REVISIONS

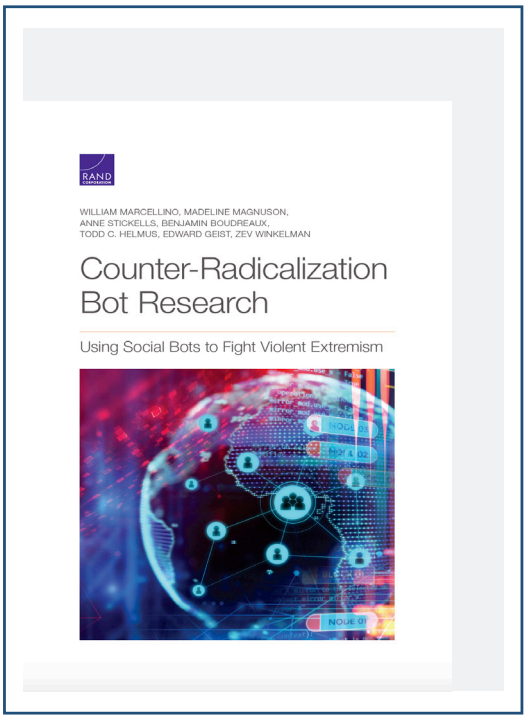
2021

التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

RAPPORTS INTERNATIONAUX

RECHERCHES SUR LES BOTS DE LUTTE CONTRE LA RADICALISATION

RECOURS AUX «BOTS» POUR LUTTER CONTRE L'EXTRÉMISME VIOLENT



Numéro
27

juillet

www.imctc.org

Rapports Internationaux

Une publication mensuelle de la Coalition Islamique Militaire pour Combattre le Terrorisme

Superviseur général

Le Major Général Mohammed bin Saïd Al-Mughaidi

Secrétaire Général de la Coalition Islamique Militaire pour Combattre le Terrorisme en charge

Rédacteur en chef

Ashour Ibrahim Aljuhani

Directeur du Département d'Études et des Recherches

Remarque: Les idées exprimées dans ce rapport représentent l'opinion de ses auteurs et pas nécessairement l'opinion de la CIMCT.

Conception, réalisation et édition

Société Taoq pour la Recherche et les Médias

TAOQ تـــوق

Courriel: info@taoqresearch.org

Téléphone: +966 114890124

Recherches sur les BOTS de lutte contre la radicalisation

Recours aux «BOTS» pour lutter contre l'extrémisme violent

Le rapport «Recherches sur les BOTS de lutte contre la radicalisation: Recours aux «bots» pour lutter contre l'extrémisme violent» a été publié par la RAND Corporation et préparé par William Marcellino, Madeline Magnuson, Anne Stickells, Benjamin Bourdeaux, Todd C. Helmus, Edward Geist, et Zev Winkelman. Il traite des programmes de robots Internet connus sous le nom de bots et évalue la possibilité pour le gouvernement américain de les employer dans la lutte contre l'extrémisme et le terrorisme.

Le rapport se compose de **cinq sections :** une introduction sur la technologie des bots, l'état actuel de son utilisation dans divers domaines, les questions éthiques et juridiques liées à son utilisation, le développement de concepts d'utilisation de bots, et enfin les recommandations soumises au gouvernement américain. Le rapport s'appuie sur plusieurs réunions avec des experts spécialisés, en plus de l'examen de la littérature juridique et éthique disponible, des cas d'utilisation antérieurs de cette technologie et de son impact sur les individus, la collecte de données et les campagnes de messages, tout en focalisant sur les groupes terroristes d'Al-Qaïda et de l'Etat islamique et les autres groupes similaires.

Types de robots

Les robots Internet sont des logiciels électroniques téléchargés sur des plates-formes de médias sociaux. Ils fonctionnent de manière autonome usant des techniques d'intelligence artificielle, de perception sociale et de capacités linguistiques. Ils visent diverses fins comme d'influencer les usagers, leur fournir des informations sur le sujet pris en charge par le bot, les leurrer sur un éventuel soutien important, leur faire du tapage électronique pour embrouiller un problème, les distraire et les diriger dans la mauvaise direction, en leur donnant des informations ou des données alternatives.

Les robots peuvent directement induire en erreur, créer des messages et de faux «récits», connecter des usagers ayant des attitudes, des opinions et des intérêts similaires et harceler les usagers pour les éloigner de l'arène des médias sociaux, créer des amitiés avec eux pour accéder aux données ciblées ou les persuader que le logiciel est un être humain en vue de les empêcher de communiquer avec un vrai utilisateur.

Des groupes extrémistes tels que Daech et des organisations de droite en Occident ont utilisé cette technologie pour diffuser leurs idées dans le cyberespace, recruter de nouveaux membres et élargir leur soutien. Le recours à cette technologie pour limiter l'influence de ces groupes est devenu une nécessité pour les autorités compétentes de lutte contre la conversion au fondamentalisme et à l'extrémisme violent. Cependant, les résultats de cet usage dépendent de plusieurs facteurs inhibants techniques, juridiques et éthiques.

L'utilisation de robots Internet ou de robots sociaux a débuté à un stade précoce du développement d'Internet, dans les années 1980 et 1990 à des fins limitées, telles que la gestion de jeux et de salles de discussion. Certains gouvernements, armées et politiciens ont eu recours aux robots pour duper l'opinion publique et diriger les discussions de leur cours normal sur diverses plateformes de médias sociaux. Twitter a admis qu'environ 23 millions de ses comptes ne sont que des «bots» et Facebook a indiqué qu'en un an les faux comptes représentaient 5 à 6% du total des comptes.

L'émergence de médias sociaux tels que Facebook et Twitter, et leur fusion avec l'intelligence artificielle et les technologies d'apprentissage automatique, ont conduit à la révolution actuelle dans le monde de la communication. L'impact de cette communication s'est accru dans divers domaines, tels que la politique et l'économie. Les effets les plus dangereux résident dans leur exploitation par les groupes extrémistes violents à des fins de propagande, de recrutement et d'influence. Des groupes comme Daech ciblent les partisans de leurs idéologies, à travers les conversations et les lettres ouvertes, avant de les regrouper dans des cellules secrètes et de les recruter.

Bots sécurisés

Les plates-formes de médias sociaux offrent aux développeurs de bots via les interfaces de programmation d'application (API) la possibilité d'exploiter le potentiel de ces plates-formes. Cela conduit de nombreux annonceurs commerciaux à utiliser, à des fins commerciales, sans violer les conditions d'utilisation de ces plateformes, les bots connus sous le nom de robots sécurisés qui ne prétendent pas être de vrais utilisateurs.

Début 2018, ces plateformes ont entamé un processus de nettoyage pour expulser des «bots» prétendant être de vrais utilisateurs, ou de faux comptes, conduisant à une sorte de course aux armements entre les plateformes et les développeurs de bots. Ainsi, Facebook peut activer son propre système de protection, basé sur des techniques d'apprentissage automatique pour examiner le plus grand nombre de comptes et boquer les bots.

Une étude publiée par l'Université de Colombie-Britannique a indiqué que «Facebook» n'a bloqué que 20% des robots signalés par les utilisateurs. Twitter a réussi à réduire l'impact des bots notamment ceux envoyés de Russie pour provoquer du cyber-tapage lors des élections de 2011. Les développeurs de robots ont pu surmonter la technique liant les comptes à l'âge de l'utilisateur pour connaitre ce dernier, et ce en achetant des comptes réels, ce qui a conduit au développement d'une technologie permettant de découvrir le comportement social des comptes.

Les chercheurs concluent que la plupart des robots actuellement utilisés, avec leurs diverses fonctions et méthodes, ont un impact négatif sur le cyberespace, et que peu servent à créer un impact positif, ce qui constitue une exception par rapport aux robots chargés de la vente de biens, du vol d'informations personnelles ou de la propagande. Le développement dans le domaine de l'intelligence artificielle peut conduire à la construction de robots plus sophistiqués

qui contribuent au bien général des sociétés, et au développement de diverses technologies, telles que la reconnaissance vocale de haute précision et la génération et la compréhension du langage naturel, de sorte que les robots soient capables de tenir une conversation avec un humain, et comprendre tous ses mots et leurs connotations.

Cependant, le défi à cet égard est l'incapacité des technologies d'apprentissage automatique disponibles à participer à de telles conversations dans le monde réel sans se passer de l'apport des données. Pour compenser ce déficit, les chercheurs suggèrent d'adopter la planification automatisée pour mettre à jour la rhétorique que les robots utilisent en vue de contrer les programmes de messagerie utilisés par les adversaires. Ce processus peut devenir un cyber-modèle qui développe une stratégie discursive en analysant les discours sur Internet. Certains chercheurs pensent que les capacités actuelles de l'intelligence artificielle peuvent évoluer vers un apprentissage en profondeur, ce qui rend le facteur humain sans importance. Cependant, le grand écart dans la «littérature» des questions d'intelligence artificielle et de ses applications montre le besoin urgent de plus d'efforts de recherche capables de réaliser un changement dans la production et la compréhension du langage naturel.

Carte d'usage

Le rapport traite de la situation actuelle de l'utilisation des robots, avec leurs différentes fonctions, dans divers domaines, allant de la santé à l'utilisation politique. Il existe des cas réussis d'utilisation de bots dans le domaine de la santé pour réaliser les fonctions émotionnelles nécessaires au suivi des cas de patients. Certains sont tripartites, impliquant le bot, le patient et les thérapeutes spécialisés, tels que: «Melody Bot» et «Babylon Bot», qui collectent des informations auprès des patients et recommandent aux thérapeutes de prendre des mesures. Les performances positives de ces robots peuvent être attribuées au facteur humain, au champ d'expertise limité requis pour activer ces robots et à l'environnement contrôlé dans lequel ils agissent.

Quant aux **«Robots d'interview»**, ils connectent des utilisateurs qui ne peuvent pas se connaître directement. Ainsi, le **Bot Sensai** connecte les utilisateurs qui ont besoin d'un bien ou d'un service. Le laboratoire multimédia du Massachusetts Institute of Technology a également développé ce que l'on appelle un «coco bot» pour connecter directement les personnes présentant des symptômes similaires d'anxiété et de dépression.

Les bots créent des liaisons entre les usagers à travers les mots spécifiques dans leurs historiques de discussion. Une expérience a montré que les

utilisateurs de programmes de messagerie sont plus enclins à suivre les comptes de célébrités, ou de ceux appartenant à leur groupe ethnique ou social. D'autres expériences ont montré que le sexe sur lequel le bot façonne sa personnalité affecte les utilisateurs. Les facteurs liés à la taille, fréquence et moyens de générer les tweets et ciblage du groupe spécifique d'utilisateurs influencent également le succès du bot.

D'autres bots appelés **«Bots de récolte»** fonctionnent de manière simple et collectent des informations sur les usagers. Sur Facebook, par exemple, des demandes d'amitié sont envoyées aux utilisateurs, et lorsque les demandes sont acceptées, les bots collectent toutes les actualités, publications, alertes et avis disponibles dans les profils des utilisateurs. Ces robots utilisent souvent des portraits de belles femmes séduisantes. L'OTAN a surnommé ces robots «bikini trolls» ou **«bots de plaisir».**

Le comportement du bot est entièrement contrôlé par le facteur humain, et le bot peut aller au-delà de la collecte de données pour avoir des conversations privées avec l'utilisateur, et le pousser à participer à certaines activités de commerce illégal par exemple, détruire son système d'exploitation ou l'infecter par des logiciels malveillants. En 2011, une équipe de recherche de l'Université de la Colombie-Britannique a pu en deux mois utiliser 102 comptes Troll sur Facebook et extraire en un temps record 250 gigaoctets de données provenant de plus de 3000 utilisateurs.

Certaines expériences ont prouvé leur incapacité à traiter avec les utilisateurs, tel le **«Chatbot»** de Microsoft, connu sous le nom de «bot Tay», dont l'échec a même eu des impacts à contrario. Le logiciel lancé en 2016 a été décrit par l'entreprise comme un programme d'apprentissage automatique qui analyse les modèles d'interaction dans les messages entre les utilisateurs. Cependant, le programme a vite développé un langage raciste, ce qui a conduit à sa suspension un jour après son lancement sur Twitter. En revanche, le logiciel d'intelligence artificielle connu sous le nom de «Xiaoice» lancé par Microsoft sur la plate-forme chinoise WeChat, a gagné en popularité et a été ajouté à un million et demi de groupes de discussion. Il a eu des conversations avec dix millions d'utilisateurs sans provoquer aucune réaction négative.

La différence entre les performances des deux logiciels, c'est que «Tay» a été lancé sur la plate-forme publique Twitter, alors que «Xiaoice» a été lancé sur une plate-forme de conversation privée, mais le contexte social politique diffère beaucoup. Les internautes de Twitter (couramment utilisés aux États-Unis et en Occident) ont tendance à utiliser un langage acerbe, voire offensant, mais en Chine, la censure stricte du contenu par le gouvernement incite les utilisateurs à l'autocensure du contenu et de la langue utilisée.

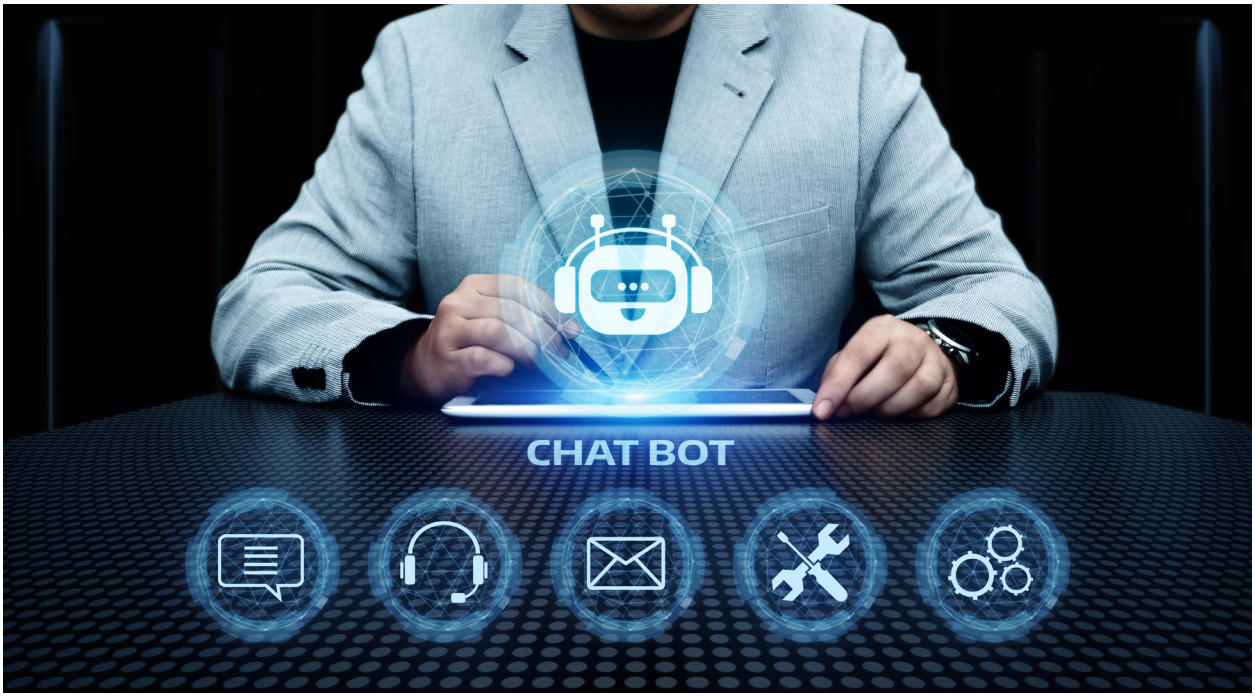
Certains robots sont utilisés pour diffuser des informations, tromper le public ou corriger une vision spécifique. Ils agissent via un réseau, ce qui leur confère un pouvoir considérable. Ce type de robots qui se confond aux trolls a été utilisé par la Russie pour influencer les choix des électeurs américains aux élections de 2016.

Les astroturf bots sont utilisés par ceux qui paient pour gagner en popularité. La campagne du politicien «Mitt Romney» a été accusée lors des élections américaines de 2012 d'avoir acheté des adeptes à l'aide de ce bot. Les partis politiques mexicains ont employé avec succès les robots aux élections de 2012, en raison des restrictions médiatiques notamment sur les questions de commerce de drogue, ce qui a conduit à une guerre féroce menée par la campagne du candidat du parti présidentiel Peña contre ses concurrents, et le bot connu sous le nom de (Peñabot) a pu influencer les médias sociaux et l'opposition et créé des hashtags qui ont gagné en popularité et polarisé les discussions.

Mesure de la maturité

Le rapport révèle que la technologie des bots a récemment évolué de manière significative du point de vue des fonctions, des types et des compétences. Il fournit un modèle pour mesurer la maturité et les capacités de développement du bot, et comparer son utilité pratique actuelle avec la perspective de son développement futur. Ce modèle consiste à mesurer la capacité du bot sur ce qui suit:

- **Conscience:** la capacité du bot à trouver, stocker et interpréter un contenu minimal. Le développement de cette capacité signifie qu'à l'avenir, le robot sera capable de traiter le langage humain naturel, et développer sa compréhension des modèles du discours humain, en faisant la différences entre les connotations précises des mots, et peut-être même leurs significations métaphoriques.
- **Décision:** c'est-à-dire la capacité du bot à classer le contenu et les données dans des catégories significatives, ce qui facilite le processus de prise de décision automatique concernant ces données. Bien que cette capacité ait largement mûri, l'apprentissage



automatique rencontre toujours diverses erreurs causées par la mauvaise classification, ce qui appelle à la prudence en donnant aux robots la pleine confiance dans la prise de décisions. De nombreux entretiens avec les chercheurs sur la poursuite des conflits à l'avenir prédisent le développement de la capacité des gouvernements à détecter les bots et la capacité des gestionnaires de bots à se cacher. Le facteur humain est une partie vitale de ce conflit. L'appareil cybernétique de Daech a tenté de corrompre un employé des entreprises chargées d'empêcher les trolls et les robots de l'EI à créer des comptes sur Twitter.

- **Action:** c'est la capacité du logiciel à effectuer des actions humaines dans le monde réel ou virtuel, comme d'envoyer une demande d'amitié ou répondre à un commentaire. La technologie des robots a beaucoup évolué dans ce sens, mais ces logiciels ne pourront pas mener de longues discussions avec l'utilisateur humain sans soulever de doutes, ce qui confirme la nécessité pour le manager humain de continuer à surveiller leurs performances, et d'intervenir autant que possible. Les chercheurs s'attendent à ce que la prochaine génération de robots dépasse la manipulation des messageries pour se tourner vers la manipulation vidéo et audio. Des chercheurs de l'Université de Washington ont pu traiter et fusionner certains clips et placer des mots sur les lèvres de certaines personnes.

Risques juridiques

Les risques liés à l'utilisation des bots sont nombreux et diffèrent d'un robot à l'autre, selon son type, sa cible et son opérateur. Ces risques sont transfrontaliers. Les robots qui violent la vie privée, la confidentialité, la connectivité et la disponibilité des informations constituent une menace réelle, ce qui incite le gouvernement américain à adopter une politique pour faire face à ces dangers, et définir diverses règles pouvant être adoptées par d'autres pays. Le rapport affirme que le gouvernement américain ne recourra pas à l'utilisation de robots pour atteindre des objectifs pouvant être atteints sans les utiliser, ni à la publication d'informations spécifiques ou à se cacher derrière le masque d'une personnalité humaine. Il serait donc plus approprié pour le gouvernement américain de participer aux plates-formes de messagerie pour activer les conditions d'utilisation légalement approuvées et réduire l'impact des bots.

Parmi les dilemmes juridiques notons ce qui suit:

- **La clause de (liberté d'expression) du premier amendement** de la Constitution prévoit de garantir la liberté d'expression et d'empêcher le gouvernement d'y interférer. Cette liberté s'étend à l'expression politique sans inclure les discours incitant à la haine et à la violence envers les minorités ou les personnes spécifiques. En raison du flou des frontières entre les deux contenus, le contenu diffusé par l'organisation terroriste Daech, telles les scènes violentes et sanglantes, peut être

considéré dans les limites de la liberté d'expression politique. Puisque certains contenus sont protégés, le gouvernement américain doit suivre les procédures légales pour les traiter, telles que l'émission d'une ordonnance du tribunal. De même, si le gouvernement souhaite utiliser des robots pour supprimer certains contenus, il devra suivre les mêmes procédures.

Cependant, le gouvernement oblige les plateformes numériques à supprimer certains contenus, car les conditions d'utilisation sur ces plateformes interdisent souvent la promotion de la propagande terroriste, même si elles sont soumises à la liberté d'expression, et ces conditions permettent aux utilisateurs de signaler un tel contenu pour le supprimer. Le gouvernement britannique a mis en place une unité de référence pour lutter contre l'extrémisme qui a réussi à supprimer 2000 articles par semaine. L'Union européenne a suivi son exemple en 2015, et a réussi à traiter plus de 11000 messages.

● **La clause (de fondation)** du premier amendement: stipule que **le gouvernement américain n'a pas le droit de suivre une politique discriminatoire envers les religions.** Ce paragraphe peut soulever des questions lorsque le gouvernement choisit d'utiliser des bots pour cibler les adeptes d'une religion particulière. Ces risques comprennent les bots d'influence, de récolte, de dissimulation et de harcèlement. La responsabilité légale s'applique si la conception et l'utilisation de robots ciblent un groupe religieux particulier ou des mots spécifiques. Pour éviter ces risques, il est possible de cibler les personnes vivant à l'étranger qui n'agiront probablement pas contre le gouvernement américain. Cependant, les développeurs doivent faire attention aux mots-clés ciblés, de crainte qu'ils ne soient étroitement liés à une religion particulière.

● **Renseignements et application de la loi:** certains robots peuvent être importants pour les opérations d'application de la loi et de renseignements, en particulier les «robots de récolte». Leur tentative d'accéder à des informations inaccessibles au public les soumet à des restrictions juridiques, notamment les lois de confidentialité et la confidentialité des communications électroniques, le supplément sur les lois applicables, la loi sur le stockage des communications, la loi sur le contrôle externe des renseignements, etc.

L'entité qui emploie des robots pour collecter des informations ou pour des opérations de renseignement doit veiller à ce qu'aucune violation de ces lois ne soit commise.

● **La loi Smith-Mont:** sur l'éducation et l'échange d'informations de 1948, autorise le gouvernement américain ou le Conseil de Diffusion des Gouverneurs à organiser des campagnes pour influencer l'opinion publique à l'étranger, mais elle impose des restrictions à ces campagnes dans le pays. Le recours aux robots dans ces campagnes nécessite de revoir la loi et de vérifier le public cible de ces campagnes.

Restrictions éthiques

Le rapport mentionne nombre de restrictions éthiques qui diffèrent des restrictions légales, mais qui manquent de moyens de mise en œuvre. Lorsqu'il mène des opérations de lutte contre l'extrémisme violent ou le terrorisme, le gouvernement américain s'appuie sur les plateformes de médias sociaux appartenant à des entreprises privées. Ces entreprises ont leurs propres intérêts qui peuvent ne pas correspondre aux intérêts et aux objectifs du gouvernement. L'utilisation de bots sur ces plateformes peut porter atteinte à leur neutralité, et les conditions d'utilisation diffèrent d'une plateforme à l'autre. Les chercheurs soulignent la nécessité de prendre en compte ces facteurs afin que ces entreprises, qui représentent une part importante de l'économie nationale, ne soient pas lésées.

Les entretiens menés par les chercheurs confirment que la transparence est une exigence éthique et pratique lors de l'activation des robots, car de nombreux Américains et d'autres ne s'attendent pas à ce que le gouvernement américain utilise des robots et d'autres techniques de communication pour atteindre des objectifs politiques ou faire de la propagande. L'utilisation abusive et la manipulation d'informations ou la désinformation intentionnelle peuvent nuire à la réputation du gouvernement et conduire à une baisse de confiance dansl'Internet en tant qu'espace sûr pour l'échange d'informations, ce qui aura des conséquences économiques, commerciales et politiques pour la politique américaine qui soutient la promotion d'espaces sûrs sur Internet. Par conséquent, les chercheurs demandent au gouvernement américain de publier une déclaration générale de principes expliquant le type de bots utilisés par le gouvernement américain et les différentes manières dont il les utilise, pour que public comprennen ce que fait le gouvernement.

Les risques éthiques liés à l'utilisation des robots varient d'une institution à l'autre. Le Département d'État assume de nombreuses responsabilités qui vont au-delà de la lutte contre l'extrémisme et le terroriste pour

promouvoir les intérêts économiques, soutenir la liberté d'Internet et les droits de l'homme dans le monde. Son recours aux robots peut porter atteinte aux intérêts des États-Unis. Quant aux institutions ayant des fonctions étroites ou non consultatives, comme le Département de la Sécurité intérieure, les risques sont moindres.

Développement et évaluation

Après avoir clarifié l'importance et la possibilité pour le gouvernement américain d'utiliser des robots dans la lutte contre l'extrémisme violent et le terrorisme, le rapport traite du développement réel de robots pour combattre les groupes terroristes tels que Daech et leurs concepts et fondements généraux. Il indique que **les critères d'évaluation de ces concepts** sont les suivants:

1. **La faisabilité technique du bot** et ses capacités interactives qui le rendent utilisable.
2. **Les risques pour les usagers de bots**, dont les risques sociaux et matériels, et les risques pour la vie privée.
3. **Les risques potentiels pour les développeurs de robots,** qui sont les risques d'exposition, et les problèmes juridiques.
4. **L'ampleur de l'impact,** comme la capacité d'interagir avec le plus grand nombre du public d'utilisateurs et la qualité de l'interaction.
5. **L'interconnexion ou la complexité,** qui inclut la capacité de coordonner l'interaction, la synchronisation et le fonctionnement avec d'autres logiciels.

À partir de ces critères, les chercheurs extraient onze facteurs sous forme de questions pour déterminer le type de processus de recours au bot, tels que: Qui est en charge du processus d'emploi? Où peut-il être utilisé? Quelle stratégie de communication le bot utilisera-t-il? Et quand un bot peut-il être activé? Comment fonctionnent les bots? Et à quel niveau de fonctionnement le bot peut-il être détecté?

Les chercheurs soulignent la possibilité d'utiliser l'intelligence artificielle et l'apprentissage profond pour améliorer le processus d'évaluation, car certains robots reposent sur la gestion humaine, et certains logiciels basés sur l'utilisation de l'intelligence artificielle et l'apprentissage profond jouissent d'indépendance totale grâce à leurs fonctions de calcul appelées algorithmes.

Les programmes qui reposent sur l'intelligence artificielle permettent d'obtenir des idées et des opinions que l'œil humain est parfois incapable de distinguer, ce qui permet d'améliorer la capacité de l'agent humain à garder l'anonymat et à s'engager dans des interactions directes avec les utilisateurs, voire à améliorer la furtivité du bot.

Le recours à l'intelligence artificielle comprend de nombreux risques. Les programmes peuvent agir loin du texte auquel ils sont assignés, s'impliquer dans des abus éthiques ou juridiques, ou agir de manière inattendue, devenant ainsi vulnérables à l'exposition. Et selon la recommandation d'un bot technologue, il est impératif que ces logiciels agissent sous contrôle humain, de crainte que de programmes sensés combattre l'intégrisme, ne finissent par se convertir en programmes fondamentalistes.

Sur la base de cette évaluation, les chercheurs concluent que les meilleurs robots ciblant le public et diffusant les informations sont les «robots d'interview», en raison du peu de risques éthiques et juridiques auxquels ils sont confrontés et de la technologie disponible pour leur fonctionnement. Les robots qui visent à saper les réseaux extrémistes et à réduire leur influence sont des «robots détecteurs», jouissant de la faisabilité technique et de faible risque pour les développeurs et le grand public des utilisateurs de plateformes de médias sociaux. Les robots utilisés pour collecter des informations confidentielles sont des «robots de récolte», plus performants que les robots conçus pour la chasse.

Le rapport présente un modèle de concept de recours au robot d'interview qui fournit des ressources adéquates aux citoyens menacés de fondamentalisme. Ce bot transparent interagit avec les utilisateurs sous la gestion d'un responsable humain qui cherche à minimiser les risques pour les développeurs et le public utilisant les plateformes de médias sociaux. Les utilisateurs sont des adultes qui ne sont pas citoyens des États-Unis.

Recommandations et suggestions

Les chercheurs ont consacré la dernière section du rapport à présenter nombre de recommandations aux autorités compétentes du gouvernement américain, sur le développement de bots, l'activation de leur utilisation et la résolution des problèmes éthiques et juridiques qui y sont liés lors de la lutte contre l'extrémisme. Ils ont indiqué que plusieurs problèmes qui préoccupent les institutions américaines devraient être tenus en compte lors du développement de logiciels robotiques, comme suit:

1. Bénéficier du développement commercial de la technologie des bots, suite aux progrès manifestes réalisés grâce à l'investissement dans cette industrie.
2. Développer les bots en fonction de l'environnement dans lequel ils seront employés, en tenant compte des mécanismes de la plateforme dans laquelle ils seront lancés, de la manière dont ils interagissent avec les utilisateurs et du contrôle gouvernemental sur les utilisateurs dans certains pays. Ces facteurs renforcent la confiance dans le processus et réduisent les risques pouvant survenir à la fois pour les développeurs et les usagers.
3. Prêter attention aux caractéristiques des réseaux avec lesquels les utilisateurs cherchent à interagir, telles que l'existence d'amis d'utilisateurs sur ces réseaux, d'intérêts communs ou de communication sociale intense en eux.

Les chercheurs suggèrent au gouvernement américain plusieurs étapes pour **réduire les risques législatifs et éthiques pouvant résulter de l'utilisation de robots**, dont:

I. Eviter la normalisation des actions et des comportements des gouvernements pouvant menacer la cybersécurité, en interférant avec la confidentialité ou l'intégrité des informations sur Internet et leur disponibilité.

II. Prendre en compte les questions liées aux côtés juridiques en limitant le nombre de bots utilisés à l'étranger, tout en évitant de cibler les utilisateurs d'une secte religieuse particulière, et en usant de pare-feu, si possible, entre les logiciels de bots et les agences de renseignement, les forces de l'ordre et les partenaires internationaux.

III. La nécessité d'obtenir l'autorisation des entreprises avant d'utiliser des robots sur les plateformes de médias sociaux.

IV. Le besoin de transparence autant que possible dans l'utilisation des bots par le gouvernement des États-Unis, tout en gardant certaines limites pour éviter les mauvaises conséquences.

V. La nécessité de faire une révision juridique des bots utilisés en coopération interne entre les institutions, de développer leurs principes de fonctionnement et de créer un registre pour cela.

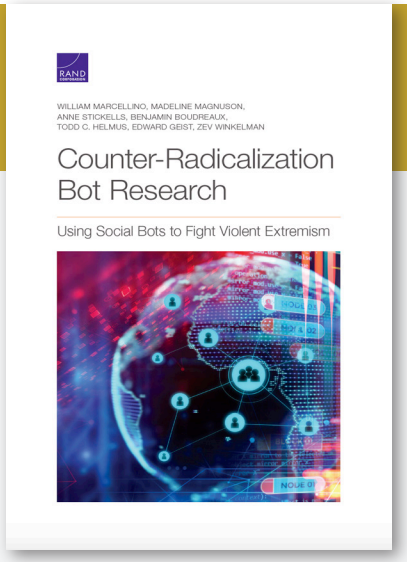
Conclusion du rapport

Les chercheurs concluent le rapport en affirmant que les robots constituent un outil pratique de lutte contre l'extrémisme violent et le terrorisme, mais que leur utilisation est limitée par de nombreux facteurs juridiques, éthiques et pratiques, ce qui nécessite toujours la présence de l'élément humain. Les décideurs devraient peser les avantages escomptés de l'emploi de tels logiciels avec les risques inhérents aux programmes automatiques. Le gouvernement américain devra

également promouvoir les technologies de détection des bots pour dissuader les adversaires de lancer des campagnes trompeuses et diffuser des informations mensongères via les bots, tout en tenant compte du contexte culturel et social lors de la création de bots.

Le rapport examine l'un des grands développements dans le monde des cyber-technologies, à savoir les robots, et évalue leur utilisation potentielle dans la lutte contre l'extrémisme violent et le terrorisme. Il discute les restrictions juridiques et éthiques à prendre en compte lorsque les gouvernements les utilisent pour lutter contre les opérations extrémistes. Cependant, le rapport se caractérise par la prédominance de l'aspect technique, ayant empêché de détailler la façon dont les bots sont utilisés dans la lutte contre l'extrémisme et le terrorisme, en particulier sur Internet, de même que le rapport comprend peu de références sur la manière dont les organisations extrémistes et terroristes utilisent les différents bots.

Le rapport indique que les organisations terroristes telles qu'Al-Qaïda et Daech utilisent des robots et d'autres techniques de recrutement et de propagande, sans fournir d'exemples, de statistiques ou de mesure du succès de ces opérations, ni leur sort après le déclin des deux organisations au Moyen-Orient en particulier. Le rapport apparaît ainsi déséquilibré, mais il demeure utile pour les institutions impliquées dans la lutte contre l'extrémisme, à travers les détails donnés sur cette lutte avec ses aspects complexes, politique, sécuritaire, économique et culturel.



RECHERCHES SUR LES BOTS DE LUTTE CONTRE LA RADICALISATION

RECOURS AUX «BOTS» POUR LUTTER CONTRE L'EXTRÉMISME VIOLENT

Éditeur

RAND 2020


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

التحالف الإسلامي العسكري لمحاربة الإرهاب

ISLAMIC MILITARY COUNTER TERRORISM COALITION