Revue Internationale du Chercheur
ISSN : 2726-5889
Volume 6 : Numéro 1

L'INTELLIGENCE ARTIFICIELLE ET LE TERRORISME

ARTIFICIAL INTELLIGENCE AND TERRORISM

ALEMAWO Komlan
Maître de Conférences Agrégé en droit privé et sciences criminelles, Doyen de la Faculté de Droit et des Sciences Politiques
Faculté de Droit et des Sciences Politiques
Université de Kara
Laboratoire de Droit et des Sciences Politiques
Togo
komanoel@yahoo.fr

FAWIE Koboyo
Doctorant en droit privé
Faculté de Droit et des Sciences Politiques
Université de Kara
Laboratoire de Droit et des Sciences Politiques
Togo
koboyofawie@gmail.com

Date de soumission : 10/02/2025

Date d'acceptation : 18/02/2025

Pour citer cet article : **ALEMAWO**, **K.** & **FAWIE**, **K.** (2025), « L'intelligence artificielle et le terrorisme », *Revue Internationale du Chercheur*, « Volume 6 : Numéro 1 », pp. 1132 – 1158.

Digital Object Identifier : https://doi.org/10.5281/zenodo.15073671.

Cet article a été rédigé et publié grâce à la subvention du Projet d'Appui à la mise en œuvre de la Réforme de l'Enseignement supérieur en Sciences et Ingénieries (**PARESI**).

Résumé

L'intégration croissante de l'intelligence artificielle (IA) dans les stratégies de lutte contre le terrorisme par les États de l'Afrique de l'Ouest constitue un enjeu actuel majeur. Cette région, hélas marquée par des menaces persistantes, pourrait tirer parti de l'IA pour renforcer sa sécurité et sa stabilité. En effet, cette technologie offre des perspectives inédites, tant en matière de prévention que dans les opérations tactiques antiterroristes. Toutefois, l'usage de l'IA soulève des questions complexes, notamment sur le plan éthique et juridique, en raison des risques qu'elle comporte. Il est donc crucial de concilier les potentialités de l'IA avec les défis qu'elle engendre, en veillant à un cadre d'utilisation rigoureux et responsable. Une voie prometteuse serait de promouvoir des recherches approfondies au sein des États de l'Afrique de l'Ouest afin de développer des systèmes d'armement défensifs et offensifs efficaces qui respectent strictement les normes éthiques et juridiques en vigueur. Dans ce contexte, la présente contribution entend démontrer que l'IA pourrait constituer un atout stratégique déterminant dans le renforcement des réponses face au terrorisme en Afrique occidentale, à condition que son utilisation respecte pleinement les droits et libertés fondamentaux.

Mots clés

Arme ; États ; IA ; Juridique ; Terrorisme.

Abstract

The growing integration of artificial intelligence (AI) into counter-terrorism strategies by West African states is a major current challenge. This region, unfortunately marked by persistent threats, could benefit from AI to strengthen its security and stability. Indeed, this technology offers unprecedented prospects, both in terms of prevention and in tactical anti-terrorist operations. However, the use of AI raises complex issues, particularly in ethical and legal terms, due to the risks it entails. It is therefore crucial to reconcile the potential of AI with the challenges it poses, by ensuring a rigorous and responsible framework for its use. One promising avenue would be to promote in-depth research within West African states to develop effective defensive and offensive weapons systems that strictly comply with current ethical and legal standards. In this context, this paper aims to demonstrate that AI could be a decisive strategic asset in strengthening responses to terrorism in West Africa, provided that its use fully respects fundamental rights and freedoms.

Keywords

Weapon ; States ; AI ; Legal ; Terrorism.

Introduction

Recherche de solutions contre le terrorisme. Le terrorisme, fléau ancré dans le monde depuis un certain temps (**PAJON** & ***alii***, 2004), constitue un défi redoutable pour l'humanité. Lutter contre cette menace demande un engagement sans relâche, un véritable chemin semé d'embûches où les experts, en quête de solutions, s'attellent à la tâche avec une détermination de pèlerin. Parmi les propositions émises, l'intelligence artificielle (IA) émerge comme une piste prometteuse. Dans ce sillage, Li MENG, ancien vice-ministre chinois des Sciences et technologies, affirmait que : « *Si nous utilisons correctement l'intelligence artificielle, nous serons capables de savoir à l'avance qui pourrait être un terroriste, qui pourrait faire quelque chose de mauvais* » (**LEFORT-LAVAUZELLE**, 2018). Cette déclaration montre combien il est crucial de mener une réflexion afin de mieux cerner les contours de la relation potentielle entre l'IA et le terrorisme.

Complexité de la définition du terrorisme et de l'IA. Le terrorisme, au contenu juridique flou et difficilement cernable, est une notion en perpétuel débat. Mais l'une des significations intéressantes et convaincantes est celle selon laquelle cette notion peut être comprise comme des « *agissements criminels destinés à semer l'épouvante dans la population civile, par leur caractère meurtrier systématiquement aveugle* » (**CORNU**, 2018). Ces agissements prennent souvent la forme d'un attentat dans les lieux publics. De façon concrète, ce sont des agissements qui, incriminés en eux-mêmes et en toutes circonstances, comme atteinte aux personnes et aux biens, revêtent la qualification spécifique d'actes de terrorisme dans le cas où ils sont en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur (**CORNU**, 2018). Plusieurs solutions sont recherchées pour lutter contre ce type d'agissements. Au rang de celles-ci, se trouve l'IA, qui est un concept polysémique. En effet, il est assez complexe, à cet instant, de trouver une définition unanime et consensuelle de ce concept qui peut renvoyer à l'« *IA forte* »[1] lorsqu'elle est généralisée et à l'« *IA faible* »[2] lorsqu'elle est spécialisée. Cependant, la signification la plus réaliste est celle qui aborde l'IA comme la « *capacité des machines à*

[1] L'« *IA forte* » renvoie à une forme hypothétique d'IA qui possède des capacités cognitives générales similaires à celles d'un être humain. Elle serait en mesure de comprendre, d'apprendre et de s'adapter à une large gamme de tâches de façon autonome. Elle est pour l'instant un idéal chimérique, même si des IA comme *ChatGPT* s'en approchent un peu.

[2] L'« *IA faible* » est fabriquée pour accomplir une tâche spécifique ou un ensemble limité de tâches. Elle n'a pas de conscience, de compréhension ou de cognition humaine et ne peut effectuer de tâches en dehors de son domaine de spécialisation. Elle est exploitée dans les assistants virtuels (Alexa, Siri ou Google Assistant), les systèmes de recommandation (Netflix ou Amazon), la reconnaissance faciale, les voitures autonomes, etc.

réaliser des tâches qui requièrent normalement l'intelligence humaine ; comme l'identification de règles, l'apprentissage par l'expérience, la réalisation de prédictions ; que ce soit dans l'espace numérique ou au travers d'un algorithme pilotant un système réel » (**GARY,** 2021).

Résurgence de la question épineuse de la lutte contre le terrorisme. La question épineuse de la lutte contre le terrorisme qui gangrène le monde se pose depuis fort longtemps. Elle a été remise sur la table des discussions à la suite des attentats du 11 septembre 2001, perpétrés par Al-Qaïda, et intensifiée par l'émergence de récentes exactions commises par le groupe État islamique. Les discussions autour de cette question dépassent largement l'aspect technique pour englober, également ceux politique, juridique, voire idéologique (**DUBUISSON**, 2017). La présente contribution tentera d'examiner les enjeux et les défis inhérents à l'utilisation de l'IA dans la lutte contre le terrorisme dans la plupart des États, avec un regard précis et particulier sur ceux de l'Afrique de l'Ouest qui sont en proie à ce phénomène. L'on s'interroge déjà sur la manière dont cette technologie pourrait aider à combattre les terroristes en Afrique de l'Ouest.

Persistance du terrorisme en Afrique de l'Ouest. L'Afrique de l'Ouest est le théâtre d'activités terroristes depuis plusieurs décennies, mais la situation a connu son paroxysme à la suite de la chute de Kadhafi en 2011, qui a favorisé la circulation des armes et des combattants dans la région (**KONÉ**, 2022). Les groupes terroristes majeurs qui donnent du fil à retordre aux États de cette région sont : le Groupe de soutien à l'islam et aux musulmans (EIGS), le Boko Haram, l'État islamique en Afrique de l'Ouest (ISWAP), l'État islamique au Grand Sahara (EIGS) au Sahel, etc. (**CENTRE D'ÉTUDE STRATÉGIQUE DE L'AFRIQUE**, 2017). Ces derniers ont mené des attaques meurtrières contre les forces de sécurité, les populations civiles, les centres de santé, les écoles, etc., dans plusieurs États de cette partie de l'Afrique, notamment le Burkina Faso, le Mali, le Nigeria, le Niger, le Bénin, la Côte d'Ivoire, le Sénégal et le Togo (**HUMAN RIGHTS WATCH**, 2022). Concrètement, ces attaques sont menées aussi bien par terre, en mer, dans les airs que dans le cyberespace (**MAINGUY**, 2022). Quelle a été alors la réaction des États face à ces agissements malveillants ?

Réactions contemporaines des États face aux menaces terroristes. Pour le moment, la réponse régionale, continentale et internationale aux menaces terroristes dans cette partie de l'Afrique repose sur la coopération militaire, politique, économique et humanitaire. Bien que cette coopération rencontre de grands défis, il est important de relever qu'au niveau régional,

le Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest (GIABA) a reconnu que l'essor de technologies émergentes, dont l'intelligence artificielle, appelle à renforcer la cybersécurité pour contrer le financement du terrorisme en Afrique de l'Ouest (**GROUPE INTERGOUVERNEMENTAL D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE DE L'OUEST**, 2022). À l'échelle continentale, lors de la 1267e session du Conseil de paix et de sécurité de l'Union africaine (UA) du 20 mars 2025, un Communiqué a souligné l'impact de l'IA sur la paix, appelant à l'élaboration de régulations pour prévenir son usage malveillant (**UNION AFRICAINE**, 2025). Au plan international, plusieurs approches de solutions sont proposées pour pouvoir venir en aide aux États victimes de ce phénomène. Au rang de celles-ci, figure le déploiement de drones armés militaires, bien que certains en fassent déjà usage. Cette suggestion a été faite par les États-Unis d'Amérique qui envisagent de déployer des drones de reconnaissance non armés sur les côtes pour la lutte contre le terrorisme dans ces États. Ils sont en pourparlers avec le Bénin, le Ghana et la Côte d'Ivoire (**AGENCE ECOFIN**, 2024). Ces initiatives illustrent combien l'IA s'impose désormais comme un enjeu stratégique dans la lutte antiterroriste.

Énoncé de la problématique. Dans un contexte où l'IA devient un levier stratégique contre le terrorisme en Afrique de l'Ouest, une interrogation importante émerge parmi d'autres : **quelle interaction pourrait exister entre cette technologie et ce phénomène ?**

Méthodologie adoptée. Cette contribution entend démontrer que l'IA pourrait constituer un atout stratégique déterminant dans le renforcement des réponses face au terrorisme en Afrique occidentale, à condition que son utilisation respecte pleinement les droits et libertés fondamentaux. Pour ce faire, une méthodologie combinant l'approche qualitative et celle comparative de sources documentaires diverses a été retenue (**SISSOKO** & **DEMBÉLÉ**, 2023). Elle mobilise notamment les contributions doctrinales, les notes jurisprudentielles pertinentes, tout en tenant compte des différents travaux parlementaires.

Annonce de la démarche à suivre. La lutte contre le terrorisme, à l'ère de l'IA, exige de protéger efficacement la majorité des citoyens et leurs droits fondamentaux. Cette technologie constituerait ainsi en Afrique de l'Ouest un levier stratégique contre le terrorisme (**1)** et un puissant vecteur d'innovation catalysé par les menaces terroristes émergentes **(2)**.

1. L'IA, une arme précieuse contre le terrorisme

IA et les États de l'Afrique de l'Ouest. L'IA se présente comme une technologie potentiellement salutaire en particulier pour les États de l'Afrique de l'Ouest, confrontés depuis longtemps à la menace terroriste. Elle pourrait s'avérer précieuse dans leur quête de solutions idoines pour enrayer ce fléau persistant, en facilitant la conception et la mise à disposition de l'arsenal militaire, utilisable tant avec le concours des soldats qu'en autonomie. Elle pourrait de ce fait se constituer non seulement en outil de prévention **(1.1)**, mais également en moyen d'action direct **(1.2)**.

1.1. Une arme préventive

Éléments essentiels de la riposte contre le terrorisme. La proactivité et l'anticipation sont des composantes cruciales dans la lutte contre le terrorisme. La détection précoce des intentions malveillantes repose sur la surveillance des communications électroniques **(1.1.1)** ainsi que sur l'emploi de la reconnaissance faciale pour l'identification des terroristes **(1.1.2)**.

1.1.1. La surveillance des communications électroniques

Concept de communications électroniques. Les communications électroniques sont, à la lecture de l'article 4 de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques au Togo, l'ensemble des *« émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ou optique* ». Ce sont des échanges qui peuvent se faire via un réseau social, un site Internet ou un réseau téléphonique à partir d'un smartphone, d'un ordinateur, etc. Elles peuvent faire l'objet d'une surveillance dans le but de détecter les activités, les plans ou le financement d'une activité illégale comme le terrorisme, et d'identifier les responsables ou les complices.

De même, la surveillance des communications électroniques s'entend de l'« *ensemble des actions visant à travailler, surveiller, interpréter, collecter, analyser, utiliser ou accéder aux informations relatives aux communications électroniques d'une personne et d'un groupe* » (**MEDIA DEFENCE**, 2021). À noter que cette forme de surveillance électronique pourrait être menée par l'État, les particuliers ou les entreprises, et elle pourrait avoir des implications sur la liberté d'expression, le droit à la vie privée et à la sécurité. La surveillance des communications électroniques dont il s'agit ici est celle menée par les États à des fins sécuritaires, notamment la lutte contre le terrorisme. Pour ce faire, ils peuvent s'appuyer sur différentes technologies comme les logiciels espions, les drones, les réseaux de capteurs, les satellites ou les écoutes téléphoniques, etc.

Encadrement de ce procédé en droit positif togolais. Cette surveillance est encadrée par la loi pour éviter des abus ou de la surveillance de masse. En droit positif togolais, le législateur autorise les interceptions de sécurité lorsque la protection de la sûreté et de la sécurité de l'État, de l'ordre public national, etc., l'exigent, notamment en vue de prévenir et de combattre le terrorisme. Selon l'article 92 de la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques au Togo, c'est une action qui peut être déclenchée par « *le Premier ministre, le ministre chargé de l'Économie et des Finances, le ministre de la Défense, le Garde des Sceaux, le ministre de la Justice, le ministre de la Sécurité et de la Protection civile* ». La substance de cette disposition existe d'une manière ou d'une autre dans les législations des autres États de l'Afrique de l'Ouest[3]. Ils gagneraient à adopter une Convention sur la surveillance des communications électroniques en Afrique de l'Ouest qui trouverait un équilibre entre la surveillance à des fins sécuritaires et le respect des droits et libertés fondamentales des citoyens. Cette Convention, en prônant l'utilisation des technologies comme l'IA dans le contrôle des communications électroniques, renforcerait également l'arsenal juridique des États qui la ratifieront.

IA et la surveillance des communications électroniques. L'IA favorise la mise en place de systèmes qui permettent aux militaires d'avoir des renseignements qui pourraient les aider à déjouer les attaques terroristes avant qu'elles ne se produisent. Le développement international du terrorisme et sa sophistication rendent les moyens classiques d'interception de sécurité obsolètes, désuets et vétustes. De ce fait, le suivi des terroristes ne peut se faire à grande échelle à l'aide des moyens traditionnels ou classiques. Cet enjeu majeur constitue le moteur de l'évolution des dispositifs d'analyse des données techniques (**DRM**, 2019). Cette transformation doit impérativement garantir le respect des données personnelles et des libertés privées, écartant toute dérive vers la surveillance de masse.

Jurisprudence européenne relative à la surveillance de masse. En ce sens, la Cour de justice de l'Union européenne (CJUE) a rendu deux arrêts le 6 octobre 2020 (**CJUE**, 6 octobre 2020, affaire C-511/18, C-512/18, C-520/18 et affaire C-623/17) dont l'importance est non négligeable. La lecture superficielle de cette jurisprudence laisse entrevoir que la CJUE réitérerait « *le principe de condamnation d'une surveillance de masse, généralisée et*

[3] Les dispositions sur les communications électroniques existant dans les États de l'Afrique de l'Ouest : la Loi n° 2014-14 relative aux communications électroniques et à la poste en République du Bénin (Bénin), le Décret n° 09-2019/AN du 23 avril 2019 portant modification de la loi n° 0061-2008/AN du 27 septembre 2008 portant réglementation générale des réseaux et services de communications électroniques générale de réseaux et services de communications électroniques au Burkina Faso (Burkina Faso), etc.

indifférenciée, y compris dans un contexte de lutte contre le terrorisme » (**MAINGUY**, 2022). Par contre, une lecture beaucoup plus approfondie « *permet d'observer que l'appréciation de la CJUE est plus nuancée* » (**MAINGUY**, 2022). Elle a principalement reconnu qu'une législation nationale peut imposer aux fournisseurs et aux opérateurs de conserver des données de connexion à des fins de sécurité nationale. La Cour européenne des droits de l'homme (CEDH) a de son côté rendu deux arrêts le 25 mai 2021 (**CEDH**, 25 mai 2021, *Big Brother Watch* et autres c. Royaume-Uni, req. n° 58170/13, 62322/14 et 24960/15 et **CEDH**, 25 mai 2021, *Centrum för Rättvisa* c. Suède, req. n° 35252/08) dans lesquels elle précise les conditions dans lesquelles un régime de surveillance de masse des communications électroniques peut être compatible avec les articles 8 et 10 de la Convention européenne des droits de l'homme. Elle accepte que la surveillance de masse revête une importance vitale pour détecter les menaces contre la sécurité nationale, tout en précisant que cela pourrait potentiellement porter atteinte au droit au respect de la vie privée. Il ressort de ces différentes positions que la CEDH est plus compréhensive envers les États que la CJUE.

Espoirs suscités par l'IA en Afrique de l'Ouest. L'un des objectifs est de pouvoir favoriser l'automatisation de la surveillance « *de cibles de plus en plus individualisées ou d'organisations atomiques, comme des cellules terroristes de quelques individus et* [des] *groupes armés disséminés dans le Sahel* » (**DRM**, 2019) et dans le sud du Sahel. « *Une autre attente vis-à-vis de l'IA est de pouvoir détecter de nouvelles cibles dans la masse de données collectées* » (**DRM**, 2019) grâce à la surveillance électronique.

Les États de l'Afrique de l'Ouest, tirant parti du soutien d'une agence de renseignement étrangère maîtrisant des technologies avancées basées sur l'IA ou en acquérant ce type de logiciels, pourraient accéder et analyser les communications cryptées des terroristes. Cette capacité renforcerait considérablement leur aptitude à neutraliser des projets d'attaques, notamment contre des installations militaires stratégiques des groupes terroristes. Par ailleurs, en utilisant des algorithmes sophistiqués pour surveiller les plateformes numériques, il deviendrait possible d'identifier et de localiser les figures clés de la propagande ou du recrutement terroriste. Une telle stratégie offrirait un levier inédit pour désorganiser voire démanteler des réseaux ennemis. De ce fait, plusieurs cellules clandestines, déjà en phase de préparation opérationnelle, pourraient être détectées et démantelées avant qu'elles ne puissent agir. De plus, l'IA, grâce à la reconnaissance faciale, permettrait aussi d'identifier et de neutraliser efficacement des individus terroristes, empêchant de cette façon la concrétisation d'attentats programmés.

1.1.2. L'utilisation de la reconnaissance faciale

Définition de la reconnaissance faciale. La reconnaissance faciale renvoie à une technologie biométrique qui permet de reconnaître le visage d'un humain et ainsi d'identifier formellement un individu. Elle constitue « *une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier* » (**COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS**, 2019). Il importe de préciser qu'elle prend place dans une palette plus large de techniques de traitement d'images vidéo. Elle se fait généralement en deux étapes importantes : « *la collecte du visage et sa transformation en un gabarit, puis la reconnaissance de ce visage par comparaison du gabarit correspondant avec un ou plusieurs autres gabarits* » (**COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS**, 2019).

Applications variées de la reconnaissance faciale. La reconnaissance faciale, à l'instar de tout procédé biométrique, peut répondre à deux fonctions différentes, notamment l'authentification [4] et l'identification [5] d'une personne. Elle pourrait être utilisée pour déverrouiller un appareil électronique, le contrôle d'accès physique à un lieu, la recherche d'une personne suspecte ou susceptible de commettre un attentat, etc. La reconnaissance faciale pourrait donc être une technologie efficace dans la reconnaissance des terroristes fichés lorsqu'ils mettent pied dans un État de l'Afrique de l'Ouest. Elle pourrait permettre, par exemple, le suivi de leurs déplacements afin d'anticiper toute action dangereuse qu'ils pourraient poser. Il convient à ce propos de préciser que l'« *efficacité de la reconnaissance faciale dépend de plusieurs facteurs clés : la qualité de l'image, la puissance de l'algorithme d'identification et l'accès à une base de données fiable* » (**KAROUTCHI**, 2016).

Leadership de la Chine dans l'utilisation de la reconnaissance faciale. La Chine, classée comme le pays qui utilise le plus largement la reconnaissance faciale, s'appuie sur le déploiement d'un réseau de plus de 200 millions de caméras équipées de systèmes d'IA. Elle utilise notamment le système Skynet, favorisant la couverture de tout le territoire avec des

[4] L'authentification vise à vérifier qu'une personne est bien celle qu'elle prétend être. Dans ce cas, le système va comparer un gabarit biométrique préenregistré (par exemple, stocké dans une carte à puce) avec un seul visage, par exemple celui d'une personne qui se présente à un point de contrôle, afin de vérifier si cette personne est la même. Cette fonctionnalité repose donc sur la comparaison de deux gabarits.

[5] L'identification vise à retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données. Dans ce cas, le système doit effectuer un test sur chaque visage capté pour générer un gabarit biométrique et vérifier si celui-ci correspond à une personne connue du système. Cette fonctionnalité repose ainsi sur la comparaison d'un gabarit avec une base de données de gabarits.

caméras reliées à une base de données nationale de visages, pour la notation sociale, la gestion de trafic ou pour prévenir des attentats. La reconnaissance faciale permet de surveiller les activités suspectes et de prévenir les menaces terroristes ou de subversion.

Pour la petite histoire, depuis 2014, le gouvernement chinois est sur le qui-vive à la suite d'une série d'attentats terroristes meurtriers, que les autorités ont imputée à des extrémistes du Xinjiang, inspirés par des messages islamistes venus de l'étranger. Les dirigeants mettent désormais à la disposition des forces de sécurité aux effectifs renforcés ce qui existe de mieux au monde en matière de technologie, afin d'instaurer un système de contrôle social qui touche essentiellement les Ouïgours (**LEFORT-LAVAUZELLE**, 2018).

Usage de la reconnaissance faciale en Afrique de l'Ouest. En Afrique de l'Ouest, les États pourraient utiliser des drones intégrant des caméras pour vérifier l'identité des voyageurs aux frontières, retrouver des personnes disparues ou détecter des individus suspects ou recherchés par la justice. Ainsi, l'IA pourrait faciliter l'identification des suspects, des victimes ou des témoins. Partant du fait que ce sont des données personnelles qui sont collectées dans ce processus et qu'il y a des risques de biais, chaque État de l'Afrique de l'Ouest devrait mettre en place une agence nationale chargée de le conseiller et de contrôler le respect de la loi dans l'utilisation de la reconnaissance faciale. Dans l'immédiat, ces États pourraient charger les autorités, les agences ou les instances de protection des données à caractère personnel de veiller à la bonne marche de ces activités.

Ces illustrations variées mettent en évidence le potentiel de l'IA en tant qu'outil préventif puissant contre le terrorisme en Afrique de l'Ouest. Toutefois, son efficacité ne doit manquer de reposer sur le strict respect des normes éthiques et juridiques garantissant la préservation des droits fondamentaux, notamment la vie privée. Une fois ces exigences intégrées, l'IA pourrait se révéler être une solution stratégique majeure, non seulement pour anticiper les menaces terroristes, mais aussi pour renforcer les capacités opérationnelles des États dans leur lutte contre ce fléau.

1.2. Une arme opérationnelle

Substitution de l'humain par l'IA. L'IA représente une technologie militaire dont le potentiel pourrait s'avérer décisif pour les États de l'Afrique de l'Ouest dans leur lutte contre le terrorisme, tout en minimisant les pertes humaines au sein des forces armées. Cette technologie pourrait se substituer à l'intervention humaine dans des situations délicates telles que le désamorçage d'engins explosifs **(1.2.1)** ou les attaques ciblées contre les groupes terroristes à l'aide de drones armés **(1.2.2)**.

1.2.1. Le désamorçage d'engins explosifs à distance (DEED)

Définition du DEED. Le DEED s'entend d'une méthode qui consiste à neutraliser ou à éliminer des engins explosifs improvisés (EEI) sans contact direct avec l'engin. C'est aussi une technique qui permet de neutraliser des EEI à l'aide d'un robot ou d'un dispositif télécommandé, en l'absence de toute intervention d'un démineur humain sur les lieux. Cette démarche permet, face à la menace terroriste, de réduire considérablement les risques que courent les militaires et les démineurs lors des différentes opérations de désamorçage. Sans oublier que la perte dans les populations civiles est également minimisée.

Appréhension des EEI. Les EEI sont quant à eux appréhendés comme des armes non conventionnelles qui peuvent prendre n'importe quelle forme et être activées de diverses manières. Les cibles de ces armes sont aussi bien les soldats que les civils. Le type et la situation de l'EEI conditionnent les différentes manières de DEED. Les explosifs contrôlés, les systèmes de brouillage, les robots télécommandés, les drones, les canons à eau ou des fusils de précision, des outils à base d'IA, peuvent par exemple être utilisés pour désamorcer les EEI (**ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD**, 2015).

Utilisation des armes DEED par les forces militaires. Les forces armées utilisent le DEED pour renforcer leur lutte contre le terrorisme, particulièrement face à la menace croissante des EEI. Ces armes artisanales, fréquemment déployées par des groupes armés non étatiques, servent à attaquer ou intimider les populations en Afrique de l'Ouest. Ces dispositifs ont été recensés dans des attaques au Mali, au Nigéria, au Burkina Faso, au Togo et au Bénin (**ABATTAN** et **KONÉ**, 2024). L'utilisation du DEED conférerait aux forces armées un avantage stratégique majeur en réduisant les pertes en vies humaines et les dégâts causés par les engins explosifs. Cette technologie de pointe optimise les capacités opérationnelles sur le terrain en permettant des interventions plus précises et adaptées aux contextes les plus complexes. En renforçant la sécurité dans les zones sensibles, elle pourrait jouer un rôle crucial dans la stabilisation des régions vulnérables, où les risques liés aux explosifs constituent une menace persistante.

Par ailleurs, le DEED facilite une gestion proactive des situations critiques, minimisant les impacts sur les civils tout en améliorant la coordination entre les unités déployées. Il représente une avancée significative pour la modernisation des approches militaires. En consolidant les bases d'une défense plus efficace et durable, cette technologie ouvre la voie à de nouvelles solutions stratégiques, essentielles pour relever les défis croissants des conflits contemporains. L'une de ces solutions pouvant être les drones armés.

1.2.2. Le recours aux drones armés lors des opérations

Perception des drones armés. Les drones armés sont très souvent perçus comme des appareils aériens sans pilote qui peuvent lancer des missiles ou des bombes sur des cibles désignées. De nombreux États, tels que les États-Unis, l'Allemagne, le Royaume-Uni et la France, déploient ces dispositifs pour exécuter des frappes ciblées contre des adversaires militaires ou des groupes terroristes, notamment en Afrique de l'Ouest et dans d'autres régions (**TOUNKARA**, 2021).

Pourquoi utiliser l'IA dans les drones armés ? Le recours à l'IA pour effectuer le guidage des drones armés vise à améliorer leur capacité de reconnaissance, de détection et de suivi des cibles, ainsi que leur autonomie et leur précision (**HENRY** & **PAIANO**, 2023). De même, l'IA pourrait aider à éviter les dommages collatéraux et les erreurs d'identification en utilisant des systèmes d'identification d'amis ou d'ennemis (**HENRY** & **PAIANO**, 2023). Le Togo et le Niger ont par exemple passé commande de drones armés *Bayraktar* TB2 en 2021 pour renforcer leur capacité de défense et de sécurité (**ALLEN**, 2022). Ces appareils sont capables de voler pendant 24 heures au moins et de couvrir une distance de 150 km (**ALLEN**, 2022).

Défis inhérents à l'usage de l'IA dans les drones armés. Toutefois, l'usage de l'IA dans les drones armés n'est pas sans défis. Elle soulève des interrogations éthiques et juridiques importantes. *Primo*, le respect du DIH et des droits de l'homme, qui requiert que les frappes soient proportionnées, discriminantes et nécessaires, et qu'elles ne causent pas de souffrances inutiles ou excessives aux civils et aux combattants (**JOMIER**, 2021). *Secundo,* la responsabilité et la transparence des décisions de frappe, qui doivent être prises par des humains et non par des machines, et qui doivent être justifiées et contrôlées par des autorités compétentes (**JOMIER**, 2021) *Tertio et in fine*, les risques de prolifération et de course aux armements, qui pourraient entraîner une escalade de conflits et une instabilité régionale, si des acteurs non étatiques et des États hostiles avaient la capacité d'acquérir de telles armes (**JOMIER**, 2021).

Dégâts causés par les armes opérationnelles. Il importe de relever que ces diverses armes opérationnelles peuvent causer d'énormes dégâts ou des pertes en vies humaines. Au Togo, dans la nuit du 09 au 10 juillet 2022, sept enfants, confondus avec des terroristes, ont été tués. D'après les propos du Général Maganawe DADJA : « *Un aéronef (de l'armée togolaise) en patrouille nocturne a pris malencontreusement pour cible un groupe de personnes qu'il a confondu [avec] une colonne de djihadistes en mouvement* » (**LASSAAD**, 2022). Un événement similaire s'est également produit au Nigéria. Un drone de l'armée a tué par

accident au moins 85 civils lors d'une fête dans un village de l'État de Kaduna, le 5 décembre 2023, dans le nord-ouest du pays (**FRANCE 24**, 2023). Il s'agit de l'un des accidents de frappe aérienne militaire les plus meurtriers du pays.

Formation des militaires à l'utilisation des armes opérationnelles. Afin de prévenir efficacement ce type d'incidents, il apparaît crucial de renforcer, de manière pérenne, les compétences des militaires chargés de manipuler des armes dotées de capacités opérationnelles avancées. De façon concrète, une maîtrise rigoureuse de ces outils s'impose aux utilisateurs, en particulier aux forces armées concernées. Il en découle que l'enjeu de la formation et de l'entraînement est d'une importance capitale (**MAINGUY**, 2022). Cette nécessité repose aussi sur une prudence stratégique visant à contrer le danger d'une « *sur-confiance* » dans l'efficacité présumée des armes intégrant l'IA, notamment en raison de l'inévitable usure ou attrition qui affecte ces équipements en situation de conflit (**MAINGUY**, 2022).

Dans ce contexte, renforcer les alliances militaires, partager des technologies innovantes et établir un cadre juridique dédié en Afrique de l'Ouest apparaissent essentiels pour réguler et coordonner l'intégration de l'IA dans les stratégies militaires régionales.

Charte éthique relative à l'utilisation de l'IA dans la lutte contre le terrorisme ? À cet égard, la mise en place d'une charte éthique relative à l'utilisation de l'IA dans la lutte contre le terrorisme, sous l'égide de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), constituerait une démarche pertinente. Une telle charte aurait pour double objectif de réglementer ce domaine en pleine expansion tout en stimulant les recherches autour de l'IA pour pallier ses limites actuelles. En outre, elle marquerait un jalon significatif vers l'émergence d'un droit militaire adapté aux spécificités de l'IA en Afrique de l'Ouest.

Un encadrement réfléchi des recherches sur l'IA dans le contexte de la lutte contre le terrorisme permettrait de produire des armes technologiquement avancées, conformes à des normes de sécurité et de performance élevées. Ce processus pourrait transformer le combat contre le terrorisme en catalyseur de progrès pour l'IA, favorisant des innovations qui surmonteraient les contraintes liées à la conception et à l'utilisation de ces armes. Par conséquent, ce phénomène, bien que problématique, pourrait devenir un puissant moteur de recherche et de développement, contribuant ainsi à l'expansion et à la maturation de l'IA dans un cadre éthique et sécurisé.

2. Le terrorisme, un propulseur éminent de l'IA

Limites de l'IA ou la stimulation de la recherche ? Les imperfections actuelles de l'IA en tant qu'outil militaire devraient encourager les concepteurs à intensifier leurs recherches. Ces recherches avancées viseraient à permettre aux forces armées de chaque État de l'Afrique de l'Ouest de surmonter les défis qu'elles rencontrent dans la lutte contre le terrorisme, tout en respectant scrupuleusement les législations en vigueur et les principes éthiques. De ce fait, elles favoriseraient la conception mesurée de capacités défensives **(2.1)** et le développement encadré de capacités offensives **(2.2)**.

2.1. Une recherche axée sur la conception mesurée des capacités défensives

IA et forces armées de l'Afrique de l'Ouest. Dans le contexte ouest-africain, une armée dépourvue de capacités défensives véritables face à la menace terroriste pourrait rapidement se retrouver en difficulté, d'autant plus que les groupes terroristes disposent et manipulent des armements de dernière génération. Il devient donc impératif de développer en particulier des systèmes de défense antimissiles **(2.1.1)** ainsi que des systèmes de protection contre les cyberattaques **(2.1.2)**.

2.1.1. La conception des systèmes de défense antimissiles

Concepts relatifs aux systèmes de défense antimissiles. Les systèmes de défense antimissiles sont un ensemble de moyens de protection qui ont la possibilité de détecter et de détruire les missiles balistiques lancés par un ennemi vers un territoire. Cette définition montre combien chaque État de l'Afrique de l'Ouest devrait en posséder pour pouvoir mener une meilleure défense de son territoire. De tels systèmes incluant la technologie de l'IA permettraient de détecter, d'identifier, de suivre et d'intercepter les missiles balistiques lancés par des adversaires potentiels. Concrètement, l'« *IA peut apporter des avantages tels que l'amélioration de la réactivité, de la précision, de la fiabilité et de la robustesse des systèmes de défense antimissiles* » (**EKOUÉ**, 2022).

Nécessité de concevoir des systèmes de défense antimissiles. L'importance de concevoir ou de s'équiper de tels systèmes en Afrique de l'Ouest réside dans le fait que cette région est en proie à des activités terroristes et à des tensions géopolitiques qui pourraient impliquer l'usage des missiles balistiques par des acteurs hostiles (**ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES**, 2021). Ils pourraient contribuer au renforcement de la sécurité et de la stabilité de cette partie de l'Afrique, ainsi qu'à protéger les populations et les forces armées de ces différents États.

Les systèmes de défense antimissiles pourraient aider les militaires en leur offrant une capacité de dissuasion et de riposte face aux attaques de missiles, en réduisant les risques de dommages collatéraux et en augmentant la confiance et la coopération entre les pays alliés (**DIRECTION : AID**, 2021). Ils pourraient également « *favoriser le développement de compétences technologiques et scientifiques dans le domaine de l'IA et de la défense* » (**MINISTÈRE DES ARMÉES**, 2019).

États œuvrant à l'élaboration de systèmes de défense antimissiles. Les États-Unis, la Russie, la Chine, l'Inde, l'Israël et la France sont notoirement connus comme les principaux États qui possèdent et développent les systèmes de défense antimissiles. Les États d'Afrique de l'Ouest pourraient s'en inspirer utilement en commençant par mettre en place des centres d'études et de recherches sur le terrorisme propres à cette région, même s'il existe un Centre africain d'étude et de recherche sur le terrorisme (CAERT) à l'échelle continentale depuis 2004. Ces futurs centres permettraient de mener des recherches conformes à la législation afin de développer des systèmes de défense antimissiles d'une précision exceptionnelle et d'une capacité considérable. Une telle initiative renforcerait la sécurité régionale et améliorerait les stratégies de lutte contre les menaces terroristes persistantes en tenant compte des spécificités de cette région.

Acquisition de systèmes d'armement antimissiles en Afrique de l'Ouest. À ce jour, aucun État de l'Afrique de l'Ouest n'a officiellement annoncé l'acquisition de systèmes de défense antimissiles. Cependant, les dynamiques sécuritaires et les alliances internationales pourraient bientôt modifier cet état de fait. Cela souligne l'urgence, pour ces États, d'investir non seulement dans les infrastructures nécessaires à leur déploiement efficace, mais aussi dans le développement de telles technologies. La conception de ces systèmes ne constitue toutefois qu'une étape préliminaire. Assurer leur usage approprié et prévenir les cyberattaques devient tout de même crucial. En effet, ces dispositifs pourraient être ciblés par des groupes terroristes déterminés à en prendre le contrôle à des fins malveillantes. Par conséquent, il revient aux États de l'Afrique de l'Ouest, qu'ils soient acheteurs ou développeurs, d'instaurer des mesures de protection avancées, notamment en investissant dans des mécanismes sophistiqués de défense contre les intrusions numériques et en renforçant leur protection directe face à de telles menaces.

2.1.2. La conception des systèmes de riposte aux cyberattaques

Définition des systèmes de riposte aux cyberattaques. Les systèmes de riposte aux cyberattaques sont des outils, des stratégies et des procédures permettant d'anticiper, de

détecter et de réagir face aux attaques visant à compromettre la confidentialité, la sécurité ou l'intégrité des données, des réseaux ou des systèmes des États, des institutions ou des entreprises. En tout état de cause, prévenir le cyberterrorisme et lutter contre les menaces cyber implique une modernisation des outils numériques des États au-delà des seuls services de renseignement (**CAZENEUVE**, 2023).

Cyberattaques en Afrique de l'Ouest : un fléau grandissant. Les États de l'Afrique de l'Ouest devraient réfléchir à concevoir des systèmes de riposte aux cyberattaques, car cette partie occidentale de l'Afrique subit des menaces croissantes de la part de cybercriminels, de groupes terroristes, d'États hostiles ou de concurrents économiques. Ainsi, ces derniers cherchent non seulement à exploiter les vulnérabilités des infrastructures numériques, mais aussi à perturber les services cruciaux et à voler des informations sensibles dans le but de nuire à la stabilité sécuritaire, politique et sociale (**EDDÉ**, 2020). D'après une étude menée en 2019, cette région a subi plus de 6000 cyberattaques, causant des pertes estimées à 3,5 milliards de dollars (**LINDEMULDER** & **KOSINSKI**, 2024). Il est alors pertinent de s'interroger sur la manière dont ces États se préparent à éradiquer, ou à tout le moins, à contenir ce phénomène.

Convention de Malabo : cadre de régulation ? Pour relever ce défi, ces États ont commencé par élaborer des cadres légaux au niveau continental, la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel [6], et national avec l'adoption par chaque État de lois sur la cybersécurité et la lutte contre la cybercriminalité. De plus, chacun installe de son côté un centre d'alerte et de réaction contre les menaces cybernétiques. Ce qui a conduit par la suite à la création du Réseau africain des équipes d'intervention d'urgence informatique (AfricaCERT). Ce Réseau regroupe des équipes nationales chargées de répondre aux incidents de sécurité informatique, de partager des informations et de coordonner des actions. Il inclut actuellement treize (13) États de l'Afrique de l'Ouest.

Des axes de progression sont d'ores et déjà identifiables. Notamment le fait que, d'une part, les différents textes adoptés semblent perfectibles et que, d'autre part, ces États pourraient utilement investir davantage dans la recherche et dans l'innovation pour pouvoir profiter pleinement des opportunités qu'offrent les technologies émergentes comme l'IA.

[6] Cette Convention a été adoptée à Malabo le 27 juin 2014 et ne peut être uniquement ratifiée que par les États africains. Elle est rentrée en vigueur le 8 juin 2023 et ratifiée par 15 États africains à ce jour (Togo, Côte d'Ivoire, Mauritanie, Zambie, Sénégal, Rwanda, Namibie, Niger, Île Maurice, Mozambique, Guinée, Ghana, République démocratique du Congo, Cap-Vert et Angola).

IA et cybersécurité. L'IA permet par exemple de mettre en place des systèmes robustes qui permettent de lutter contre le terrorisme en ligne. C'est l'exemple du projet Cyber4Dev, qui est financé par l'Union européenne dans le but d'optimiser les capacités des États de l'Afrique en matière de cybersécurité et de lutte contre le terrorisme (**INTERPOL**, 2021). L'Institut national de recherche en informatique et automatique (INRIA) a développé en France un système de détection et de réponse aux cyberattaques (CDAR) qui utilise l'IA pour analyser les flux de données et détecter les anomalies, les intrusions et les attaques (**DUNN**, 2022). En effet, l'un des enjeux majeurs de l'IA française militaire de demain est le développement et l'exploitation de systèmes dits de « *cyberdéfense* » (**MAINGUY**, 2022). Ce terme aux contours larges englobe des pratiques variées, allant de la lutte contre les intrusions malveillantes à l'utilisation de logiciels espions visant à collecter des données sensibles ou perturber des systèmes critiques. Notamment les *kilwares*, outils pernicieux conçus pour contaminer délibérément des infrastructures stratégiques comme les hôpitaux, les usines chimiques, les centrales nucléaires, avec l'intention préméditée de causer des pertes humaines, parfois dans le cadre d'actions à visée terroriste (**MAINGUY**, 2022).

Les États de l'Afrique de l'Ouest gagneraient à s'engager résolument dans une recherche stratégique orientée vers le renforcement équilibré de leurs capacités, en mettant un accent particulier sur les dimensions défensives et offensives. Ce positionnement leur permettrait non seulement de mieux anticiper les menaces contemporaines, mais aussi de développer une posture proactive et dissuasive. L'approfondissement des capacités offensives s'impose comme un levier essentiel dans la dynamique de souveraineté et de puissance régionale.

2.2. Une recherche axée sur l'élaboration contrôlée des capacités offensives

Maîtriser les défauts des armes autonomes offensives. La limitation des impacts négatifs liés aux armes autonomes offensives repose nécessairement sur la conduite de recherches axées sur l'application des normes les plus strictes en la matière, tout en veillant au respect des législations existantes. Ces recherches permettraient ainsi le développement des armes autonomes entièrement indépendantes **(2.2.1)** ou celles nécessitant une intervention humaine **(2.2.2)**.

2.2.1. Les systèmes d'armes sans intervention humaine

Perception des armes sans intervention humaine. Les systèmes d'armes sans intervention humaine sont perçus comme des appareils autonomes offensifs qui sont en mesure de sélectionner et d'attaquer des cibles sans que l'homme n'intervienne, en utilisant l'IA pour analyser les données et prendre des décisions (**BRUUN**, 2022). Ce sont des systèmes d'armes

qui, lorsqu'ils sont activés, peuvent sélectionner et engager des cibles sans qu'il soit nécessaire ou possible pour un opérateur humain d'intervenir (**FONDATION FRIEDRICH-EBERT STIFTUNG**, 2015). Ils sont également connus sous l'appellation SALA.

SALA comme protection pour les soldats. L'un des arguments qui milite en faveur de la recherche et du développement de ce type d'armes est qu'elles pourraient aider à lutter contre le terrorisme, en réduisant les risques pour les soldats humains, en augmentant la précision et l'efficacité des frappes, et en diminuant les coûts des opérations militaires (**ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES**, 2019). Les États de l'Afrique de l'Ouest pourraient bénéficier des avantages de ces armes pour renforcer leur sécurité et leur stabilité s'ils investissent dans la recherche et dans l'innovation (**ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES**, 2019).

Enjeux soulevés par les SALA. Les recherches pour développer ce type d'armes sont encouragées par certains pays comme la Russie et la Chine (**MAINGUY**, 2022). Mais leur développement et leur déploiement posent d'innombrables défis techniques, juridiques et éthiques. « *Il faut notamment assurer que ces systèmes d'armes respectent le droit international humanitaire, qui impose des principes de distinction, de proportionnalité et de précaution dans l'attaque* » (**BRUUN**, 2022 ; **MAINGUY**, 2022). Il importe également de garantir la fiabilité, la transparence, la responsabilité et le contrôle humain de ces différents systèmes d'armes. L'adoption d'une approche multidisciplinaire est nécessaire pour pouvoir mener des recherches dans ce domaine. Une approche qui rassemblerait des experts en IA, en droit, en éthique, en sécurité et en politique.

Exemple de SALA : cas du sous-marin autonome *Sea Hunter*. Le sous-marin autonome *Sea Hunter*, développé par les États-Unis, est un exemple de système d'arme sans intervention humaine qui a la capacité de naviguer et de traquer des sous-marins ennemis pendant des mois sans que l'homme n'intervienne. L'utilisation d'une telle arme fait naître un débat juridique et éthique très complexe et controversé (**BRUUN**, 2022 ; **MAINGUY**, 2022). Cela se matérialise par la divergence des opinions sur la nécessité, la légalité, la moralité et la faisabilité de ces différentes armes (**BRUUN**, 2022 ; **MAINGUY**, 2022). D'une part, le Parlement européen ainsi que la campagne *Stop Killer Robots* appellent à une interdiction préventive de ces armes, au nom du respect de la dignité humaine, de la protection des civils et de la prévention des conflits (**COMITÉ INTERNATIONAL DE LA CROIX-ROUGE**, 2022). D'autre part, certains États ou industries défendent le droit de développer et d'utiliser

ces armes, au nom de la souveraineté, de la sécurité et de l'innovation (**COMITÉ INTERNATIONAL DE LA CROIX-ROUGE**, 2022). Depuis 2014, les États participant à la Convention sur certaines armes classiques discutent de la question des systèmes d'armes létales autonomes, mais n'ont pas encore abouti à un consensus sur un cadre juridique ou une politique commune.

Proposition d'encadrement juridique rigoureux de l'utilisation des SALA. Bien que cette contribution n'encourage pas prioritairement l'usage de ce type d'armements contre les terroristes, il importe de souligner qu'une interdiction absolue de leur utilisation limiterait les capacités des forces armées, d'autant plus que ces armes figurent déjà dans l'arsenal des groupes terroristes, créant de cette manière un déséquilibre stratégique préoccupant. Il serait préférable de restreindre leur emploi à des circonstances spécifiques et encadrées par un dispositif légal rigoureux et bien structuré. Une telle approche en particulier offrirait aux États de l'Afrique de l'Ouest l'opportunité d'approfondir des collaborations scientifiques, en menant des travaux conjoints sur ces catégories d'armements et les systèmes intégrant une intervention humaine.

2.2.2. Les systèmes d'armes avec intervention humaine

Définition des systèmes d'armes sous contrôle humain. Les systèmes d'armes avec intervention humaine s'entendent comme des systèmes d'armement qui utilisent l'IA pour sélectionner et engager des cibles, mais qui nécessitent une intervention humaine pour confirmer ou annuler l'attaque (**COMITÉ INTERNATIONAL DE LA CROIX-ROUGE**, 2023). Ils sont souvent dénommés « *armes semi-autonomes* » ou « *armes à contrôle humain significatif* » (**GARY**, 2021). Le premier type d'armes est un système d'armes qui, une fois activé, peut engager une cible ou un groupe de cibles préalablement sélectionnés et autorisés à l'attaque par un opérateur humain (**FONDATION FRIEDRICH-EBERT STIFTUNG**, 2015). Le second, quant à lui, renvoie à « *un système d'armes qui offre à l'opérateur humain la possibilité d'intervenir et de refuser certaines actions, telles que l'engagement des armes.* » (**FONDATION FRIEDRICH-EBERT STIFTUNG**, 2015).

Utilité de ces armements en Afrique occidentale. Ces deux systèmes d'armes pourraient aider les États de l'Afrique de l'Ouest à mener leurs ripostes contre le terrorisme, qui se trouve être l'un des défis de l'heure. Il urgerait alors de mener des études et des recherches qui permettraient de développer des armes performantes. Ces États pourraient par exemple s'inspirer des recherches qui existent et visent le développement des armes utilisant l'IA de façon responsable et éthique, en respectant les principes du DIH et des droits de l'homme. Le

projet *Trustworthy Autonomy for Military Systems* (TAMS), par exemple, vise à concevoir des systèmes autonomes qui sont fiables, transparents, explicables et responsables (**BRANDI**, 2023). Le projet *Ethical Governance of Emerging Technologies* (EGEST), quant à lui, explore les implications éthiques, juridiques et sociales des technologies émergentes, telles que l'IA, les drones ou les robots, dans le contexte de la sécurité et de la défense (**UNIVERSITA CATTOLICA DEL SACRO CUORE**, 2012).

Discussions autour de ces systèmes d'armes et les lueurs d'espoir. Le débat juridique et éthique entourant ce type d'armements s'inscrit dans une dynamique comparable à celle évoquée antérieurement. En effet, plusieurs enjeux militaires appellent une vigilance accrue, qu'il s'agisse des systèmes d'armes autonomes ou des implications plus vastes de l'IA dans le domaine de l'armement. Sur la scène internationale, les réflexions concernant les menaces potentielles de l'IA sur la paix et la sécurité mondiale ne font qu'émerger. Par exemple, les Nations unies ont amorcé des discussions visant à encadrer ces technologies, tandis que certains États commencent à élaborer des stratégies nationales intégrant l'IA dans leurs dispositifs de défense. Toutefois, la contribution des États africains aux débats et négociations multilatérales sur ces enjeux reste limitée. Il demeure impératif de mener des recherches approfondies pour analyser l'impact de l'IA sur la paix et la sécurité en Afrique, un continent dont les dynamiques géopolitiques méritent une attention accrue [Traduction] (**AFRICAN UNION**, 2024).

Malgré les débats entourant les dangers potentiels de l'IA dans le domaine militaire, une perspective optimiste semble se dessiner. En effet, les avancées technologiques dans le domaine des capteurs promettent de doter les systèmes d'armement futuristes d'une efficacité accrue. Parmi ces progrès, on note une amélioration significative de la capacité à distinguer alliés et adversaires, ainsi qu'à identifier les cibles avec une précision remarquable. Ces avancées s'accompagnent d'une interconnexion plus sophistiquée des dispositifs, opérant souvent en formation « *en essaim* »[7], favorisant une coordination accrue. Par ailleurs, les interfaces homme-machine gagnent en maturité, renforçant la synergie entre opérateurs humains et systèmes automatisés. Ces évolutions sont directement portées par le développement toujours plus abouti de logiciels basés sur l'IA, laissant entrevoir un avenir où technologie et stratégie pourraient se conjuguer efficacement (**FONDATION FRIEDRICH-EBERT STIFTUNG**, 2015).

[7] Les machines qui fonctionnent la plupart du temps ensemble avec une interconnexion notable.

Apport de la technologie 6G. La technologie 6G[8] pourrait transformer profondément les capacités de l'IA intégrée aux systèmes d'armement, qu'ils soient supervisés ou autonomes. Concrètement, elle promet d'accélérer et de perfectionner l'analyse des données, rendant la sélection et l'engagement des cibles, notamment celles considérées comme terroristes, plus précis et efficaces (**COTTIER**, 2022). Cette avancée s'accompagnerait d'une amélioration significative de la reconnaissance visuelle et auditive, tout en optimisant les algorithmes de prise de décision autonome. Cependant, ces évolutions technologiques ne sauraient se déployer pleinement sans être encadrées par des régulations juridiques et des réflexions éthiques rigoureuses (**COTTIER**, 2022). L'impact de la 6G sur ces systèmes d'armement devra demeurer tributaire des débats internationaux en cours, visant à établir des normes garantissant que leur utilisation demeure conforme au DIH et aux principes éthiques fondamentaux (**ORGANISATION DES NATIONS UNIES**, 2023). Ces discussions, encore en gestation, cherchent à prévenir les dérives potentielles tout en ouvrant la voie à une utilisation responsable et maîtrisée de ces technologies (**ORGANISATION DES NATIONS UNIES**, 2023).

Toutes ces avancées, ainsi que bien d'autres, doivent impérativement être intégrées dans les divers centres de recherche et d'étude en IA qui seront créés par les États de l'Afrique de l'Ouest. Une telle approche permettra non seulement de stimuler l'innovation, mais également de favoriser une meilleure adaptation des pays aux enjeux technologiques mondiaux.

[8] La technologie 6G représente l'avenir des communications sans fil, après les réseaux 5G actuels. Elle devrait être nettement plus rapide et prendre en charge un plus large éventail d'applications, notamment les expériences mobiles avancées, l'IA et l'IoT. Pour l'instant, les réseaux 6G sont en cours de développement et il n'existe pas encore de normes universellement acceptées. Ils devraient être déployés d'ici 2028.

Conclusion

Interaction mutuelle entre l'IA et le terrorisme. Tout bien considéré, l'IA pourrait devenir un atout majeur dans la lutte contre le terrorisme en Afrique de l'Ouest. Grâce à la surveillance des communications électroniques et à la reconnaissance faciale, elle faciliterait le démantèlement des cellules terroristes avant qu'elles ne passent à l'action. De plus, son intégration dans l'artillerie des forces armées permettrait de réduire les pertes humaines et d'améliorer l'efficacité opérationnelle, notamment grâce aux drones armés et aux dispositifs explosifs à détection électronique. Cependant, malgré ces avancées, l'IA soulève des défis importants. Son utilisation requiert une formation adéquate des militaires et l'adoption d'un cadre législatif garantissant une exploitation éthique et responsable. Ainsi, plutôt que de rejeter cette technologie, il conviendrait d'en encadrer l'usage et d'encourager des recherches visant à renforcer l'intervention humaine. Dans cette optique, le développement d'algorithmes avancés, adaptés aux contextes sécuritaires complexes, ouvre de nouvelles perspectives. Toutefois, il pose également des questions interdisciplinaires en croisant IA, éthique, droit et autres sciences. La capacité de l'IA à conjuguer efficacité opérationnelle et respect des principes juridiques devient alors un enjeu central, notamment dans des environnements instables où la transparence des algorithmes et les risques de dérives sécuritaires restent préoccupants. Malgré ces défis, l'IA constitue une avancée significative pour optimiser les stratégies antiterroristes et protéger les populations civiles. Son usage, bien encadré, pourrait ainsi représenter une véritable révolution dans la lutte contre le terrorisme. Quoi qu'il en soit, cette technologie ne devrait servir qu'un seul objectif : œuvrer pour le bien de l'humanité.

Bibliographie

Doctrine

AFRICAN UNION (2024), « Continental Artificial Intelligence Strategy », *AU Executive Council during its 45th Ordinary Session*, République du Ghana, 63 p.

AMER, M., HILMI, Y., & EL KEZAZY, H. (2024, April). Big Data and Artificial Intelligence at the Heart of Management Control: Towards an Era of Renewed Strategic Steering. In The International Workshop on Big Data and Business Intelligence (pp. 303-316). Cham: Springer Nature Switzerland.

CAZENEUVE, Bernard (2023), « Aspects cyber de la lutte antiterroriste », *Dalloz IP/IT*, n° 7, France, pp. 380-381.

CORNU, Gérard (2018), *Vocabulaire juridique*, 12e éd., P.U.F, Coll. « Quadrige », France, 2300 p.

DRM (2019), « L'intelligence artificielle et renseignement militaire », *Revue Défense Nationale*, no 820, France, pp. 107-116.

DUBUISSON, François (2017), « La définition du « terrorisme » : débats, enjeux et fonctions dans le discours juridique », *Confluences Méditerranée*, no 102, France, pp. 29-45.

FONDATION FRIEDRICH-EBERT STIFTUNG (2015), « Les nouvelles technologies militaires numériques et les systèmes d'armes autonomes », *Analyses et documents*, France, 8 p.

GARY, Arnaud (2021), « Intelligence artificielle et armées françaises : une technologie du présent à mettre en œuvre immédiatement », *Revue Défense Nationale*, France, pp. 200-213.

GROUPE INTERGOUVERNEMENTAL D'ACTION CONTRE LE BLANCHIMENT D'ARGENT EN AFRIQUE DE L'OUEST (2022), « Avis de manifestation d'intérêt pour la conduite des typologies de blanchiment de capitaux et de financement du terrorisme associé à la cybercriminalité en Afrique de l'Ouest », *GIABA*, Sénégal, 5 p.

KAROUTCHI, Roger (2016), « Proposition de loi relative à la reconnaissance faciale dans les enquêtes terroristes », *Présidence du Sénat français*, no 699, France, 6 p.

LEFORT-LAVAUZELLE, Patrice (2018), « Le contrôle social en Chine : 1,42 milliard de suspects sous surveillance », *Défense*, no 194, France, pp. 52-55.

MAINGUY, Daniel (2022)**,** « Intelligence artificielle et droit militaire », *in* **BENSAMOUN**, Alexandra & **LOISEAU**, Grégoire (dir.), *Droit de l'intelligence artificielle*, 2e éd., L.G.D.J, France, pp. 473-504.

SISSOKO, Etienne Fakaba & **DEMBÉLÉ**, Alexis (2023), « La digitalisation et le journalisme : L'impact des réseaux sociaux et du journalisme citoyen sur la scène médiatique malienne », Revue *Francophone*, vol. 1, n° 2, France, pp. 152-176.

UNION AFRICAINE (2025), « Communiqué de la 1267e réunion du Conseil de paix et de sécurité, tenue le 20 mars 2025, sur l'intelligence artificielle et son impact sur la paix, la sécurité et la gouvernance en Afrique », *Conseil de paix et de sécurité 1267e réunion (Au niveau ministériel)*, Éthiopie, 4 p.

Législation

Loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques (Togo).

Loi n° 2014-14 relative aux communications électroniques et à la poste en République du Bénin (Bénin).

Décret n° 09-2019/AN du 23 avril 2019 portant modification de la loi n° 0061-2008/AN du 27 septembre 2008 portant réglementation générale des réseaux et services de communications électroniques générale de réseaux et services de communications électroniques au Burkina Faso (Burkina Faso).

Jurisprudence

CJUE, 6 octobre 2020, affaire C-511/18, C-512/18, C-520/18 et affaire C-623/17.

CEDH, 25 mai 2021, *Big Brother Watch* et autres c. Royaume-Uni, req. n° 58170/13, 62322/14 et **CEDH**, 25 mai 2021, *Centrum för Rättvisa* c. Suède, req. n° 35252/08.

Webographie

ABATTAN, Jeannine Ella et **KONÉ**, Hassane (2024), « Le Bénin doit contrer la menace des engins explosifs improvisés » : https://issafrica.org/fr/iss-today/le-benin-doit-contrer-la-menace-des-engins-explosifs-improvises (Consulté le 10/12/2024).

AGENCE ECOFIN (2024), « Les États-Unis envisagent d'installer des bases militaires dans trois pays côtiers d'Afrique de l'Ouest » : https://urlr.me/unGwXH (Consulté le 25/01/2024).

ALLEN, Karen (2022), « Drones armés : la dernière menace technologique en date pour l'Afrique » : https://urlr.me/TQHcRZ (Consulté le 18/01/2024).

BRANDI, Vincent (2023), « Inside the DOD's trusted AI and autonomy tech review that brought together hundreds of experts » : https://urlr.me/UgPu7f (Consulté le 22/01/2024).

BRUUN, Laura (2022), « Les systèmes d'armes autonomes : ce que le droit dit - et ne dit pas - sur le rôle de l'être humain dans l'usage de la force » : https://urlr.me/n9WNqb (Consulté le 22/01/2024).

CENTRE D'ÉTUDE STRATÉGIQUE DE L'AFRIQUE (2017), « Carte des groupes islamiques militants actifs en Afrique » : https://urlr.me/eDazxp (Consulté le 24/01/2024).

COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (2022), « Questions-réponses – Ce qu'il faut savoir sur les armes autonomes » : https://www.icrc.org/fr/document/questions-reponses-armes-autonomes (Consulté le 22/01/2024).

COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (2023), « Ce que vous devez savoir sur l'intelligence artificielle dans les conflits armés » : https://urlr.me/FYTcy3 (Consulté le 23/01/2024).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2019), « Reconnaissance faciale : Pour un débat à la hauteur des enjeux » : https://urlr.me/EyPgks (Consulté le 16/01/2024).

COTTIER, Damien (2022), « L'Émergence des systèmes d'armes létales autonomes (SALA) et leur nécessaire appréhension par le droit européen des droits humains » : https://urlr.me/YfPN6t (Consulté le 18/03/2024).

DIRECTION : AID (2021), « Le guide pour l'intégration de l'intelligence artificielle (IA) dans les programmes évolue » : https://www.defense.gouv.fr/aid/actualites/guide-lintegration-lintelligence-artificielle-ia-programmes-evolue (Consulté le 20/01/ 2024).

DUNN, Craig (2022), « Top 10 des cyberattaques qui ont marqué 2021 » : https://www.hiscox.fr/blog/je-protege-mon-activite/cyberattaques-top-10-2021 (Consulté le 21/01/2024).

EDDÉ, Rhéa (2020), « Les entreprises à l'épreuve des cyberattaques » : https://www.cairn.info/revue-flux-2020-3-page-90.htm (Consulté le 21/01/2024).

EKOUÉ, Blamé (2022), « Antiterrorisme : l'Afrique de l'Ouest vers plus de solutions endogènes ? » : https://www.lepoint.fr/afrique/antiterrorisme-l-afrique-de-l-ouest-vers-plus-de-solutions-endogenes-06-05-2022-2474550_3826.php (Consulté le 19/01/2024).

FRANCE 24 (2023), « Au Nigéria, un drone de l'armée tue par erreur 85 civils lors d'une fête » : https://www.france24.com/fr/afrique/20231205-au-nig%C3%A9ria-un-drone-de-l-arm%C3%A9e-tue-par-erreur-85-civils-lors-d-une-f%C3%AAte (Consulté le 18/01/2024).

GENEVA INTERNATIONAL CENTRE FOR HUMANITARIAN DEMINING (2020), « Éducation aux risques des engins explosifs dans des environnements complexes : étude de nouvelles méthodes et technologies » : https://urlr.me/qsgS3m (Consulté le 17/01/2024).

HENRY, L. & **PAIANO**, Jonathan (2023), « L'IA dans les drones militaires : meilleure que les humains ou potentielle menace » : https://trustmyscience.com/ia-drone-militaire-reconnaissance-cible-valide/ (Consulté le 18/01/2024).

HUMAN RIGHTS WATCH (2022), « Burkina Faso – Événements de 2022 » : https://www.hrw.org/fr/world-report/2023/country-chapters/383648 (Consulté le 24/01/2024).

INTERPOL (2021), « Un rapport d'INTERPOL recense les principales cybermenaces en Afrique » : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2021/Un-rapport-d-INTERPOL-recense-les-principales-cybermenaces-en-Afrique (Consulté le 21/01/2024).

JOMIER, Solene (2021), « Utilisation des drones armés par des États de l'UE : enjeux, juridiques et éthiques » : https://www.google.com/amp/s/www.grip.org/utilisations-drones-armes-etats-ue-enjeux-politiques-juridiques-ethiques/amp/ (Consulté le 18/01/2024).

KONÉ, Hassane (2022), « Le trafic d'armes entre la Libye et le Niger reprend de plus belle » : https://urlr.me/tDYdzZ (Consulté le 24/01/2024).

LASSAAD, Ben Ahmed (2022), « L'armée togolaise reconnait avoir tué, par erreur, 7 enfants et non par attaque terroriste » : https://www.aa.com.tr/fr/afrique/larm%C3%A9e-togolaise-reconnait-avoir-tu%C3%A9-par-erreur-7-enfants/2637238 (Consulté le 30/01/2024).

LINDEMULDER, Gregg & **KOSINSKI**, Matt (2024), « Qu'est-ce que la cybersécurité » : https://www.ibm.com/fr-fr/topics/cybersecurity (Consulté le 11/12/2024).

MEDIA DEFENCE (2021), « La surveillance numérique par le gouvernement » : https://urlr.me/f3Pvpk (Consulté le 15/01/2024).

MINISTÈRE DES ARMÉES (2019), « L'intelligence artificielle au service de la défense » : https://www.vie-publique.fr/rapport/270333-lintelligence-artificielle-au-service-de-la-defense (Consulté le 20/01/2024).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (2019), « L'intelligence artificielle dans la société » : https://urlr.me/Qnz5bg (Consulté le 22/01/2024).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (2021), « Réseaux et interventions militaires en Afrique du Nord et de l'Ouest » : https://urlr.me/uq7vCd (Consulté le 20/01/2024).

ORGANISATION DES NATIONS UNIES (2023), « La Première Commission adopte huit projets de résolution sur les armes classiques, dont un nouveau texte sur les systèmes d'armes létaux autonomes » : https://urlr.me/JWge3c (Consulté le 18/03/2024).

ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD (2015), « Lutte contre les engins explosifs improvisés » : https://urlr.me/V4dQSU (Consulté le 18 janvier 2024).

PAJON, Céline & ***alii*** (2004), « Chronologie du terrorisme dans le monde et des attentats et actes terroristes » : https://urlr.me/K5X4j9 (Consulté le 21/02/2025).

TOUNKARA, Georges Ibrahim (2021), « Les drones armés, efficaces mais très controversés » : https://urlr.me/jgEHDG (Consulté le 18/01/2024).

UNIVERSITA CATTOLICA DEL SACRO CUORE (2012), « The Ethical Governance of emerging technologies – New Governance Perspectives for Integrating Ethics into Technical Development Projects and Applications » : https://urlr.me/qhQTSg (Consulté le 22/01/2024).