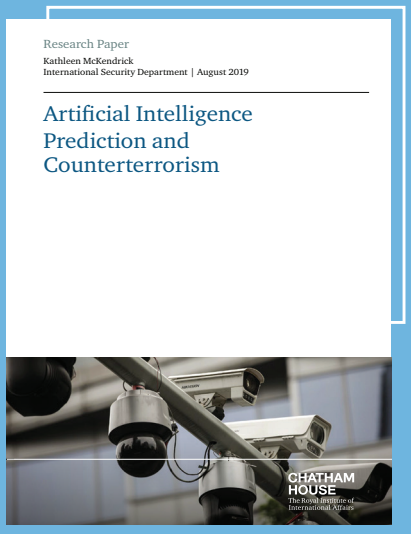
التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION
Département Général de la
Planification et de la Coordination

À propos

9
Rapports spéciaux
Jan. 2020

Intelligence artificielle et lutte contre le terrorisme

Limites, opportunités et risques




التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

9

Rapports spéciaux

Jan. 2020

À propos

Intelligence artificielle et lutte contre le terrorisme

Limites, opportunités et risques

Le terme intelligence artificielle fait référence à la capacité des machines numériques et des ordinateurs à effectuer des tâches spécifiques similaires à ce que font les êtres vivants intelligents, comme la capacité de penser et de planifier, d'apprendre et de créer, d'adapter et d'interagir, d'améliorer les procédures, d'extraire des connaissances et de prédire à partir de données numériques volumineuses et variées, et d'autres opérations qui nécessitent des processus mentaux précis.

Les experts antiterroristes disent qu'il existe deux façons de prévenir les attaques terroristes. La première consiste à protéger les infrastructures et les individus et à mettre en place des contrôles de sécurité. L'autre consiste à priver les terroristes de la possibilité de lancer des attaques, en les arrêtant avant de mener à bien leurs plans et en luttant contre l'extrémisme et le recrutement de terroristes.

Le rapport, préparé par le chercheur, Kathleen McKendrick sous l'intitulé (Intelligence artificielle et lutte contre le terrorisme) publié par le Chatham House Institute en août 2019, discute la relation multidimensionnelle entre le terrorisme et l'intelligence artificielle, les limites, les opportunités disponibles et les risques potentiels.

Une question logique peut venir à l'esprit au sujet de la relation entre l'intelligence artificielle et la lutte contre le terrorisme, or la réponse réside dans un mot, la «prédiction», qui est l'une des fonctions les plus importantes de l'intelligence artificielle, car elle contribue à prévenir les attaques terroristes en fournissant une protection physique de l'infrastructure et en améliorant l'attribution des ressources aux sites considérés comme des cibles potentiels d'attaques terroristes. L'IA aide aussi à empêcher les terroristes de lancer des attaques, en les appréhendant avant qu'ils ne passent à l'action. Elle contribue également à lutter contre le recrutement de terroristes et à reconnaître les personnes les plus exposées à l'extrémisme ou au recrutement par des organisations terroristes.

La lutte réussie contre le terrorisme vise à assurer la sécurité de la majorité des citoyens, avec une atteinte minimale aux droits et libertés. La prédiction permet d'appliquer des mesures préventives pour réduire les dommages que peut subir la population, et peut focaliser sur les actions violentes que les terroristes ont l'intention de mener ou sur les individus exposés à l'extrémisme, de sorte que la prédiction fournie par l'intelligence artificielle soit un moyen pour mieux gérer les ressources réservées à la lutte contre le terrorisme, et d'éviter de gaspiller les efforts et les ressources dans ce domaine.

L'utilisation de l'intelligence artificielle dans la lutte contre le terrorisme peut conduire à des prévisions précises qui limitent les mesures inutiles appliquées à un grand nombre de personnes et réduisent le biais humain dans la prise de décision, en attirant soigneusement l'attention sur les zones ou les individus les plus vulnérables aux menaces, et en réduisant le nombre de citoyens soumis aux contrôles serrés. D'un autre côté, le manque de garanties adéquates pour l'utilisation de l'intelligence artificielle, et les énormes bases de données dont elle dépend, conduit non seulement à leur utilisation abusive aux dépends des citoyens, mais également à une violation excessive d'autres droits tels que le respect de la vie privée et la liberté d'expression.

L'utilisation de l'intelligence artificielle terrorisme peut conduire à des prévisions précises qui limitent les mesures inutiles appliquées à un grand nombre de personnes et réduisent les biais humains dans la prise de décision.

L'approche consistant à utiliser des techniques de prévision précises usant de l'intelligence artificielle dans la lutte contre le terrorisme peut être soumise à des objectifs contradictoires, mais cela n'empêche pas d'examiner les possibilités et les coûts d'une telle approche et la manière d'organiser ce domaine naissant.

Applications de l'intelligence artificielle dans la lutte contre le terrorisme

Les capacités d'intelligence artificielle prédictive sont reconnues dans la lutte contre le terrorisme, mais son application est encore à petite échelle. Les services de sécurité et de renseignement utilisent l'analyse automatique des données pour évaluer les risques que présentent certains passagers aériens et révéler les liens entre les organisations terroristes et leurs membres. La police l'utilise également pour analyser les réseaux de gangs criminels et certaines entreprises technologiques utilisent des mesures prédictives avancées pour surveiller et désactiver les activités terroristes sur les plateformes de médias sociaux. L'intelligence artificielle est utilisée également dans le secteur des services financiers pour signaler toute activité suspecte.

L'absence de garanties adéquates pour l'utilisation de l'intelligence artificielle et les énormes bases de données qui en dépendent conduisent non seulement à son utilisation abusive en imposant le contrôle aux citoyens, mais aussi à une violation excessive d'autres droits tels que le respect de la vie privée et la liberté d'expression.

Voici à présent quelques exemples des capacités de l'intelligence artificielle à lutter contre le terrorisme par le biais de la prédiction:

1- Prédire le moment et le lieu des attaques terroristes

L'intelligence artificielle peut être utilisée pour prédire les opérations terroristes en fonction des métadonnées de communication, des informations sur les transactions financières, des modèles de voyage et des activités de navigation sur Internet. Des prototypes ont été développés pour prédire l'emplacement et le moment des attaques terroristes. En 2015, par exemple, une startup technologique a affirmé que son modèle prédictif était capable de prédire les attentats suicides avec une précision de 72%. Certains autres modèles se sont également appuyés sur des données des logiciels libres pour les personnes qui utilisent les médias sociaux et les applications sur leurs téléphones portables, y compris un système de reconnaissance préventif d'événement qui intègre les résultats de différents modèles prédictifs distincts pour prévoir des événements spécifiques. Davantage de données ne signifient pas nécessairement que la qualité des prévisions s'est améliorée, mais il faudrait avant tout valider ces prévisions.

2- Connaître les vulnérabilités et les dispositions à l'extrémisme

Certaines entreprises technologiques ont développé des outils pour évaluer la vulnérabilité aux idées et croyances extrémistes violentes. Une entreprise a annoncé un projet appelé (Réorientation) ciblant les utilisateurs de sites (vidéo) susceptibles de faire l'objet de propagande terroriste. Le projet en question les redirige vers des clips (vidéo) qui adoptent une narration fiable et anti-terroriste.

3- Connaître les terroristes

Certaines informations divulguées sur un programme de la National Security Agency (SKYNET) relevant des Etats-Unis font état d'un algorithme basé sur l'IA ayant été utilisé pour analyser les métadonnées d'environ 55 millions d'utilisateurs de téléphones mobiles au Pakistan en 2007 ; le résultat obtenu montre qu'environ 15 000 personnes pourraient devenir des terroristes sur une population de 200 personnes millions à l'époque. Bien que le modèle utilisé n'ait pas fait preuve d'efficacité en soi, il a toutefois montré la valeur prédictive des données en cas d'identification de liens étroits avec le terrorisme.

Ces cas d'utilisation de capacités prédictives de l'IA dans la lutte contre le terrorisme demeurent toujours du ressort de l'éventuel, et l'IA ne devrait pas fournir de réponses immédiates, complètes et précises à des questions complexes. Cependant, la capacité de développer des outils d'IA à cette fin dépend de ceux qui ont la possibilité d'accéder aux données ou de les protéger. Avec l'amélioration des performances de l'IA, il y aura plus de possibilités pour obtenir des prédictions précises sur le terrorisme à l'avenir et recourir davantage à cet outil pour combattre ce fléau.

La possibilité de prédire une implication terroriste était auparavant impossible, mais ce n'est plus le cas. Il est possible d'améliorer la précision des modèles prédictifs basés sur une source unique de données en combinant ses résultats avec d'autres conclusions.

Les Défis

Il existe deux défis liés à l'utilisation de l'intelligence artificielle dans la lutte contre le terrorisme, le premier concernant les droits de l'homme et le second lié aux implications pratiques de cette technologie.

I. Défis relatifs aux droits de l'homme:

1- L'absence de normes établies pour l'utilisation des technologies d'intelligence artificielle

Il n'y a pas de position internationale unifiée sur les limites de l'utilisation de l'intelligence artificielle, ce qui met en jeu les droits et libertés des citoyens, de sorte que le besoin de garanties adéquates pour l'utilisation de l'intelligence artificielle par les gouvernements et les services de sécurité augmente, de même qu'un examen des mesures établies pour protéger la vie privée et les libertés fondamentales des citoyens.

En décembre 2014, l'Assemblée générale des Nations Unies a adopté la résolution 68/167 sur le droit à la vie privée à l'ère numérique selon laquelle les États ont la responsabilité de veiller à ce que leurs activités soient conformes au droit international. En décembre 2016, la Cour européenne a rendu une décision contre la Grande-Bretagne pour non-respect des droits fondamentaux garantis par l'Union européenne dans les pratiques de conservation des données.

2- Collecte aléatoire de données

De nombreuses pratiques liées à l'utilisation de la technologie prédictive de l'intelligence artificielle dans la lutte contre le terrorisme s'appliquent à l'ensemble de la population, ce qui les rend aléatoires et viole la vie privée du public. Les cadres législatifs et les principes de gouvernance liés à l'utilisation des données tendent à réglementer les pouvoirs d'accès aux données et ignorent souvent toute réglementation sur la manière dont ces données devraient être utilisées ou protégées contre les abus.

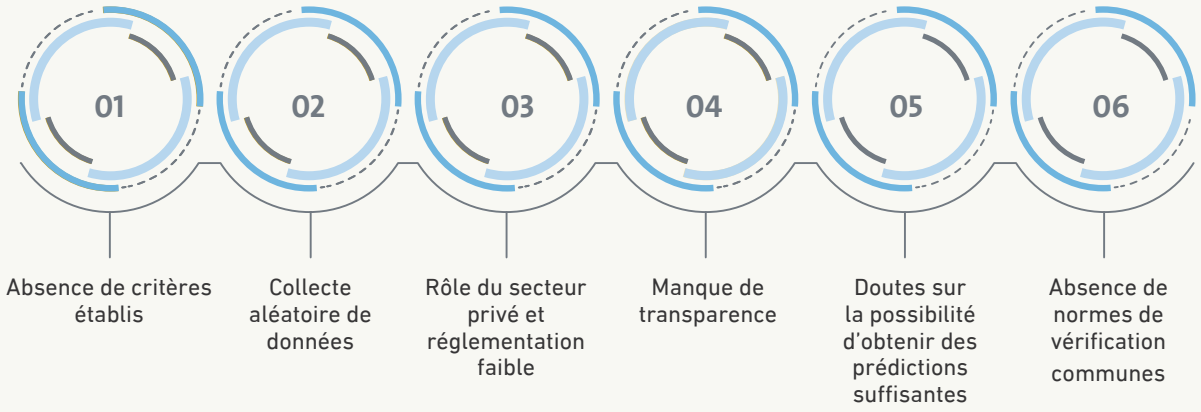
3- Rôle du secteur privé en croissance et faiblesse de l'organisation

La responsabilité des utilisations prédictives de l'intelligence artificielle pour lutter contre le terrorisme est répartie entre un large éventail d'acteurs, dont les entreprises technologiques, qui ont pour certaines transformé les données publiques en une marchandise à vendre à qui veut bien payer! Les organismes chargés de l'application des lois peuvent être en mesure de les obtenir légalement, ce qui signifie que les obligations des entreprises de protéger la confidentialité des clients sont à mettre en doute.

4- Manque de transparence

Les types de recours à l'intelligence artificielle pour lutter contre le terrorisme sont sujets à un black-out serré, à cause duquel il est difficile d'obtenir des garanties juridiques de transparence dans la lutte contre le terrorisme.

Défis de l'utilisation de l'intelligence artificielle pour lutter contre le terrorisme



2. Défis pratiques:

1- Faible capacité à réaliser des prévisions adéquates

Le phénomène terroriste présente de nombreux aspects et emprunte des voies multiples, ce qui signifie qu'il est impossible d'établir une liste finale d'indicateurs d'implication ou d'exclusion du terrorisme. Le petit nombre de terroristes parmi la population générale fait en sorte que la détermination de larges caractéristiques des terroristes sur la base de stéréotypes n'a aucune valeur prédictive. La faible incidence du terrorisme et la tendance des moyens terroristes à se développer rapidement rendent difficile la mise au point de bons modèles prédictifs.

Un groupe de recherches récentes a confirmé que les résultats prédictifs de l'IA pourraient être scientifiquement plus objectifs que les évaluations humaines affectées par les biais culturels.

Cependant, la recherche a montré qu'il est fort possible d'utiliser l'intelligence artificielle pour analyser les communications et les caractéristiques distinctives, telles que le degré d'extrémisme ou l'intention d'agression, ce qui signifie que la capacité de prédire une implication terroriste n'est plus de l'ordre de l'impossible à l'heure actuelle. Il est possible d'améliorer la précision des modèles prédictifs basés sur une seule source de données en combinant ses résultats avec les autres conclusions. Toutefois, la restriction d'accès aux données peut limiter (l'efficacité) de l'intelligence artificielle dans l'accomplissement de ces tâches.

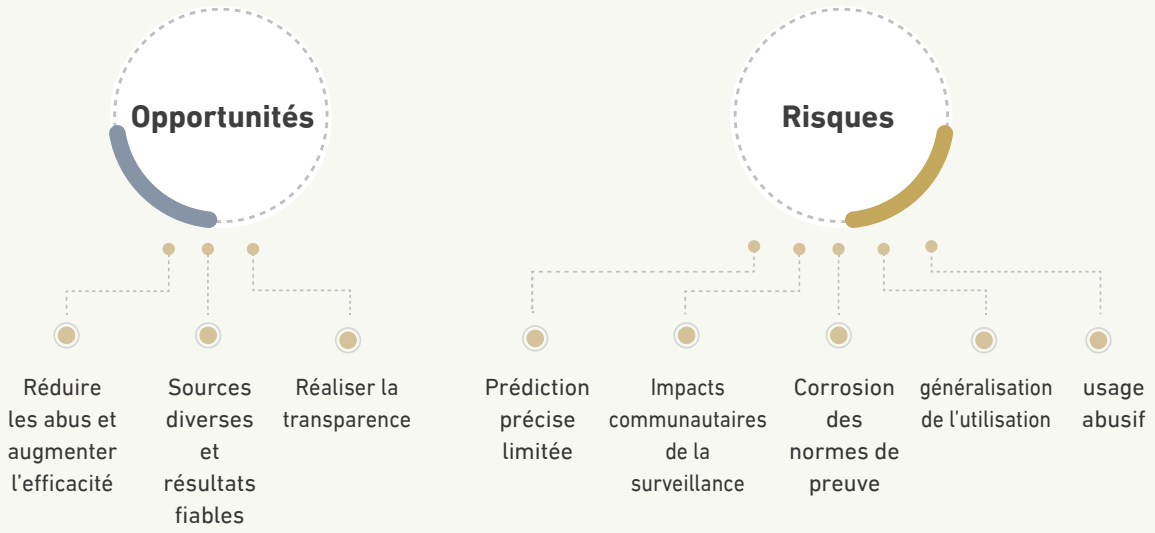
2- L'absence de critères communs de vérification

Tout important qu'il soit, l'accès aux données ne garantit pas à lui seul la construction de modèles prédictifs précis et viables. La validation et l'examen des résultats donnés par ces modèles sont indispensables pour mesurer leur exactitude prédictive et évaluer la pertinence de leur utilisation. Étant donné le large éventail d'acteurs impliqués, l'établissement de normes communes acquiert une grande importance. L'adoption par les agences de renseignement, les forces de l'ordre et le secteur privé, des techniques utilisées par l'intelligence artificielle signifie que le recours à l'IA et le développement de ses techniques pour lutter contre le terrorisme est en croissance. Un groupe de recherches récentes s'est concentré sur l'étendue du parti pris de la part de l'intelligence artificielle et a confirmé que les résultats prédictifs de l'intelligence artificielle pourraient être scientifiquement plus objectifs que les évaluations humaines affectées par les biais culturels.

Opportunités et risques

Les défis susmentionnés résultent du développement désorganisé de l'intelligence artificielle comme moyen pour prédire le terrorisme. Est-il possible d'utiliser le pouvoir prédictif de l'intelligence artificielle de manière

Opportunités et risques de l'intelligence artificielle dans la lutte contre le terrorisme



légitime comme outil de détection du terrorisme par l'État?

Cela stipule d'accorder aux agences gouvernementales un accès plus large aux données publiques, avec une réglementation plus précise de la façon dont ces données sont utilisées. Cette approche nécessite la collecte et l'analyse des données sur les citoyens, ce qui est inacceptable dans de nombreux pays.

I. Opportunités:

1- Réduire les abus et renforcer l'efficacité

Le processus d'analyse automatisée des données est entaché de nombreuses violations, mais il contribue néanmoins à réduire la violation de la vie privée des citoyens par rapport à l'analyse humaine. Il peut s'avérer nécessaire, lors de l'utilisation d'un modèle prédictif pour automatiser l'analyse des données publiques, de poser comme condition l'efficacité du modèle, c'est-à-dire de fournir une relation causale avec un objectif spécifique, à défaut d'autres alternatives, et de démontrer que les avantages l'emportent sur les coûts associés à la violation des droits.

2- Sources Diverses et résultats fiables

L'intelligence artificielle peut aider à développer des sources distinctes pour collecter des informations et valider les résultats, plutôt que de compter sur une option centralisée dépendant d'un système unique qui inclut tous les individus, qu'ils soient terroristes ou susceptibles de l'être. Bien que la validation soit nécessaire, ce domaine est encore en pleine mutation, et l'utilisation de méthodes automatisées offre la possibilité d'évaluer les performances du modèle et de mesurer sa faisabilité.

Les fournisseurs de services de télécommunications seraient plus disposés à accepter les demandes d'accès à leurs données s'ils se rendent compte que les normes de ces requêtes sont élevées et qu'elles poursuivent un objectif légitime et réalisent de bons résultats.

Il ne fait aucun doute que le traitement des personnes exposées à l'extrémisme et les vrais terroristes au sein du système lui-même engendre une ambiguïté qui empêche de veiller à une véritable discrimination entre eux, sauf par le biais de systèmes prédictifs basés sur l'analyse de données créées et préservées numériquement,

car ces données sont neutres, fiables et efficaces et peuvent être utilisées pour conduire des interventions précoces non coercitives, telles que les interventions dont l'objectif est d'empêcher les jeunes d'être abusés par la pensée extrémiste violente.

3- Réalisation de la transparence

Les normes quantitatives fournissent une mesure de la transparence technique et l'échange de normes quantitatives peut accroître la confiance et créer les conditions d'un meilleur échange d'informations entre les acteurs et les agences internationales. Il est également important de renforcer la transparence du cadre juridique supportant l'analyse prédictive en vue d'améliorer les performances des modèles et de parvenir à une compréhension claire et cohérente de la nature de l'analyse et de sa viabilité.

L'augmentation de la disponibilité des données peut entraîner une corrosion des normes actuelles relatives à la confirmation des charges. Les performances offertes par la capacité de collecter des données et les utiliser dans la prévision conduiront à un plus grand intérêt pour les opérations préventives et proactives, et à sanctionner avant que le crime ne se produise.

La centralisation de la responsabilité de supervision de cette analyse et la collaboration avec les agences gouvernementales améliorent la capacité de parvenir à une compréhension claire de l'analyse, de même que la mise à disposition de ces informations renforce la surveillance et permet de traiter les injustices liées à la discrimination. A titre d'exemple: les procédures d'arrestation à l'aéroport ont été élaborées selon un modèle qui combine des schémas de voyage suspects, des motifs inhabituels et des signes physiologiques d'inconfort, ce qui a entraîné une diminution de 50% du nombre total de personnes faisant l'objet de fouilles. La connaissance par les voyageurs de ces mesures réduira leurs inquiétudes quant au fait que ces procédures soient basées sur des préjugés raciaux ou ethniques. Le partage de critères quantitatifs peut créer les meilleures conditions pour l'échange d'informations entre les acteurs et les agences internationales. Ainsi, les fournisseurs de services de télécommunications seraient plus disposés à accepter les demandes d'accès à leurs données s'ils se rendent compte que les normes de ces requêtes sont élevées et qu'elles poursuivent un objectif légitime et réalisent de bons résultats.

2. Risques:

1- Précision limitée de la prédiction

Prédire les attaques terroristes et traiter l'extrémisme en utilisant uniquement des procédures mathématiques peut s'avérer inexact. Par conséquent, il faudrait proposer les procédures, les essayer et les évaluer en premier lieu, voire s'en débarrasser si elles n'atteignent pas une valeur prédictive suffisante. Il existe de nombreux exemples d'intelligence artificielle utilisés avec succès dans l'industrie et qui ont permis d'améliorer les capacités de prédiction à l'aide de l'apprentissage automatique et de l'adaptation dynamique, en plus de l'adaptation aux changements de données au sein du système, l'imposition de normes de validation avant l'utilisation et la mise à jour progressive. Ces mesures constituent la condition préalable sine qua non à l'utilisation coordonnée de l'intelligence artificielle dans la lutte contre le terrorisme, tout en sachant que les résultats de tout système prédictif n'offrent qu'une éventualité et non des preuves.

2- Effets sociétaux de la surveillance

L'analyse automatisée des données réduit souvent l'intrusion dans la vie privée au niveau individuel, mais augmente la probabilité que tout le monde se sente surveillé à tout moment. Nombre d'universitaires ont étudié la manière dont la surveillance numérique peut susciter la crainte généralisée de traiter avec les questions et les activités politiques, d'exprimer une opinion dissidente, de critiquer des idées ou d'être en désaccord avec les normes en vigueur. Cette question a été une source de préoccupation pour les groupes de la société civile, en particulier après la divulgation des détails du programme d'espionnage (PRISM) en 2013 par Edward Joseph Snowden, un contractant de la CIA, qui a dévoilé la taille des programmes nationaux de surveillance aux EU. L'expérience historique du comportement

des citoyens sous des régimes autoritaires fournit des preuves convaincantes des résultats effrayants de la surveillance de masse. D'un autre côté, il y a ceux qui pensent que la poursuite de l'opposition politique, de la liberté d'expression et l'augmentation de l'échange volontaire d'informations via les médias sociaux, prouvent que l'on exagère les effets négatifs de ce contrôle.

L'utilisation des capacités d'intelligence artificielle à des fins prédictives dans la lutte contre le terrorisme n'est ni bonne ni mauvaise en soi, mais dépend plutôt de la façon dont ces capacités sont utilisées.

3- Corrosion des normes de preuve

Il existe des avertissements selon lesquels une augmentation de la disponibilité des données peut entraîner la corrosion des normes actuelles relatives à la confirmation des charges, car les possibilités offertes par la capacité de collecter et d'utiliser des données dans les prévisions conduiront à un plus grand intérêt pour les opérations préventives et proactives plus qu'auparavant. Ces nouvelles technologies prédictives permettront aux autorités de punir l'accusé avant qu'il ne commette son crime! Et c'est alors qu'apparaît le fantôme du (pré-crime), qui ne peut être évité qu'en reconnaissant que tout modèle prédictif est une éventualité et non une preuve, et que l'intervention sur la base de ces modèles doit être du ressort de la décision humaine prise par un expert fin connaisseur des limites et des capacités de ces modèles.

4- Généraliser l'utilisation de l'intelligence artificielle dans les délits

Il existe des antécédents dans lesquels ont été utilisés les systèmes d'intelligence artificielle destinés à combattre le terrorisme dans la lutte contre d'autres crimes, comme ce fut la cas auprès de la police de New York qui a combiné 3000 caméras de télévision en circuit fermé avec d'autres capteurs. Certes, la disponibilité d'un grand nombre de données publiques est un trésor inestimable pour les responsables chargés d'enquêter sur les crimes ou intéressés par les interventions sociales.

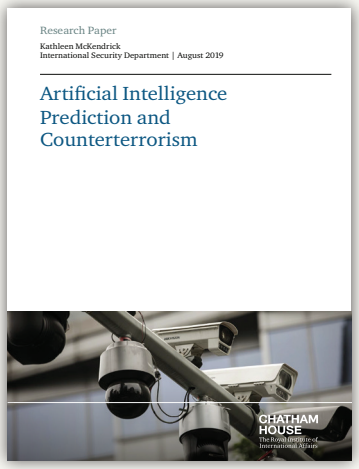
5- Utilisation abusive de l'intelligence artificielle

Même en réglementant l'utilisation de l'intelligence artificielle pour lutter contre le terrorisme et en imposant des restrictions à cette utilisation, l'interprétation des résultats reste purement personnelle, ce qui fait craindre que le terme (terroriste) ne soit utilisé à des fins politiques. Autoriser la collecte et l'analyse de données publiques comporte un risque potentiel d'utilisation abusive. Les limites et les contrôles imposés à l'utilisation de l'intelligence artificielle dans l'analyse des données sont atténués par le manque de compréhension générale de la quantité de données créées et de la façon dont elles sont utilisées.

Auteur

Kathleen McKendrick, officier de l'armée britannique, a servi en Irak et en Afghanistan et a donné des cours de formation, d'éducation et de lutte contre le terrorisme au Centre d'excellence pour la défense contre le terrorisme (COE-DAT) relevant de l'Organisation du Traité de l'Atlantique Nord (OTAN) à Ankara, en Turquie. En 2017 et 2018, elle a travaillé comme chargée de recherche au Département de la Sécurité Internationale au Royal Institute of International Affairs (Chatham House).

Elle a un BA en génie des systèmes aériens de l'Université de Cranfield et une maîtrise en Relations Internationales de la London School of Economics and Political Science. Ses intérêts de recherche comprennent: La défense, la sécurité et l'application de l'intelligence artificielle aux opérations militaires.




التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION

Département Général de la
Planification et de la Coordination