التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

EXPLOITATION DES OUTILS DE L'INTELLIGENCE ARTIFICIELLE DANS LA LUTTE CONTRE LE TERRORISME

DR. OBAID SALEH ALMUKHTAN
CHERCHEUR EN INTELLIGENCE ARTIFICIELLE ET CYBERCRIMINALITÉ
ÉMIRATS ARABES UNIS

5
Questions de Terrorisme
Dec. 2023

Questions de Terrorisme

Numéro mensuel - Coalition Islamique Militaire Contre le terrorisme

---

Superviseur général

Major-Général Mohammed bin Saïd Al-Mughaidi

Secrétaire Général désigné de la Coalition Islamique Militaire Contre le Terrorisme

---

Rédacteur en chef

Ashour Ibrahim Aljuhani

Directeur du Département des Études et des Recherches

EXPLOITATION DES OUTILS DE L'INTELLIGENCE ARTIFICIELLE DANS LA LUTTE CONTRE LE TERRORISME

DR. OBAID SALEH ALMUKHTAN

CHERCHEUR EN INTELLIGENCE ARTIFICIELLE ET CYBERCRIMINALITÉ

ÉMIRATS ARABES UNIS

Exploitation de l'intelligence Artificielle dans la Lutte Contre le Terrorisme

L'utilisation de l'intelligence artificielle (IA) dans la lutte contre le terrorisme peut potentiellement avoir un effet significatif et bénéfique sur les efforts visant à contrer cette menace. L'IA permet aux systèmes d'analyser d'énormes quantités de données plus rapidement et avec plus de précision, ce qui leur permet de détecter des modèles et des menaces potentielles, ainsi que de prendre des mesures appropriées pour prévenir (Al-Haqil, 2023) et anticiper les attaques terroristes. À l'échelle internationale, se dessine une tendance majeure vers l'exploitation de l'IA dans la lutte contre le terrorisme et la criminalité organisée. Cette orientation découle d'une prise de conscience croissante de l'importance cruciale des données au sein des futures stratégies de prévention et de répression de la criminalité. Dans ce contexte, les stratégies adoptées se concentrent sur plusieurs aspects fondamentaux, tels que l'analyse des données et l'extraction de modèles et de menaces potentielles, le développement de systèmes de reconnaissance d'images et de vidéos, la détection des comportements suspects, l'analyse prédictive, la fourniture d'évaluations concernant les menaces futures, l'analyse du comportement terroriste, ainsi que la suppression du contenu extrémiste sur les plateformes de médias sociaux.

1- Objectifs de l'étude :

- Un des objectifs fondamentaux de l'utilisation de l'IA dans l'analyse des données massives pour les opérations de renseignement est d'assurer une accessibilité rapide aux informations requises, d'identifier et d'arrêter rapidement les criminels, ainsi que d'anticiper les actes terroristes avant qu'ils ne se produisent.

- Utiliser les techniques de l'IA dans la lutte contre le terrorisme et surveiller le contenu terroriste sur les plateformes de médias sociaux. Cela implique une connaissance approfondie des différentes étapes et des composantes fondamentales de ces techniques telles que l'apprentissage automatique, les algorithmes, le traitement du langage naturel, les réseaux neuronaux artificiels, l'identification du contenu de l'extrémisme violent, la lutte contre la propagation des discours de haine, ainsi que la lutte contre la diffusion d'idées extrémistes et terroristes sur les plateformes de médias sociaux.

- Élaborer une stratégie numérique pour la coopération en matière de sécurité numérique entre les services de sécurité arabes dans le but de lutter contre le terrorisme qui s'étend à l'environnement cybernétique.

- Découvrir ce qu'est le Dark Web, décrire le réseau caché d'Internet et son fonctionnement, et mettre en lumière les tactiques du terrorisme via le Deep Web ainsi que le financement du terrorisme.

2- Questions de l'étude :

- Quels sont les mécanismes d'exploitation de l'IA pour protéger les communautés et les individus contre l'extrémisme et le terrorisme ?

- Comment peut-on définir l'intelligence artificielle dans le contexte de la lutte contre l'extrémisme et le terrorisme sur les plateformes de médias sociaux ? Quelles sont les capacités exploitées par les entreprises technologiques pour lutter contre la diffusion des contenus à caractère terroriste en ligne ?

- Quelles sont les menaces sécuritaires des réseaux sociaux et leur impact sur la sécurité sociétale au sein de la région arabe ?

- Quelles sont les méthodes de financement du terrorisme à travers le Dark Web ? Quelles sont les défis mondiaux auxquels font face les services de sécurité pour surveiller et traquer ces activités illégales ?

3- Mots clés :

Extrémisme violent – terrorisme – cyberespace – intelligence artificielle (IA) – réseaux de neurones – apprentissage automatique et profond – algorithmes – plateformes de médias sociaux.

4- Plan de l'étude :

La première section, intitulée « Tactiques intelligentes du terrorisme dans le processus de financement, de recrutement et de propagation de l'extrémisme », comporte trois points essentiels : le premier concerne l'utilisation de la technologie et du cyberespace par les groupes terroristes, le deuxième porte sur la propagation de l'extrémisme violent via les plateformes électroniques, et le troisième aborde les tactiques de diffusion de l'extrémisme et du terrorisme sur le Dark Web. La seconde section, intitulée « L'IA et les opportunités de lutte contre l'extrémisme et le terrorisme », aborde trois aspects essentiels : le premier porte sur les opportunités d'exploiter les applications d'IA pour prédire les opérations terroristes, le deuxième concerne l'exploitation des logiciels basés sur des algorithmes pour renforcer la lutte contre l'activité terroriste, le troisième met en avant les mécanismes de coopération numérique en matière de lutte contre le cyberterrorisme. Enfin, l'étude se termine par une conclusion mettant en évidence les principaux résultats et recommandations.

La première section

Tactiques intelligentes du terrorisme dans le processus de financement, de recrutement et de propagation de l'extrémisme

Préambule et division :

Les tactiques intelligentes du terrorisme reposent sur l'utilisation de stratégies avancées dans le financement, le recrutement et la propagation de l'extrémisme. Ces tactiques comprennent le recours au financement, aux communications cryptées, aux médias sociaux, au chiffrement et à l'exploitation intelligente du multimédia, ainsi qu'à une présence numérique diversifiée (La Stratégie antiterroriste mondiale de l'ONU, 2020). En fait, l'utilisation de l'IA par les organisations terroristes peut représenter une menace considérable lorsqu'elle est employée à des fins malveillantes. Avec un passé riche en cybercriminalité, l'IA est devenue un outil puissant susceptible d'accroître ou de faciliter le terrorisme et l'extrémisme violent. Par exemple, elle offre de nouvelles méthodes pour mener des attaques physiques à l'aide de drones ou de véhicules autonome, en augmentant les cyberattaques contre des infrastructures vitales, ou en favorisant la propagation plus rapide et efficace de discours haineux et d'incitations à la violence. Nous abordons ces risques à travers les trois aspects fondamentaux suivants :

1. L'utilisation de la technologie et du cyberespace par les groupes terroristes.
2. La propagation de l'extrémisme violent via les plateformes électroniques.
3. Les tactiques de diffusion de l'extrémisme et du terrorisme sur le Dark Web.

1. L'utilisation de la technologie et du cyber-espace par les groupes terroristes

Les groupes extrémistes exploitent habilement la technologie, l'adaptant rapidement à leurs besoins. Il est donc crucial de comprendre pleinement les menaces liées à l'extrémisme et de développer des stratégies efficaces pour les prévenir et les endiguer. La compréhension de la menace croissante de l'extrémisme et de l'évolution des outils technologiques utilisés par les groupes extrémistes est d'une importance capitale pour élaborer des stratégies efficaces visant à prévenir et à combattre ce phénomène. Avec l'augmentation de l'utilisation d'Internet et des médias sociaux en tant qu'instruments de diffusion de l'idéologie extrémiste, il devient impératif d'analyser et de surveiller le contenu numérique, tout en développant des techniques de reconnaissance de modèles et de prédiction du comportement futur des extrémistes.

De nos jours, les groupes terroristes exploitent les technologies de pointe à leur disposition. Par exemple, les auteurs des attentats de Mumbai en 2008 ont utilisé des technologies telles que les systèmes de positionnement global (GPS), les téléphones portables et Internet pour planifier, coordonner et exécuter leurs missions. Cette utilisation novatrice des dernières avancées technologiques démontre la capacité des groupes terroristes à s'adapter à un environnement de plus en plus numérique. De même, les terroristes ont récemment recours à des actifs virtuels basés sur la technologie de la blockchain comme le « Bitcoin ». Ils utilisent également les services bancaires mobiles et le financement participatif, que ce soit pour collecter des fonds ou pour effectuer des transferts d'argent. En parallèle, le Dark Web est devenu un marché pour la vente d'une multitude de produits, d'armes et de documents falsifiés.

Il existe de nombreuses preuves que les groupes terroristes exploitent des technologies liées à l'IA. Cela est particulièrement évident dans l'exploitation de systèmes aériens sans pilote, connus sous le nom des drones. En effet, ces derniers sont considérés comme une technologie étroitement liée à l'IA. L'utilisation des drones par ces groupes a pris des formes variées, incluant des attaques réelles, des tentatives d'attaques, des perturbations, des surveillances, des propagandes, des mobilisations, des collectes de fonds, et des recrutements de nouveaux membres. En réalité, le recrutement de nouveaux membres au sein des organisations terroristes est essentiel à leur survie ainsi qu'à leur continuité. Ces organisations exploitent la sympathie d'autres utilisateurs d'Internet envers leurs causes et les attirent avec des discours séduisants et enthousiastes au sein des forums de discussion électroniques (Abdel-Moaty, 2012). Les terroristes suivent les stratégies suivantes lors du processus de recrutement en ligne :

- Fournir des instructions et endoctriner en ligne : Internet regorge de sites web qui contiennent des manuels et des directives détaillant la fabrication de bombes et l'utilisation d'armes chimiques mortelles.
- La guerre psychologique : diffuser des informations trompeuses, semer la terreur et la peur dans le cœur des individus en filmant les crimes qu'ils commettent et les opérations terroristes qu'ils mènent, ainsi que documenter les attentats terroristes en glorifiant leurs auteurs (Abdelsalam, 2020).
- Le financement : Internet est utilisé pour collecter des dons au moyen de transferts financiers en ligne. Des organisations internationales à caractère humanitaire ou caritatif peuvent être utilisées comme couverture pour fournir des fonds ou opérer sous leur couvert.

2- La propagation de l'extrémisme violent via les plateformes électroniques

La politique des organisations terroristes, telles que l'État islamique (EI), repose sur plusieurs stratégies, notamment la polarisation des masses, la violation de la vie privée numérique, et la diffusion de vidéos violentes. Ils utilisent également des tactiques telles que le piratage des hashtags, des applications, des logiciels de messagerie instantanée, et même des robots

Web configurés localement, dans le but de réaliser leurs objectifs. Le tableau de l'extrémisme et du terrorisme ne serait pas complet sans tenir compte de la rapidité, car la rapidité et la dissimulation caractérisent la production médiatique de l'État islamique et sa diffusion ultérieure. Le comportement médiatique de cette organisation, qui a accompagné les attentats-suicides du 14 novembre 2015 à Paris, au cours desquels 127 personnes ont été tuées ainsi que 8 extrémistes, témoigne d'un travail médiatique coordonné et prémédité. Cela démontre la synchronisation entre les opérations sur le terrain et la communication médiatique dans le contexte terroriste (terrorisme et droits de l'homme).

Avec l'essor des médias sociaux, les individus peuvent devenir vulnérables à la manipulation à travers la propagation d'informations trompeuses et la divulgation d'informations. De même, l'intégration de l'IA dans cette équation, par exemple via la propagation des deepfakes, renforcera considérablement la nature des menaces sécuritaires (ALGORITHMES ET TERRORISME, 2023). Nous abordons la propagation de l'extrémisme violent via les plateformes électroniques et les violations des droits humaines comme suit : -

Premièrement - Plateformes de communication et couverture des actes terroristes :

Les organisations terroristes utilisent les sites de médias sociaux comme outil pour identifier et surveiller leurs cibles, en particulier dans le cadre d'opérations d'assassinat dans les pays cibles. Cela peut se faire en surveillant ceux qui possèdent des comptes sur ces sites ou en surveillant leur cercle d'amis et de connaissances pour les atteindre et recueillir les informations nécessaires sur leurs mouvements. Il existe plusieurs objectifs principaux des groupes terroristes en utilisant les médias sociaux, notamment : les objectifs des communications opérationnelles, la collecte de renseignements et l'échange d'informations, le recrutement et la formation, ainsi que d'autres utilisations fonctionnelles. En 2014, un rapport publié par le Centre Simon Wiesenthal, basé à Los Angeles, a révélé qu'il existait plus de trente mille forums, sites web et comptes sur les réseaux sociaux faisant la promotion du terrorisme aux États-Unis et ailleurs. De plus en plus, les extrémistes rejoignent ces plateformes de médias sociaux, ce qui renforce encore la menace sécuritaire. Il est à noter que de nombreux groupes d'extrême droite sur les médias sociaux redirige constamment leur public vers leurs forums, et révèlent régulièrement les pages et les comptes de leurs membres sur les plateformes de médias sociaux telles que Facebook et Twitter (Wiesenthal, 2021).

Deuxièmement - Exploitation de l'IA par les groupes terroristes :

Les groupes terroristes exploitent de plus en plus l'IA, ce qui constitue une violation des droits de l'homme, en raison de l'usage abusif de la technologie et des préjudices infligés aux sociétés et à l'humanité. Ceci est d'autant plus préoccupant avec l'accès accru des individus à la technologie d'auto-apprentissage. En février 2020, le bon fonctionnement des systèmes basés sur l'IA a été compromis lorsqu'un artiste allemand a trompé Google Maps en lui faisant croire que le trafic dans les rues de Berlin était plus élevé qu'il ne l'était en réalité. Pour ce faire, il a volontairement alimenté l'algorithme de Google Maps avec des données trompeuses. Il s'est baladé dans la rue en tirant une charrette contenant un peu moins d'une centaine de smartphones. Google Maps a interprété ces signaux comme étant des personnes à bord de véhicules, entraînant ainsi un dysfonctionnement du système. Cet incident met en évidence comment des acteurs malveillants peuvent exploiter les capacités de l'IA pour semer la confusion et le chaos à des fins préjudiciables.

Troisièmement - Propagation des discours de haine et des deepfakes via les plateformes en ligne :

Les médias sociaux sont utilisés comme outils pour diffuser la haine et les rumeurs en ligne, ce qui entraîne une augmentation de la violence dans la société. Cela est dû au fait que les médias sociaux facilitent et accélèrent la capacité des individus à propager ou s'engager dans un comportement violent ou incitatif, tout en se cachant derrière leurs écrans.

Les plateformes de médias sociaux sont également utilisées en tant qu'arrière-plan pour les activités terroristes. Ils servent de canal pour propager la haine, la désinformation et des contenus extrémistes. Ces plateformes offrent à chaque individu violent une tribune publique constamment accessible. De plus, l'anonymat sur les médias sociaux permet à certains pays d'adopter et d'inciter à la haine au-delà des frontières nationales. Par ailleurs, les groupes terroristes comptent sur les plateformes de médias sociaux pour légitimer la violence, recruter des tueurs et glorifier leurs victoires. Lors de son ascension, Daech a su manier de manière élaborée les médias sociaux pour diffuser des vidéos d'exécutions, d'attaques, et d'autres contenus de nature similaire (Al-Sharqawi Nisreen, 2022).

Il existe diverses formes de menaces sécuritaires posées par la technologie Deepfake, ayant un impact sur la sécurité nationale et sociétale (Khalifa, 2018) :

- **Fabriquer de fausses déclarations diffamatoires** et les attribuer à des politiciens pourrait déclencher des actes de violence, des manifestations, voire provoquer des tensions dans les relations internationales.
- Forcepoint, une entreprise leader en cybersécurité, prévoit que les cybercriminels utiliseront la technologie Deepfake pour créer des images et des vidéos pouvant être exploitées pour demander des rançons. En parallèle, le vol de données est susceptible d'augmenter en incitant les employés à divulguer des informations, notamment les identifiants d'accès, les données et les dossiers financiers, etc. Il est également possible de prévoir une augmentation des attaques de phishing, au moyen de vidéos contenant des logiciels malveillants ou de messages conçus pour inciter les utilisateurs à cliquer sur des liens dans le cadre d'attaques de phishing (Hames, 2020).

Quatrièmement - Médias sociaux et leur impact sur

la sécurité sociétale :

Les médias sociaux jouent un rôle actif dans la formation de l'opinion publique, favorisant la promotion d'idées adoptées par l'élite de la société. Parmi les programmes et innovations les plus inquiétants de l'ère numérique, « TikTok » s'impose comme une plateforme mondialement reconnue. Des enjeux mondiaux de sécurité se posent concernant l'application « TikTok », notamment des accusations de collecte excessive des données personnelles des utilisateurs et de leur soumission à des analyses approfondies, y compris la duplication non nécessaire de données depuis les téléphones, le recueil d'informations susceptibles de permettre la localisation et le suivi des utilisateurs, ainsi que son utilisation pour la propagation de rumeurs, en particulier celles qui constituent une menace pour la sécurité nationale et arabe. De plus, certaines vidéos « TikTok » diffusent des discours haineux, promeuvent des idées extrémistes et terroristes, ce qui crée des situations de conflit et de discorde au sein de la société, menaçant ainsi sa sécurité et sa stabilité.

Parmi les risques de sécurité liés à l'application « TikTok » et les inconvénients de l'IA, nous citons par exemple :

- Diffusion des vidéos montrant des enfants victimes d'agressions sexuelles et de meurtres.
- Accroissement des menaces sécuritaires, avec une attention grandissante portée à l'utilisation de l'application « TikTok » par certains extrémistes et terroristes, qui l'exploitent à des fins criminelles et extrémistes. Par exemple, lors des émeutes et de l'invasion du Capitole en janvier 2021, certains extrémistes au sein de la société américaine ont utilisé l'application « TikTok » pour recruter des individus, les inciter à la violence, promouvoir des armes à feu et partager des directives tactiques liées aux activités criminelles qui ont été perpétrées (Abou Doh Khald Kazem, 2022).

3- Les tactiques de diffusion de l'extrémisme et du terrorisme sur le Dark Web.

Les opérations de financement, d'échange de fonds et de collecte de dons au sein des organisations terroristes ont évolué. Elles n'ont plus besoin de recevoir des fonds de ses partisans via des comptes bancaires soumis à la surveillance et au contrôle. De même, elles ne dépendent plus d'entreprises ou d'institutions pour blanchir ou augmenter les fonds. Internet est devenu un substitut crucial, suffisant, mais aussi dangereux, permettant à l'organisation « Daech » de collecter des millions de dollars, de les multiplier et de les dépenser via le web, en utilisant la cryptomonnaie « Bitcoin ». Les responsables des organisations terroristes peuvent ainsi communiquer en toute confidentialité et collecter des dons via le Deep Web.

Cela a poussé de nombreux services de sécurité à travers le monde à créer des plateformes et des outils d'IA afin de surveiller les contenus interdits en les faisant passer par des sites moins connus, voire parfois totalement inconnus, qui manquent des ressources nécessaires pour une surveillance adéquate.

Pour établir et gérer des réseaux financiers électroniques, il suffit à toute organisation terroriste ou criminelle dans le monde de fournir une connexion Internet, de disposer de comptes virtuels et de portefeuilles financiers dans un certain nombre de banques en ligne, d'avoir des membres bien formés pour opérer sur le marché des monnaies virtuelles, et de remplir ses portefeuilles financiers de monnaies virtuelles, soit grâce aux dons de ses partisans et fans, soit en recevant des financements via Internet de la part des agences, des pays et des entités qui le soutiennent (belfercenter.ksg.harvard, 2023).

Nous abordons les tactiques terroristes dans l'environnement du « Dark Web » comme suit :

Premièrement – Le recrutement de jeunes et le lavage de cerveau représentent des éléments clés de la menace terroriste à travers les plateformes électroniques :

Le recrutement des jeunes et l'impact des groupes terroristes sur la jeunesse via les médias sociaux et le Dark Web sont des composantes cruciales des dynamiques de la menace terroriste pour les États. Les terroristes exploitent ces plateformes pour promouvoir des idéologies extrémistes, collecter des informations et orienter les jeunes vers des actions terroristes. Voici quelques aspects clés de ces opérations (Manuel de référence pour la lutte contre le terrorisme, 2023) :-

- L'impact de la confiance et la promotion de l'extrémisme : Les terroristes visent à établir une relation de confiance avec les jeunes et à les convaincre de leurs idéologies extrémistes. Ils recourent à la manipulation psychologique et à des manœuvres émotionnelles pour attirer les jeunes et les recruter dans leurs rangs. Les idées extrémistes sont promues à travers des publications et des vidéos motivantes ciblant cette jeunesse.

Deuxièmement - Utiliser Bitcoin pour financer le terrorisme via le cyber environnement :

Daech exploite la cryptomonnaie Bitcoin de deux manières différentes. La première consiste à acheter ses besoins auprès de magasins et de boutiques illégaux sur le Dark Web (Al-Attar Ahmed Shawqi, 2021), et la deuxième consiste à convertir ces fonds virtuels en argent liquide pour subvenir à ses besoins de subsistance et ses opérations terroristes. Les marchés illégaux sur le darknet pour l'achat et la vente de marchandises interdites sont considérés comme l'une des principales destinations où Daech dépense les Bitcoins qu'il détient pour répondre à ses besoins opérationnels comme l'achat de faux passeports qui permettent aux extrémistes de traverser facilement les frontières, la location de véhicules et de logements sécurisés, l'achat d'armes, de matériel pour fabriquer des bombes et de petits drones, ainsi que le vol de données sensibles sur les cibles surveillées par l'organisation terroriste partout dans le monde, telles que des cartes secrètes, des codes et des numéros

confidentiels. Ces informations peuvent faciliter la réalisation d'opérations terroristes.

Les sites de Daech sur le « Deep Web » publient des annonces de dons pour des opérations « terroristes ». Sur la page d'accueil du site d'information affilié à « Daech », on pouvait trouver une annonce intitulée « Financement de la bataille islamique à partir d'ici ». Cette annonce utilise l'Islam comme couverture pour les opérations terroristes (Saghur Hisham, 2019). En réalité, il s'agit de combats terroristes, dont l'Islam est innocent. Les titres sont traduits en arabe et en anglais. En cliquant sur l'annonce, vous êtes redirigé vers une page intitulée « Fonds d'al-Kifah (combat) » pour faire des dons aux opérations terroristes, en monnaies électroniques via une adresse dédiée aux transactions financières. Il convient de noter que l'**Agence de l'Union européenne pour la coopération des services répressifs (Europol)**, a mis en garde contre le risque que Daech lance des attaques en Europe et que ce risque reste extrêmement élevé. Manuel Navarrete, directeur du Centre européen de lutte contre le terrorisme (ECTC) d'Europol, a déclaré : « Avec le déclin de Daech, ses membres sont incités à mener des attaques individuelles dans leurs propres pays plutôt que de les encourager à voyager ».

La seconde section

« L'IA et les opportunités de lutte contre l'extrémisme et le terrorisme »

Préambule et division :

Il existe de nombreuses opportunités pour exploiter les systèmes de lutte contre les opérations terroristes et tirer parti des résultats de l'IA pour analyser les comportements terroristes prévus, et détecter les indicateurs du terrorisme. De plus, l'IA peut être utilisée pour surveiller et empêcher la diffusion de contenus terroristes sur les plateformes de médias sociaux, lutter contre la contrebande d'armes à feu, et actualiser des stratégies antiterroristes à l'aide des systèmes de réseaux neuronaux artificiels (course.elementsofai, 2020). Ces aspects sont traités à travers les trois points suivants :-

1. Les opportunités d'exploiter les applications d'IA pour prédire les opérations terroristes.
2. L'exploitation des logiciels basés sur des algorithmes pour renforcer la lutte contre l'activité terroriste.
3. Les mécanismes de coopération numérique en matière de lutte contre le cyberterrorisme.

1. Les opportunités d'exploiter les applications d'IA pour prédire les opérations terroristes.

- L'IA représente un outil puissant pour améliorer les mesures de lutte contre la criminalité organisée et renforcer l'activité de renseignements. Elle peut être utilisée dans de nombreux domaines de la recherche criminelle, tels que l'analyse criminelle, les enquêtes, l'analyse génétique, la reconnaissance faciale et la géolocalisation (El-Babli Ammar, 2023). Grâce à l'utilisation de techniques d'IA, les enquêteurs criminels peuvent analyser de vastes quantités de données et d'informations disponibles. Cela accroît leurs chances de succès et leur permet de prendre des décisions appropriées concernant les crimes similaires à l'avenir. De plus, l'IA peut analyser les données génétiques, aider à identifier les suspects, et contribuer à établir des preuves solides.
- Il est possible d'améliorer les opérations antiterroristes en analysant de grandes quantités de données et d'informations disponibles, telles que les casiers judiciaires, les rapports de police et les documents judiciaires, afin de détecter des modèles, des tendances et des informations importantes pouvant être utilisées dans les enquêtes criminelles. De plus, les techniques d'apprentissage automatique, de classification, et de prédiction peuvent être employés pour analyser les données et générer des prévisions précises concernant d'éventuels événements futurs. En parallèle, l'analyse d'images, de vidéos et de fichiers audio s'avère essentielle pour découvrir des éléments de preuve et des informations importantes dans le cadre d'enquêtes criminelles.

L'utilisation adéquate et efficace de l'intelligence artificielle peut contribuer à améliorer les efforts de lutte contre le terrorisme et à renforcer la sécurité publique.

L'application de l'IA dans le domaine de la sécurité réside dans la technologie de photographie, de surveillance et de reconnaissance faciale. Cette dernière constitue un outil essentiel pour identifier les auteurs d'actes terroristes. L'IA a été également utilisée avec succès pour réduire les marges d'erreur aux différentes étapes de l'enquête, de l'investigation, de la surveillance et de l'application de la loi dans la lutte contre le terrorisme. Elle a permis de resserrer les cercles de suspicion, de simplifier les opérations de tri et de classification des informations, des individus et des données pertinentes. Tout cela a contribué à élever le niveau d'exactitude et d'efficacité des mesures de sécurité directement liées à la lutte contre le terrorisme. De plus, l'utilisation de l'IA a créé un climat de confiance dans les services de sécurité et a instauré un sentiment de sérénité au sein du grand public à l'égard des institutions et des mécanismes impliqués (Fahd, Wejdan, 2022).

À partir de ce qui précède, nous explorons la notion d'IA de la manière suivante :

Premièrement – Définition de l'IA:

L'IA est une branche de l'informatique qui se concentre sur la création de machines ou d'ordinateurs capables de prendre des décisions de manière intelligente ou rationnelle, en utilisant les connaissances stockées en elles ou en apprenant de nouvelles connaissances par le biais de l'alimentation de données.

Deuxièmement - Le concept d'IA dans le contexte de la lutte contre l'extrémisme et le terrorisme sur les plateformes de médias sociaux :

- Il s'agit de l'activation de logiciels intelligents et d'algorithmes en vue d'atteindre des objectifs comportementaux et techniques spécifiques dans le but de servir des individus à *travers* le monde en diffusant des informations spécifiques à des fins diverses. Concernant les aspects *de la sécurité et du renseignement*, les logiciels intelligents travaillent pour accélérer l'identification d'informations, de mots, de significations, d'images et de vidéos qui laissent présager un contenu terroriste sur les plateformes, que ce soit la violence ou la diffusion de la culture terroriste. Ces logiciels permettent également de les repérer, de les surveiller et de suivre leur trajectoire au sein des grandes entreprises technologiques, en vue de les analyser et de les supprimer.
- L'IA est utilisée pour lutter contre l'extrémisme violent en ligne, en particulier sur les plateformes de médias sociaux, en identifiant les personnes susceptibles d'adhérer aux idées extrémistes, c'est-à-dire les cibles potentielles soit pour des groupes idéologiquement extrémistes, soit pour des organisations terroristes, grâce à l'analyse des plateformes de médias sociaux à l'aide d'algorithmes intelligents.

Le recours à l'IA dans la lutte contre le terrorisme a apporté divers avantages qui ont constitué des points forts évidents. Ces avantages ont contribué à réduire certaines activités terroristes en exploitant les opportunités suivantes :

- Analyser les données massives et prédire l'avenir, en s'appuyant sur des outils basés sur l'IA tels que les moteurs de recherche et les systèmes de traitement du langage naturel, ont permis aux entreprises technologiques et aux services de sécurité de comprendre le langage utilisé par les groupes terroristes et les extrémistes. Ils ont également contribué à déchiffrer et identifier les écritures suspectes, facilitant ainsi la gestion du contenu en ligne, notamment en ce qui concerne les langues dans lesquelles les groupes de personnes communiquent (Valentini D. ; Lorusso A. ; Stephan A., 2020).
- Il existe d'autres plateformes qui soutiennent ce qui est considéré comme de l'extrémisme sous prétexte de permettre la liberté d'expression, prétendant ne pas vouloir restreindre les utilisateurs. Cependant, le traitement amélioré du langage naturel (NLP) permet de traduire le contenu dans des langues maîtrisées par les modérateurs, tout en détectant des modèles sémantiques inhabituels sur les sites Web. Cela permet d'identifier les activités extrémistes, le terrorisme, et leurs promoteurs ainsi que la nature de ces activités sur les plateformes de médias sociaux.
- **La susceptibilité à l'extrémisme** : les entreprises technologiques ont mis au point des outils permettant d'évaluer la susceptibilité des individus à adhérer à des idéologies extrémistes violentes. Par exemple, la société « Jigsaw », une filiale d'« Alphabet Inc », anciennement connue sous le nom de « Google Ideas », a lancé un projet intitulé « Redirect » visant les utilisateurs de plateformes de partage de vidéos qui pourraient être vulnérables à la propagande de groupes terroristes tels que « Daech »(Kathleen, 2019).
- **La surveillance** : les applications de l'IA contribuent à identifier le groupe, la partie ou les personnes impliquées dans l'acte terroriste, que ce soit dans son exécution ou sa planification. Cela se fait en analysant les données spécifiques à l'opération, telles que le type d'opération, le lieu, le type d'armes, la cible, en les faisant correspondre avec les antécédents des groupes ou des individus suspects.

2. L'exploitation des logiciels basés sur des algorithmes pour renforcer la lutte contre l'activité terroriste.

Les techniques de reconnaissance faciale et de géolocalisation intégrées à l'IA peuvent être d'une grande utilité pour les enquêteurs criminels en ce qui concerne l'identification des suspects et la détermination de leurs emplacements, ce qui améliore l'efficacité des enquêtes et contribue à maintenir la sécurité. Nous allons aborder le rôle de l'IA dans l'amélioration de l'efficacité des opérations antiterroristes de la manière suivante :

Premièrement - les outils exploitables pour analyser les preuves médico-légales à l'aide de l'IA :

L'IA avancée désigne un système d'IA sophistiqué qui exploite l'apprentissage automatique ainsi que les techniques de reconnaissance vocale, d'images et de traitement du langage naturel pour analyser les éléments de preuve dans les affaires criminelles. Ce système s'appuie sur des données relatives aux crimes, aux suspects, aux victimes, aux témoins et à d'autres informations disponibles afin d'effectuer une analyse précise et efficace des preuves (Salah Ahmed, 2022).

Deuxièmement, le rôle des algorithmes dans l'inférence et la détection des indices de terrorisme :

- L'utilisation de l'IA pour prédire le terrorisme représente une transition d'une approche réactive à une approche proactive dans la lutte contre le terrorisme (Issa Haidi, 2021).
- Les algorithmes d'inférence sont utilisés pour détecter les signes du terrorisme dans n'importe quel environnement et pour identifier les modèles ou tendances dans les données ou les informations du renseignement qui pourraient indiquer la possibilité d'une attaque terroriste. Ces algorithmes analysent les données à la recherche de modèles ou de liens spécifiques entre les différents éléments qui pourraient indiquer un complot terroriste (Fahd, Wijdan, 2022).
- L'analyse des données provenant des caméras de surveillance et d'autres sources permet de repérer des comportements ou des activités suspectes.

Ensuite, l'inférence peut être utilisée pour déduire des conclusions à partir de ces données (Babili Ammar, 2023).

- **L'analyse des données massives :** cela implique l'examen des données relatives au terrorisme, la détection de modèles, de tendances et d'informations exploitables pour repérer d'éventuelles menaces terroristes.
- **Les techniques d'apprentissage automatique**, telles que la classification, le regroupement et la prédiction, sont utilisées pour analyser les données liées au terrorisme et identifier des modèles potentiels des activités terroristes (Schroeter-Marie, 2022).
- **L'analyse textuelle** consiste à examiner les textes liés au terrorisme, identifier les mots, les phrases et les schémas de communications terroristes.
- **L'analyse temporelle** peut être utilisée pour déterminer les moments d'activité des terroristes et les opérations terroristes potentielles.
- **L'analyse comportementale** peut être utilisée pour analyser le comportement des suspects et les activités terroristes potentielles, ainsi que pour identifier les informations permettant d'identifier les suspects et de prévenir les attaques terroristes.
- Ces outils et techniques sont couramment utilisés par les services de sécurité et de renseignement pour lutter contre le terrorisme et réduire les risques d'attaques terroristes potentielles. De nombreux exemples concrets illustrent comment l'IA et les algorithmes peuvent être utilisés pour lutter contre le terrorisme et prédire les opérations terroristes.

Troisièmement, l'utilisation de l'IA dans la lutte contre la contrebande d'armes à feu :

Les flux d'armes illégales jouent un rôle prépondérant dans l'exacerbation des conflits dans de nombreux pays, allant des délits mineurs aux activités terroristes. Leurs effets négatifs sont multiples, notamment en ce qui concerne les armes légères et de petit calibre illégales, qui menacent la sécurité nationale et la paix dans les États. Environ 80 % des armes légères sont détenues par des civils, y compris des milices et des groupes terroristes.

L'IA peut jouer un rôle essentiel dans la lutte contre la contrebande d'armes à feu vers les terroristes. Voici quelques exemples de son utilisation dans ce contexte :

- **La surveillance des frontières et des ports** : l'analyse des données géographiques, des flux de circulation et des informations portuaires permet de détecter des modèles inhabituels ou suspects de contrebande d'armes à feu. Les systèmes dotés d'intelligence artificielle peuvent alerter les services de sécurité sur les activités suspectes.
- **L'analyse des renseignements** : il s'agit de l'analyse des informations et du renseignement liés aux réseaux terroristes et au trafic illégal d'armes à feu. Les techniques avancées d'apprentissage automatique peuvent analyser des données massives, extraire des modèles, des tendances et établir des liens entre les suspects et les activités de contrebande d'armes à feu.
- **L'analyse comportementale et la reconnaissance de modèles** : il s'agit de l'analyse des données comportementales et de la reconnaissance des modèles communs dans les comportements des trafiquants et des terroristes potentiels grâce à la surveillance et à l'analyse du comportement. Cela permet de détecter les comportements inhabituels ou suspects qui indiquent la contrebande d'armes à feu.

Dans le contexte de la lutte contre la contrebande d'armes à feu vers les terroristes, il est possible d'utiliser divers outils, méthodes et algorithmes reposant sur l'IA, notamment : -

- L'apprentissage automatique : les techniques d'apprentissage automatique peuvent être utilisées pour développer des modèles capables de reconnaître les schémas de contrebande d'armes à feu. Ces modèles sont formés à l'aide d'un large éventail de données, y compris des exemples connus de cas de trafic.
- La reconnaissance d'images et de vidéos par la vision par ordinateur : les techniques de vision par ordinateur peuvent être employées pour repérer les armes à feu dans les images. Les algorithmes de détection de formes et de motifs analysent les images et les vidéos en vue de reconnaître les armes qu'elles contiennent. Ces méthodes peuvent être utilisées aux points de contrôle ou pour surveiller les frontières en vue de détecter les armes de contrebande.
- **Les réseaux de neurones profonds** : ils permettent d'extraire des informations à partir de données non structurées et complexes, et peuvent être utilisés pour analyser les textes, les images et les vidéos liés aux opérations de contrebande afin de détecter des modèles et des comportements inhabituels. Les réseaux de neurones profonds établissent des liens entre les individus, les groupes terroristes et criminels opérant clandestinement, en effectuant un regroupement de ces entités et en les surveillant, tout en extrayant des informations pour les services de sécurité.

Quatrièmement - le développement des réseaux de neurones et des algorithmes dans les enquêtes criminelles liées au terrorisme :

Le développement des réseaux de neurones et des algorithmes joue un rôle crucial dans les enquêtes criminelles liées au terrorisme. Les réseaux de neurones

artificiels sont des modèles informatiques inspirés du système cérébral humain. Ils font partie des outils de l'IA utilisés pour analyser les données et extraire des informations essentielles. Leur rôle peut être décrit comme suit :-

- Les réseaux neuronaux et les algorithmes permettent d'extraire des informations cruciales et d'analyser les données massives liées aux crimes terroristes. Plusieurs approches peuvent être utilisées dans ce contexte :

- **Les réseaux neuronaux profonds** peuvent être employés pour analyser les données associées aux actes terroristes. Ils permettent de former des modèles en vue d'extraire des informations et des motifs distinctifs pour identifier les comportements terroristes et anticiper les activités potentielles.
- **Les algorithmes de classification**, tels que la Machine à vecteurs de support (MVS) et l'Arbre de Décision, peuvent être utilisés pour classer les données liées aux enquêtes criminelles liées au terrorisme. Ces algorithmes contribuent à l'identification des comportements terroristes et à la distinction entre les activités normales et anormales.
- **Analyse de clusters** consiste à examiner les données relatives aux actes terroristes et les regrouper en catégories similaires. Cela permet d'identifier des motifs communs, des liens entre les actes et de déterminer des groupes potentiels de suspects.

Cinquièmement - le rôle de l'IA dans le renseignement public et l'amélioration du processus de prise de décision, ainsi que dans l'analyse des données massives à des fins de sécurité :

L'analyse des données massives et des informations est devenue un pilier essentiel dans la prise de décisions stratégiques visant à lutter contre la criminalité, le terrorisme et les menaces à la sécurité nationale, ainsi qu'à bâtir des capacités humaines et logistiques pour l'avenir. Le traitement et l'analyse des données massives, associés à l'utilisation de l'IA, révèlent les pistes nécessaires pour détecter et décourager de manière proactive l'activité terroriste, et pour réduire l'espace d'opération, ainsi que pour économiser des efforts et des ressources. Cette approche permet d'améliorer l'efficacité et l'expertise en établissant des connexions et des modèles, en développant des algorithmes pour extraire des prévisions et des indicateurs scientifiques, et en élaborant des étapes d'exécution à partir du flux de données et d'informations. Nous traitons les types d'analyses comme suit (Al-Hajaya Ziad, 2021) :

- Grâce à l'analyse d'informations variées, les systèmes d'IA facilitent une compréhension plus profonde et globale de l'environnement. Ils permettent d'analyser les motifs, de prédire les événements futurs, et de proposer des solutions et des mesures efficaces dans les domaines de la sécurité et du renseignement. En analysant cette grande quantité de données massives, il est possible de fournir des analyses et des scénarios en temps réel et immédiats qui prennent en compte les changements rapides et contribuent ainsi à améliorer le processus de prise de décision et à soutenir les forces militaires sur le terrain. Les données massives sont utilisées dans le domaine de la sécurité nationale pour analyser les actions des individus et collecter des informations sur leurs comportements via les réseaux sociaux. Ces données comprennent des discussions sur des sujets sensibles et délicats, et sont considérées d'une valeur extrême. L'analyse des réseaux sociaux peut être utilisée pour identifier les individus possédant plusieurs «profils» sur ces réseaux en analysant et en connectant les données. L'analyse des réseaux sociaux est également un outil efficace dans la lutte contre le terrorisme, car elle permet de cibler les réseaux de soutien, les localisations des partisans et analyser les données (Rajab Iman, 2019).

Les mécanismes de coopération numérique en matière de lutte contre le cyberterrorisme.

La coopération internationale en matière de sécurité sur divers fronts vise plusieurs objectifs principaux, représentant en réalité de nouvelles dimensions de cette coopération. Ces objectifs sont essentiellement les aspirations communes de toutes les institutions de sécurité des pays arabes. L'objectif ultime est d'étendre la coopération entre les institutions de sécurité arabes et de réaliser la sécurité nationale arabe (Abdul Rahman Moataz, 2020).

Premièrement - les principaux axes de développement des politiques de coopération numérique entre les services de sécurité arabes :

- La coopération entre les services de sécurité arabes s'effectue par le biais de la collecte, de l'analyse et de l'évaluation des informations liées au terrorisme, la détermination des niveaux de menace, l'émission d'alertes concernant les menaces, l'analyse des informations collectées, ainsi que la mise en commun de l'expertise des forces de police, des administrations et des agences gouvernementales impliquées dans la lutte contre le terrorisme, favorisant ainsi une approche collaborative pour l'analyse et le traitement des données. De plus, cette coopération inclut la participation active avec Interpol et Europol en vue de l'échange d'applications de pointe et de technologies relatives aux empreintes génétiques.

Deuxièmement – Moyens de coopération en matière de sécurité numérique pour limiter la propagation de la cybercriminalité :

Crimes de terroristes et financement du terrorisme :

- L'échange d'informations relatif aux activités et aux crimes des groupes et organisations terroristes, ainsi que leurs relations mutuelles, leur leadership, leurs membres, leur structure organisationnelle clandestine, leur visibilité publique, leurs zones d'implantation, leurs sources de

financement, leurs méthodes de formation, et les armes employées, (Hamouda Montaser, 2021) :

- Le développement et le renforcement des méthodes de surveillance, ainsi que l'échange d'informations pour repérer les plans ou les activités visant à faciliter le transport, l'importation, l'exportation, le stockage et l'utilisation d'armes à feu, de munitions, et d'explosifs, ainsi que d'autres matériaux et moyens qui contribuent à commettre des actes terroristes, au-delà des frontières.
- L'examen des flux de données d'un pays à l'autre, ainsi que des données de suivi des adresses IP (protocole Internet).
- La cybercriminalité s'est développée en tant que service, où les criminels utilisent de nouvelles technologies pour commettre des cyberattaques contre des gouvernements, des entreprises et des individus. Ces activités criminelles ne connaissent pas de frontières, qu'elles soient physiques ou virtuelles, et elles causent des dommages significatifs, constituant une menace concrète pour les victimes à travers le monde. Cela souligne l'importance de l'échange de technologies, en particulier pour les services de police chargées de lutter contre la cybercriminalité, afin de comprendre les capacités offertes aux criminels et comment les utiliser comme des outils de lutte contre la cybercriminalité. Cette importance est d'autant plus accentuée par les évolutions des comportements et des tendances en ligne, notamment dans le contexte de la pandémie de COVID-19.
- L'échange des expériences entre les services de sécurité pour combler les lacunes de sécurité liées à la collecte et à l'analyse de toutes les informations disponibles sur les activités criminelles commises dans l'espace numérique dans le but de fournir aux pays des renseignement, tels que :
- La protection de l'infrastructure critique contre les cyberintrusions, et la défense contre les cyberattaques visant les installations importantes et vitales, en particulier les attaques par déni de service.

Bibliographie:

1. Références en Arabe :

Abou Douh Khaled Kazem. (2022). Stratégies pour faire face aux défis de sécurité de l'application « Tik Tok », Centre de recherche sur la sécurité, Université arabe Naif des sciences de sécurité, https://spp.nauss.edu.sa/index.php/spp/article/view/82/60.

Stratégie antiterroriste mondiale des Nations Unies. (s.d.). Stratégie antiterroriste mondiale des Nations Unies. (M.A. Terrorisme, éditeur) Récupéré de https://news.un.org/ar/focus/counter-terrorism.

Terrorisme et droits de l'homme. (s.d.). https://www.ohchr.org/ar/documents/reports/terrorism-and-human-rights-report-united-nations-high-commissioner-human-rights. Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme A/HRC/45/27.

Européen. (2021). « Bitcoin et l'aumône du Jihad sur le Dark Web », Centre européen d'études sur la lutte contre le terrorisme et le renseignement.

Babbli, Ammar. (2023). L'intelligence artificielle face aux rumeurs et au financement du terrorisme dans cyberenvironnement, « Répercussions et moyens de confrontation », Organisation arabe pour le développement administratif, Ligue des États arabes.

Babbli, Ammar. (2023). Mécanismes de l'intelligence artificielle pour lutter contre l'extrémisme violent. Revue des Sciences Policières et Juridiques : Revue scientifique, Volume 14.

Al-Barr Adnan Mustafa. (2020). Big Data et ses Applications, Collège d'Informatique et de Technologie de l'Information, Université King Abdulaziz.

Al-Bahi Raghda. (27,3, 2021). Deepfake : Défis de sécurité et véritables menaces. https://ecss.com.eg/14200/. Centre égyptien d'études stratégiques (ESCC), Unité de cybersécurité.

Al-Hajaya, Ziad. 10 mai 2021. (s.d.). Traitement des mégadonnées et de l'intelligence artificielle dans la lutte contre le crime organisé et le terrorisme « BIG DATA & IA », Jordanie, Centre Shurafat pour les études et la recherche sur la mondialisation et le terrorisme.

Al-Hajaya, Ziad. 10 mai 2021. Traitement des mégadonnées et de l'intelligence artificielle dans la lutte contre le crime organisé et le terrorisme « BIG DATA & IA », Jordanie, Centre Shurafat pour les études et la recherche sur la mondialisation et le terrorisme.

Al-Haqil, N. A. (21 juin, 2023). Efficacité de l'intelligence artificielle dans la lutte contre la criminalité et le terrorisme.

Al-Samalouti, Nabil. (septembre, 2021). Extrémisme et groupes terroristes en Égypte : Origines, objectifs, attitude de l'Islam et méthodes de la lutte. Revue de recherches en sciences sociales et développement, numéro 3.

Al-Sharqawi, Nasreen. (13 octobre 2022). Les rôles doubles des plateformes de médias sociaux. L'Observatoire égyptien. https://marsad.ecss.com.eg/73432/. Centre égyptien de pensée et d'études stratégiques.

Al-Attar, Ahmed Shoukry. (5 avril 2021). Les banques en ligne de Daech effectuent des transactions en Bitcoin. https://www.albawabhnews.com. Consulté le 3 mars 2022.

Al-Alawi, Ibrahim. (2 juillet 2023). Applications de l'intelligence artificielle dans les sciences médico-légales. Revue scientifique des sciences médico-légales.

Al-Amri. (2013). Planification de la sécurité pour faire face aux conséquences des crises internationales, thèse de doctorat, Académie de police.

Le manuel de référence pour la lutte contre le terrorisme. (s.d.). https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF(2020).

Al-Wazan, El Sayed. (2014). Le Pouvoir de l'Information : Une Vision de la Sécurité Contemporaine. Dar Al-Nahda Al-Arabiya.

- Orofino, Elsa. (9 19, 2022). Extrémisme en ligne : comment détecter et traiter les contenus extrémistes (Le cas de Royaume-Uni). https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/. Rapport du site European Eye on Radicalisation.

Programme d'Interpol pour le renforcement des capacités policières. (2019). Interpol. rapport d'Interpol. Disponible sur https://www.interpol.int/ar/1/2/2019/88th-INTERPOL-General-Assembly.

Hamouda, Montasser. (2021). L'Organisation internationale de police criminelle, 2ème édition, Dar Al-Fikr Al-Jami'i.

Khalifa, I. (2018). Opportunités et menaces de l'intelligence artificielle dans les dix prochaines années, Rapport sur l'avenir.

David Omand, Carl. (2015). L'intelligence des médias sociaux, numéro 152, Centre d'Études et de Recherches Stratégiques des Émirats Arabes Unis.

Rashed, Sameh. (octobre, 2021). Intelligence Artificielle face au terrorisme: Opportunités et défis. Revue Perspectives Stratégiques (4).

Al-Qadi Ramy Metwally, La confrontation sécuritaire internationale des activités criminelles commises sur le Dark Web. Reu de la sécurité publique (253).

Rajab Iman. (2019). Politiques antiterroristes en Égypte (296) Centre d'études politiques et stratégiques.

Schroeter-Marie. (2022). Intelligence artificielle et lutte contre l'extrémisme violent. King's College London : Projet GNET. Centre international pour l'étude des radicaux.

Saghur Hisham. (7, 11, 2019). Les sites de réseaux sociaux : une plateforme fertile pour propager l'extrémisme et attirer les « djihadistes ». https://www.europarabct.com/?p=53141. Centre européen d'études sur la lutte contre le terrorisme et le renseignement.

Saleh, Ahmed. (2022). Applications de l'intelligence artificielle et leur rôle dans la gestion sécuritaire des foules. [Thèse de doctorat, Académie de police].

Saleh, J.A. (2014). Le terrorisme intellectuel, ses formes et ses pratiques. Librairie du Droit et de l'Économie.

Abdelsalam, Sh. (2020). Les guerres de cinquième génération : Les méthodes d'explosion depuis l'intérieur sur la scène internationale. Centre d'études et de recherche avancée sur l'avenir.

Abdel-Sadek, Adel. (2018). Les cryptomonnaies : une menace pour l'économie et la sécurité nationale. Centre arabe de recherche sur le cyberespace.

Abdel-Moaty, N. (2012). Les plateformes de médias sociaux et la production de l'extrémisme et du terrorisme. La réalité et les stratégies de lutte : Revue de politique internationale (213).

Al-Babli, Ammar. (2022). La coopération numérique en matière de sécurité entre les organismes de sécurité arabes. Documents de politique de sécurité, Université arabe Naif des sciences de sécurité.

Wajdan, Fahd. (2022, 1er mars). Étude sur l'intelligence artificielle : entre les tactiques terroristes et les stratégies nationales. https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/. Centre de recherche et d'études Trends.

Fouda Hala. (2020, 11 22). Médias sociaux et sécurité nationale des pays. https://marsad.ecss.com.eg/21163. Centre égyptien de pensée et d'études stratégiques.

Kanso, Ali. (2021). La guerre électronique. Revue scientifique de la Défense Nationale Libanaise, (118).

Centre d'innovation INTERPOL. (2019). Intelligence artificielle et application de la loi, Partenariat pour les futures menaces de sécurité. https://www.interpol.int/ar/4/4/2. Interpol, Rapport sur la sécurité internationale.

Abdulrahman, Moataz. (2020). Le rôle de l'échange international d'informations dans la preuve pénale. [Thèse de doctorat, Académie de police].

Miqdadi Saleh. (3, 5, 2021). Rapport international, incitations à la coopération internationale dans la lutte contre le terrorisme, Coalition Islamique Militaire Contre le Terrorisme (CIMCT). https://imctc.org/ar/Pages/default.aspx.

Office des Nations Unies contre la drogue et le crime. (2021). Coopération internationale en matière pénale liée à la lutte contre le terrorisme. https://www.unov.org/unov/ar/unodc.html.

Site « Independent » en arabe. (17 décembre, 2021). Les cyberattaques, l'arme économique la plus dangereuse au monde en 2022. https://www.independentarabia.com.

Issa Haidi. (1, 2021). Les droits de l'homme à l'ère de l'intelligence artificielle : données, visions et solutions. Revue de la charia et du droit, volume 35.

Références en Anglais :

Le Manuel de Référence pour la Lutte Contre le Terrorisme. (2023)

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF (2020)

ALGORITHMS AND TERRORISM. (2023). *THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE FOR TERRORIST PURPOSES, United Nations Office of Counterterrorism (UNOCT), 2021 New York, AT.* https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1.

belfercenter.ksg.harvard. (2023). *Joseph S. Nye ،The Future of Power. Press Release ،Harvard Kennedy School ،Belter Center for Science and International Affairs ، December 2019 at :http://belfercenter.ksg.harvard.edu/publication/20690/joseph_s_nyes_the_future_of_power.html* .Récupéré belfercenter.ksg.harvard.

blog.khamsat. (2022). *https://blog.khamsat.com/tiktok-profit-guide ./*Récupéré https://blog.khamsat.com/tiktok-profit-guide./

Canada Police. (2021). *Police use of Facial Recognition Technology in Canada and the way forward .'*police science ،Canada.

Christopher Rigano) .January, 2019' .(*Using Artificial Intelligence to Address Criminal Justice Needs) ,'US NIJ Journal 280, January 2019* .(Récupéré www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx accessed 2 December 2021.

Course.elementsofai. (2020). *https://course.elementsofai.com/1/1: Reaktor & University of Helsinki) 2018(, How should we define AI.2 '? Page 10* ....Récupéré https://course.elementsofai.com/1/1.

Demandsage . (2023, 2). *https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of .%*Récupéré https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of.%

Hames (sep 4, 2020). Récupéré Terror and Technology from Dynamite to Drones. War on the Rocks. Accessible at https://warontherocks.com/2020/09/terror-and-technology-from-dynamite-to-drones/

Kathleen. (2019). *International security Department ،CHATHAM HOUSE ،August 2019. P.9* .CHATHAM HOUSE.

molla, R. and Stewart, E. (3 12, 2019). *(2019), How 2020 Democrats think about breaking up Big Tech ,'Vox. Accessed* .Récupéré https://www.vox.com/policy-and-politics/2019/12/3/20965447/tech-2020-candidate-policies-break-up-big- tech.

Office of the Privacy Commissioner of Canada. (n.d.). *Office of the Privacy Commissioner of Canada' ،Police use of Facial Recognition Technology in Canada and the way forward.'*

Quemener (M). (2017). *Quemener (M ،(Enquetes dans le Darkweb، Dalloz IP/IT*) Version Dalloz IP/IT.(

Valentini D.; Lorusso A.; Stephan A. (2020). *Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization, in Frontiers in Psychology. ,*

Wiesenthal. (2021). Récupéré https://www.wiesenthal.com/about/regional-offices/los-angeles.html

Abou Douh Khaled Kazem. (2022). Stratégies pour faire face aux défis de sécurité de l'application « Tik Tok », Centre de recherche sur la sécurité, Université arabe Naif des sciences de sécurité, https://spp.nauss.edu.sa/index.php/spp/article/view/82/60.

Stratégie antiterroriste mondiale des Nations Unies. (s.d.). Stratégie antiterroriste mondiale des Nations Unies. (M.A. Terrorisme, éditeur) Récupéré de https://news.un.org/ar/focus/counter-terrorism.

Terrorisme et droits de l'homme. (s.d.). https://www.ohchr.org/ar/documents/reports/terrorism-and-human-rights-report-united-nations-high-commissioner-human-rights. Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme A/HRC/45/27.

Européen. (2021). « Bitcoin et l'aumône du Jihad sur le Dark Web », Centre européen d'études sur la lutte contre le terrorisme et le renseignement.

Babbli, Ammar. (2023). L'intelligence artificielle face aux rumeurs et au financement du terrorisme dans cyberenvironnement, « Répercussions et moyens de confrontation », Organisation arabe pour le développement administratif, Ligue des États arabes.

Babbli, Ammar. (2023). Mécanismes de l'intelligence artificielle pour lutter contre l'extrémisme violent. Revue des Sciences Policières et Juridiques : Revue scientifique, Volume 14.

Al-Barr Adnan Mustafa. (2020). Big Data et ses Applications, Collège d'Informatique et de Technologie de l'Information, Université King Abdulaziz.

Al-Bahi Raghda. (27,3, 2021). Deepfake : Défis de sécurité et véritables menaces. https://ecss.com.eg/14200/. Centre égyptien d'études stratégiques (ESCC), Unité de cybersécurité.

Al-Hajaya, Ziad. 10 mai 2021. (s.d.). Traitement des mégadonnées et de l'intelligence artificielle dans la lutte contre le crime organisé et le terrorisme « BIG DATA & IA », Jordanie, Centre Shurafat pour les études et la recherche sur la mondialisation et le terrorisme.

Al-Samalouti, Nabil. (septembre, 2021). Extrémisme et groupes terroristes en Égypte : Origines, objectifs, attitude de l'Islam et

méthodes de la lutte. Revue de recherches en sciences sociales et développement, numéro 3.

Al-Sharqawi, Nasreen. (13 octobre 2022). Les rôles doubles des plateformes de médias sociaux. L'Observatoire égyptien. https://marsad.ecss.com.eg/73432/. Centre égyptien de pensée et d'études stratégiques.

Al-Attar, Ahmed Shoukry. (5 avril 2021). Les banques en ligne de Daech effectuent des transactions en Bitcoin. https://www.albawabhnews.com. Consulté le 3 mars 2022.

Al-Alawi, Ibrahim. (2 juillet 2023). Applications de l'intelligence artificielle dans les sciences médico-légales. Revue scientifique des sciences médico-légales.

Al-Amri. (2013). Planification de la sécurité pour faire face aux conséquences des crises internationales. Thèse de doctorat. Faculté des études supérieures. Académie de police. Le Caire.

Al-Wazan, El Sayed. (2014). Le Pouvoir de l'Information : Une Vision de la Sécurité Contemporaine. Dar Al-Nahda Al-Arabiya.

Orofino, Elsa. (9 19, 2022). Extrémisme en ligne : comment détecter et traiter les contenus extrémistes (Le cas de Royaume-Uni). https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/. Rapport du site European Eye on Radicalisation.

Khalifa, I. (2018). Opportunités et menaces de l'intelligence artificielle dans les dix prochaines années, Rapport sur l'avenir.

Programme d'Interpol pour le renforcement des capacités policières. (2019). Interpol. rapport d'Interpol. Disponible sur https://www.interpol.int/ar/1/2/2019/88th-INTERPOL-General-Assembly.

Jamal al-Din Muhammad Saleh. (2014). «Le terrorisme intellectuel: ses formes et pratiques» (Volume 1). Riyadh : Librairie du Droit et de l'Économie.

Hamouda, Montasser. (2021). L'Organisation internationale de police criminelle, 2ème édition, Dar Al-Fikr Al-Jami'i.

David Omand, Carl. (2015). L'intelligence des médias sociaux, numéro 152, Centre d'Études et de Recherches Stratégiques des Émirats Arabes Unis.

Rashed, Sameh. (octobre, 2021). Intelligence Artificielle face au terrorisme: Opportunités et défis. Revue Perspectives Stratégiques (4).

Ramy Metwally, Al-Qadi. La confrontation sécuritaire internationale des activités criminelles commises sur le Dark Web. Reu de la sécurité publique (253).

Rajab Iman. (2019). Politiques antiterroristes en Égypte (296) Centre d'études politiques et stratégiques.

Ziad, Al-Hajaya. 10 mai 2021. (s.d.). Traitement des mégadonnées et de l'intelligence artificielle dans la lutte contre le crime organisé et le terrorisme « BIG DATA & IA », Jordanie, Centre Shurafat pour les études et la recherche sur la mondialisation et le terrorisme.

Shady, Abdelsalam. (2020). Les guerres de cinquième génération : Les méthodes d'explosion depuis l'intérieur sur la scène internationale. Centre d'études et de recherche avancée sur l'avenir.

Schroeter-Marie. (2022). Intelligence artificielle et lutte contre l'extrémisme violent. King's College London : Projet GNET. Centre international pour l'étude des radicaux.

Saghur Hisham. (7, 11, 2019). Les sites de réseaux sociaux : une plateforme fertile pour propager l'extrémisme et attirer les «djihadistes». https://www.europarabct.com/?p=53141. Centre européen d'études sur la lutte contre le terrorisme et le renseignement.

Saleh, Ahmed. (2022). Applications de l'intelligence artificielle et leur rôle dans la gestion sécuritaire des foules. [Thèse de doctorat, Académie de police].

Saleh, J.A. (2014). Le terrorisme intellectuel, ses formes et ses pratiques. Librairie du Droit et de l'Économie.

Abdel-Sadek, Adel. (2018). Les cryptomonnaies : une menace pour l'économie et la sécurité nationale. Centre arabe de recherche sur le cyberespace.

Ali, Moataz Abdulrahman. (2020). Le rôle de l'échange international d'informations dans la preuve pénale. [Thèse de doctorat, Académie de police].

Ammar, Al-Babli. (2022). La coopération numérique en matière de sécurité entre les organismes de sécurité arabes. Documents de politique de sécurité, Université arabe Naif des sciences de sécurité.

Ammar, Al-Babli. (2022). La coopération numérique en matière de sécurité entre les organismes de sécurité arabes. Documents de politique de sécurité, Université arabe Naif des sciences de sécurité.

Fahd, Wajdan. (1er mars, 2022). Étude sur l'intelligence artificielle : entre les tactiques terroristes et les stratégies nationales. https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/. Centre de recherche et d'études Trends.

Fouda Hala. (2020, 11 22). Médias sociaux et sécurité nationale des pays. https://marsad.ecss.com.eg/21163. Centre égyptien de pensée et d'études stratégiques.

Kanso, Ali. (2021). La guerre électronique. Revue scientifique de la Défense Nationale Libanaise, (118).

Centre d'innovation INTERPOL. (2019). Intelligence artificielle et application de la loi, Partenariat pour les futures menaces de sécurité. https://www.interpol.int/ar/4/4/2. Interpol, Rapport sur la sécurité internationale.

Abdulrahman, Moataz. (2020). Le rôle de l'échange international d'informations dans la preuve pénale. [Thèse de doctorat, Académie de police].

Miqdadi Saleh. (3, 5, 2021). Rapport international, incitations à la coopération internationale dans la lutte contre le terrorisme, Coalition Islamique Militaire Contre le Terrorisme (CIMCT). https://imctc.org/ar/Pages/default.aspx.

Office des Nations Unies contre la drogue et le crime. (2021). Coopération internationale en matière pénale liée à la lutte contre le terrorisme. https://www.unov.org/unov/ar/unodc.html.

Site« Independent »en arabe. (17 décembre, 2021). Les cyberattaques, l'arme économique la plus dangereuse au monde en 2022. https://www.independentarabia.com.

Miller, M. David Omand, Carl. (2015). L'intelligence des médias sociaux, numéro 152, Centre d'Études et de Recherches Stratégiques des Émirats Arabes Unis.

Naglaa Abdelrahman Al-Haqil. (21 juin, 2023). Efficacité de l'intelligence artificielle dans la lutte contre la criminalité et le terrorisme.

Noha, Abdel-Moaty. (2012). Les plateformes de médias sociaux et la production de l'extrémisme et du terrorisme. La réalité et les stratégies de lutte : Revue de politique internationale (213).

Issa Haidi. (1, 2021). Les droits de l'homme à l'ère de l'intelligence artificielle : données, visions et solutions. Revue de la charia et du droit, volume 35.