisation du continent africain, ainsi que vers les États-Unis via les câbles transatlantiques. À l'est, d'autres routes, et notamment les « routes de la soie numériques » chinoises, relient le continent africain au Pakistan, à l'Inde puis à la Chine. Une zone de transit structurante autour du Canal de Suez propose un autre chemin de connexion entre l'Europe, l'Afrique du Nord, le Moyen Orient, l'Afrique de l'Est et l'Asie. (O. Coelho, 2025, p. 137.).

La majorité des données africaines sont donc stockées dans des datacenters situés hors du continent, affaiblissant la souveraineté numérique et la protection de la vie privée. Une telle situation complique le contrôle total des flux de données et la réaction rapide en cas d'intrusion. « La dépendance excessive vis-à-vis des technologies, infrastructures et plateformes étrangères expose le continent à des risques géopolitiques, des menaces sur la vie privée de ses citoyens et une fuite de valeur économique » (Webgram, 2025, paragr. 2.). La dépendance crée une vulnérabilité systémique qui touche la sécurité nationale des pays. La situation place le continent dans un rôle de simple consommateur d'outils technologiques et numériques, dont il ne maîtrise ni les standards ni l'architecture de sécurité. Ceci dit, le continent africain peine à développer les outils technologiques et les modèles d'intelligence artificielle adaptés aux réalités locales comme les langues, l'agriculture et la santé. Ainsi, l'absence de géants technologiques et numériques locaux rend les données nationales vulnérables aux ingérences extérieures. De plus, une autre difficulté de l'accès aux ressources numériques est liée à l'enclavement géographique de certains pays africains sans littoral, à l'instar du Mali, complique l'accès au haut débit en raison de la dépendance absolue aux infrastructures des pays côtiers pour se connecter aux câbles sous-marins internationaux.

L'absence d'accès direct à la mer complique l'infrastructure et augmente considérablement les coûts. Le passage par les pays voisins côtiers engendre des frais de transport des données qui renchérissent considérablement le prix final de la connexion internet pour les citoyens et les

entreprises. L'enclavement géographique constitue ainsi un obstacle majeur au développement du numérique en Afrique. Au total, le continent souffre donc d'un manque de souveraineté technologique et numérique, préférant l'importation de solutions au lieu du développement d'infrastructures locales adaptées telles que de petits datacenters frugaux. La dépendance aux technologies importées entrave le développement industriel local et ne répond pas toujours aux réalités socio-économiques du continent, renforçant, du coup, le sous-développement. Cette dépendance technologique rend les pays africains vulnérables au cyber-espionnage et au sabotage d'infrastructures sensibles. De plus, « un autre défi est la pénurie de compétences technologiques de haut niveau sur le marché du travail et le manque de ressources financières et matérielles pour développer les infrastructures de technologies de l'information et de la communication (TIC) au niveau national » (Soulé, 2023, paragr. 1.).

- **Le déficit de compétences techniques** : le manque de spécialistes locaux en cybersécurité constitue une réalité critique dans les pays africains. « De nombreux pays africains sont confrontés à une pénurie de talents dans divers domaines critiques du secteur numérique, notamment la cybersécurité, la protection des données, l'ingénierie logicielle, etc » (Soulé, 2023, paragr. 1.). N. I. M. Rachid aussi évoque le déficit de compétences techniques en ces termes :

Le déficit de compétences en cybersécurité est un problème majeur en Afrique. De nombreux pays manquent de professionnels qualifiés capables de détecter, prévenir et répondre aux cybermenaces. Cette pénurie limite la capacité des entreprises et des institutions à sécuriser efficacement leurs systèmes. (N. I. M. Rachid, 2024, paragr. 1.).

Le déficit affaiblit la capacité des Etats et des entreprises à répondre efficacement non seulement aux cyberattaques de « haute intensité », mais aussi au cyber-espionnage qui augmente avec la numérisation rapide du continent. Africa Defense Forum écrit :

Le manque de réponse efficace est dû en partie aux déficits de capacité, écrit le Dr Allen. Le continent fait face à un manque de professionnels certifiés en cybersécurité de 100.000 personnes, chiffre qui est en augmentation. Un grand nombre d'organisations, de commerces et d'agences manquent de sensibilisation cybernétique de base ; ils manquent aussi de mettre en œuvre des mesures de cybersécurité rudimentaires. Les gouvernements échouent fréquemment pour surveiller les menaces, recueillir des preuves forensiques numériques, ou tenter des poursuites relatives à la criminalité informatique. 96 % des incidents de cybersécurité restent non signalés ou non résolus, ce qui veut dire que les menaces cybernétiques en Afrique sont sans doute bien pires que ce qui est reconnu. (Africa Defense Forum (adf), 2022, p. 1.).

Les cybermenaces sont aujourd'hui exacerbées par un vide juridique spécifique dans beaucoup de pays africains.

- **L'absence de cadre juridique** : de nombreux pays africains manquent encore d'une législation en cybersécurité. L'absence de régulation laisse les systèmes de contrôle industriel

et les réseaux de données critiques exposés aux cyberattaques, ransomwares et au cyber-espionnage. Selon F. I. Zo'o, « l'arsenal juridique de la majeure partie des Etats Membre de l'UA est loin d'être congruent pour constituer une réponse idoine à l'évolution des délits relatifs aux TIC » (Zo'o, 2021, paragr. 2.). Néanmoins, des États comme le Nigéria, l'Afrique du Sud et le Maroc ont commencé à combler le retard avec des lois sur la cybercriminalité qui servent désormais de modèles pour le reste du continent. Malgré les efforts particuliers, l'Afrique fait face à un défi d'harmonisation. La Convention de Malabo de l'Union africaine sur la cybersécurité encourage les États membres à identifier les infrastructures critiques et à renforcer la sécurité. Mais la convention nécessite encore une ratification plus large pour devenir un standard uniforme sur tout le continent. Le problème s'amplifie sur le continent par le manque d'une position commune africaine.

- Le manque d'une position commune de l'Union africaine : la fragmentation politique reflète la difficulté de concilier des positions africaines face à des chocs qui exigent des réponses rapides et coordonnées. Le manque d'une position commune opérationnelle de l'Union africaine met en évidence des divergences d'intérêts nationaux. Bien que l'Union développe des stratégies continentales, la mise en œuvre est souvent entravée par une faible intégration régionale et une réticence des États membres à céder la souveraineté. Une chose qui affaiblit la position commune de l'Union africaine et elle piétine la lutte contre des réseaux cybercriminels sur le continent africain. Selon N. Ifeanyi-Ajufo, « *l'Afrique reste la région la plus faible en termes de digitalisation, ce qui a un impact sur l'approche de la cybersécurité* » (Ifeanyi-Ajufo, 2023, p. 1.). Pour elle, en termes d'infrastructures, l'Afrique est à la traîne en raison de divers facteurs, notamment la dépendance technologique et le manque d'harmonisation. De ce fait, N. Ifeanyi-Ajufo écrit ce passage :

L'Union africaine, contrairement à l'UE, n'exerce pas la même influence régionale et est reléguée au statut d'observateur dans les négociations sur la cybercriminalité. La limitation empêche l'UA de parler au nom des États membres ou de les demander des comptes sur les questions numériques. L'approche individualisée de la gouvernance dans les pays africains a un impact sur la cybergouvernance. Bien que l'Union africaine ait commencé à rechercher une position africaine unifiée sur la cybersécurité, un simple document d'orientation n'équivaut pas nécessairement à un consensus, comme le montre l'impact limité de la convention de Malabo. (Ifeanyi-Ajufo, 2023, p. 1.).

Le manque d'une position unifiée et d'une application homogène des cadres juridiques au sein de l'Union africaine, illustré par la lenteur de ratification de la Convention de Malabo (2014), fragilise la coopération transfrontalière et offre aux réseaux cybercriminels des zones de non-droit.

En somme, la forte dépendance technologique du continent africain envers l'extérieur, en matière de matériel, de logiciels et de capitaux, nécessite de repenser la souveraineté numérique, en s'appuyant notamment sur les stratégies d'architecture souveraine mises en œuvre en Iran. Autrement dit, la quête de la souveraineté numérique en Afrique exige de réduire la dépendance à l'égard des infrastructures, des logiciels et des financements étrangers en s'inspirant de modèles de résilience et de localisation comme celui de l'Iran, tout en les adaptant aux réalités démocratiques du continent.

2.2. Le modèle de développement technologique de l'Iran comme boussole pour l'Afrique

L'adoption d'un modèle d'autosuffisance technologique inspiré de l'Iran, forgé par des décennies d'isolement et de sanctions économiques, offre une perspective radicale de souveraineté. L'escalade technologique iranienne offre une voie pragmatique vers l'autonomie, nécessitant une adaptation prudente par l'Afrique pour renforcer sa souveraineté sécuritaire. L'Iran émerge comme une puissance technologique qui offre une « boussole » potentielle pour les États africains cherchant à renforcer la souveraineté technologique et industrielle. Le modèle iranien repose sur l'investissement massif dans l'éducation et les STEM et la stratégie de « l'économie de résistance ».

- L'investissement massif dans l'éducation et les STEM : l'Iran a misé sur la formation de la population, atteignant des taux d'alphabétisation très élevés et produisant un grand nombre de diplômés en sciences, technologie, ingénierie et mathématiques (STEM), avec une forte parité de genre dans l'enseignement supérieur. Les universités techniques se multiplient dans tout le pays et des centaines de milliers d'étudiants se dirigent vers les filières scientifiques. L'affirmation ci-dessous de N. Déjoui illustre bien les résultats de la politique iranienne de la modernisation de l'enseignement supérieur :

L'Iran formerait chaque année entre 230 000 et 234 000 ingénieurs, soit davantage que la France et l'Allemagne réunies, et à un niveau comparable à celui des États-Unis. C'est ce que révèlent les données relayées par la chaîne de télévision française *BFMTV* et l'Institut de statistique de l'UNESCO. (Déjoui, 2026, p. 1.).

Pour N. Déjoui, la capacité de formation explique pourquoi l'Iran est souvent cité parmi les grands pôles mondiaux de production de profils techniques ; malgré un contexte de sanctions et de fortes tensions régionales. En effet, le pays a massivement développé son enseignement supérieur technique, notamment aux sciences, à l'ingénierie et aux technologies, dans une logique d'autonomie industrielle et de montée en gamme du capital humain, (Déjoui, 2026, p. 1.). Ainsi, ce système mise fortement sur la formation de centaines de milliers d'étudiants et d'ingénieurs dans les filières scientifiques et techniques, illustrant qu'un pays peut bâtir une base technologique solide en investissant d'abord dans ses propres universités. Pour l'Afrique, cela

souligne l'importance de former des ingénieurs et des experts locaux pour réduire la dépendance technologique.

- **La stratégie de « l'Économie de Résistance »** : face aux sanctions, Téhéran a favorisé la production locale et l'innovation indigène plutôt que l'importation, créant une base industrielle résiliente dans des secteurs clés. Le développement d'avions de chasse (comme le HESA Kosar) et d'hélicoptères de conception nationale montre qu'une base industrielle locale est vitale pour la souveraineté. Le modèle iranien, fondé sur la production locale face aux sanctions. Concernant cette particularité iranienne, A. Kharief a écrit ceci :

Ce qui distingue la stratégie iranienne n'est pas la sophistication technologique, mais la logique économique qui la sous-tend. Un drone Shahed coûte environ 20 000 dollars. Un missile de croisière américain pour l'intercepter : deux millions. Déployez cent drones, et vous obligez l'adversaire à dépenser deux cents millions de dollars pour se défendre, indépendamment des dégâts causés. (A. Kharief, 2026, p. 1.).

La doctrine iranienne est simple, presque brutale dans sa logique : là où vous ne pouvez rivaliser en précision, submergez par le nombre. Là où vous ne pouvez égaler la technologie, épuisez les finances. Les drones iraniens ne visent pas à détruire une cible avec précision. Ils visent à saigner l'adversaire. (A. Kharief, 2026, p. 1.). L'objectif, selon le spécialiste, est de multiplier les petits équipements peu coûteux et rapides afin de causer de lourdes pertes en cas d'invasion ennemie, rendant ainsi impossible le contrôle du territoire. (A. Kharief, 2026, p. 1.). La stratégie de l'économie de résistance inspire les Africains en incarnant une rupture avec la dépendance extérieure. Ainsi, à l'ère de la transition numérique, la souveraineté numérique et la cybersécurité en Afrique constituent des défis stratégiques majeurs pour s'affranchir des dépendances technologiques extérieures et protéger les infrastructures critiques face à la hausse des cyberattaques.

2.3. Les défis de la souveraineté numérique et de la cybersécurité en Afrique

L'Afrique est de plus en plus connectée à l'Internet. Les entreprises, les infrastructures, les gouvernements, les citoyens et les industries clés sont de plus en plus liés à l'Internet. (Internet Society et Commission de l'Union africaine, 2017, p. 7.). La souveraineté numérique et la cybersécurité sont des impératifs stratégiques pour l'Afrique, visant à maîtriser les infrastructures, données et choix technologiques face aux cybermenaces croissantes. Il s'agit des piliers stratégiques fondamentaux pour le continent africain et le garant de la protection des économies nationales en pleine transformation digitale. Face à une transformation accélérée, le continent cherche à maîtriser les infrastructures, les données et les choix technologiques pour contrer des cybermenaces en pleine expansion. Les africains connaissent la plus forte augmentation mondiale de cyberattaques par organisation. Selon Check Point Research,

« l'Afrique a connu le plus grand volume d'attaques avec 2 960 attaques hebdomadaires par entreprise, suivie de l'Amérique latine avec 2 667 attaques hebdomadaires par entreprise » (Check Point Research (CPR), 2024, p. 1.). Les secteurs financiers, les administrations publiques et les infrastructures critiques sont les plus ciblés. En cela, la souveraineté numérique est devenue une condition de la liberté stratégique et de la sécurité continentale.

Au total, le conflit souligne l'urgence pour l'Afrique de renforcer la souveraineté stratégique pour se mettre à l'abri des conséquences de rivalités lointaines. Ainsi, le modèle iranien suggère des pistes pour l'Afrique. De ce fait, la souveraineté numérique en Afrique vise à maîtriser les infrastructures, les données et les technologies pour assurer une autonomie stratégique. Les enjeux clés incluent le renforcement des capacités institutionnelles, réglementaires et stratégiques de l'Union africaine, la protection des données locales et la construction des datacenters, la promotion d'innovations locales et la nécessité de l'intégration de la cyberéducation dans les réformes éducatives en Afrique et la multiplication des alliés stratégiques de l'Union africaine en matière de la technologie.

- **La nécessité du renforcement des capacités institutionnelles, réglementaires et stratégiques de l'Union africaine :** la souveraineté numérique de l'Afrique est impérativement liée au renforcement des capacités institutionnelles, réglementaires et stratégiques de l'Union africaine. Face à une forte dépendance technologique et aux cybermenaces, le continent doit, sous l'égide de l'Union africaine, créer un cadre unifié pour maîtriser les données, les infrastructures et la réglementation. La mise en œuvre du cadre de politique de données de l'Union, comme Data Policy Framework, est essentielle pour la gouvernance des données, la localisation des données et la création d'un marché numérique unique africain. La construction de datacenters en Afrique dans la politique de l'Union africaine est le levier fondamental pour garantir la protection des données locales et assurer la souveraineté numérique du continent. L'opération est donc essentielle pour passer de la dépendance à la maîtrise de l'information. Pour réussir le pari, l'Afrique doit coupler la construction des datacenters avec le développement massif d'énergies renouvelables pour garantir l'invulnérabilité. De plus, dans le cadre réglementaire et juridique, l'application de la *Convention de Malabo sur la cybersécurité et la protection des données personnelles* (2014) est cruciale pour harmoniser les politiques nationales. Enfin, le renforcement des capacités de l'Union africaine est nécessaire pour réguler les plateformes étrangères comme transparence fiscale et audit des algorithmes, afin de favoriser l'émergence d'un écosystème d'innovation local.

- **La promotion d'innovations locales et la nécessité de l'intégration de la cyberéducation dans les réformes éducatives en Afrique :** la promotion d'innovations locales

en matière de cyber-sécurité est essentielle pour garantir la souveraineté numérique et adapter les solutions aux menaces spécifiques de chaque territoire. Elle permet de réduire la dépendance technologique extérieure tout en stimulant l'écosystème économique local. Ainsi, pour développer efficacement un vivier d'innovations locales, il faut un soutien à la recherche et au développement en finançant des projets axés sur des technologies de pointe comme l'intelligence artificielle appliquée à la détection. En outre, les innovations peuvent aussi être soutenues par une politique de cyberéducation intégrée aux réformes éducatives permettant de combler le déficit de compétences. Il s'agit d'intégrer la cybernétique dès l'école primaire et secondaire et dans l'enseignement supérieur permettant de former une nouvelle génération de talents capables de faire face aux attentes du marché du travail africain.

Au niveau primaire et secondaire, l'objectif sera de former les jeunes à maîtriser les outils technologiques plutôt qu'à les subir. Il s'agit d'initier les jeunes aux bases du fonctionnement de l'ordinateur afin de développer chez eux l'esprit de créativité technologique et numérique. Quant au niveau supérieur, le travail de base des étudiants et des enseignants-chercheurs sera l'utilisation de l'intelligence artificielle et l'analyse de données. Cela permettra de produire des compétences numériques demandées par les services publics et les entreprises privées demandeurs de main-d'œuvre qualifié en informatique, en logistique et en service. Grâce à la politique de cyberéducation, les jeunes Africains pourront saisir des opportunités sur le marché du travail à distance. Ainsi, l'intégration de la cybernétique et des technologies numériques dans les cursus scolaires africains est un levier stratégique pour transformer l'éducation en un moteur de développement économique. La politique, visant à former des citoyens numériquement autonomes, nécessite une souveraineté technologique renforcée, passant par la diversification des partenariats.

- La multiplication des alliés stratégiques de l'Union africaine en matière de la technologie : l'Union africaine doit diversifier les partenariats pour garantir l'indépendance numérique et la souveraineté technologique. Il s'agit d'une façon de réduire la dépendance numérique vis-à-vis des infrastructures étrangères et éviter de dépendre d'un seul fournisseur ou partenaire étranger, notamment en matière d'intelligence artificielle et de centres de données.

Conclusion

Le conflit de 2026 en Iran marque une transition vers une guerre automatisée grâce à l'usage massif de l'intelligence artificielle, des drones et des armes hypersoniques. Le conflit transforme le Moyen-Orient en un laboratoire technologique où la suprématie technique surpasse la masse humaine. Il démontre qu'aucun pays n'est invulnérable sans une maîtrise des

infrastructures de données et une formation technologique poussée. La souveraineté nationale dépend désormais du contrôle des technologies, le cyberspace s'imposant comme un nouveau champ de bataille. La guerre hybride mêle cyberattaques, désinformation et mercenariat numérique, offrant des leçons critiques pour les États africains. Face aux menaces, l'Afrique doit repenser de manière urgente la souveraineté numérique et la sécurité globale. Le modèle de développement technologique iranien peut alors servir de boussole aux nations africaines pour assurer l'autonomie du continent. L'Iran prouve l'efficacité d'armements à bas coût pour déstabiliser les systèmes de défense aérienne hautement sophistiqués et onéreux. La doctrine de défense inspire le continent africain dans la volonté de réduire la dépendance envers l'Occident et la Chine. Pour y parvenir, l'Afrique doit unifier les politiques via l'Union africaine, sécuriser les données, former la jeunesse et diversifier les partenariats.

Références bibliographiques

- Africa Defense Forum (adf), 2022, *La défense contre les menaces hybrides : comment la haute technologie et les tactiques émergentes mettent l'Afrique en danger*,. Les menaces hybrides Volume 15, 2ème trimestre sur l'<https://adf-magazine.com> › ADF_V15N2_FR
- ASSIGNON Carole, 2026, *La guerre en Iran vue depuis l'Afrique*. Programme francophone de la Deutsche Welle (DW), sur <https://www.dw.com> › iran-guerre-israel-usa-afrique-dr.
- AZIMI Amir, 2026, *L'Iran semble avoir élaboré une stratégie fondée sur la dissuasion et l'endurance*. BBC News Afrique sur <https://www.bbc.com> › afrique › articles.
- Check Point Research (CPR), 2024, *Rapport sur la hausse record des cyberattaques dans le monde depuis les deux dernières années*. Check Point Research (CPR) sur <https://engage.checkpoint.com> › items › report--cyber-se...
- COELHO Ophélie, 2025, "Le numérique africain face aux dépendances structurelles et à l'impérialisme privé". *Revue Recherches Internationales*, pp.137-162. sur <https://shs.cairn.info/revue-recherches-internationales-2025-1-page-137?lang=fr>
- DIOUF Daouda, 2026, *Complexe, hybride et technologique : le conflit en Iran illustre les transformations de la guerre*. Le Soleil, sur <https://fr.news.yahoo.com/complexe-hybride-technologique-conflit-iran>.
- DÉJOUÏ Nadja, 2026, *L'équation iranienne : ingénieurs, drones et souveraineté*. Journal tunisien L'Économiste Maghrébin, sur <https://www.leconomistemaghrebin.com> › Blog
- FOUCHER Laure, 2026, *La guerre israélo-américaine contre l'Iran*, Fondation pour la recherche stratégique (FRS), sur <https://www.frstrategie.org> › publications › autres › gu
- IFEANYI-AJUFO Nnenna, 2023, *L'état actuel de la cybersécurité en Afrique est la tendance à la cyber-militarisation de la cybergouvernance*. Global Economic Governance Programme (GEG), sur <https://www.geg.ox.ac.uk/content/nnenna-ifeanyi-ajufo>

- Internet Society et Commission de l'Union africaine, 2017, *Lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique*. Internet Society Portal.
- INTERPOL, 2026, *Rapport d'évaluation des cybermenaces en Afrique 2025*,. Lyon: INTERPOL, sur <https://cybersecuritymag.africa> › CYBER-ACTU
- KHARIEF Akram, 2026, *Dans l'ombre du Shahed : L'épopée du programme de drones iranien*. French Edition. Amazon, sur www.amazon.fr/Dans-lombre-Shahed-Légal-programme
- LOKOSSI Maxime, 2025, *Cybersécurité en Afrique : les stratégies du Ghana, du Kenya et du Bénin face aux menaces numériques*,. Digital Frontiers Institute Digital Frontiers Institute.
- MARTIAL Paul, 2026, *L'Afrique face aux chocs de la guerre contre l'Iran*. NPA-L'Anticapitaliste, sur <https://lanticapitaliste.org> › arguments › international.
- RACHID Najah Idrissi Moulay, 2024, *La Cybersécurité en Afrique : Enjeux, Défis et Opportunités*. AMTS Group Africa, sur <https://mtsgroup.ma/cyber-security-experts-maroc-afrique/>
- ROMANO Camille, 2024, *Qu'est-ce que les « Fattah », ces missiles hypersoniques balistiques utilisés par l'Iran contre Israël ?* sur <https://www.publicsenat.fr> › Actualités › International
- SIMON Paul, 2026, *Iran : comment le fiasco des États-Unis contribue à remodeler l'équilibre des forces*. Le Vent Se Lève (LVSL), sur <https://lvsl.fr/iran-comment-le-fiasco-des-etats-unis-contribue-a-remodeler-lequilibre-des-forces/>.
- SOULÉ Folashadé, 2023, *Rivalités géopolitiques et partenariats numériques en Afrique. Stratégies d'adaptation et défis*. Études de l'Ifri.
- VAUGOUDE Martin, 2026, *Guerre au Moyen-Orient : qui frappe qui ?* Le Télégramme, sur <https://www.letelegramme.fr/monde/guerre-au-moyen-orient-qui-frappe-qui-6995111.php>.
- VIRGINIE Robert, 2026, *La guerre en Iran entre dans une deuxième phase où la technologie bat l'idéologie*. Les Echos, sur <https://www.lesechos.fr> › Monde › Enjeux internationaux.
- Voxafrica, 2026, *Diplomatie : La CEDEAO a exprimé*. Voxafrica.
- WEBGRAM, 2025, *La Souveraineté Numérique en Afrique : Enjeux Stratégiques, Défis et Opportunités pour une Maîtrise Continentale des Données et des Technologies*. Agence WEBGRAM.
- ZO'O Ferdin Isaac, 2021, *Les réponses juridiques africaines pour la prévention et la répression de la cybercriminalité*. Revue mensuelle de publication en droit international, N o 010 - Avril 2021, sur <https://www.academia.edu> › LES_REPONSES_JURIDI