Recours à l'intelligence artificielle pour réduire les opérations terroristes

Techniques de suivi, d'analyse et de prévision comme « modèle »

Dr. Imran Awan

Expert en lutte contre le terrorisme et professeur de criminologie à l'Université de Birmingham, Royaume-Uni

La technologie de l'intelligence artificielle (IA) se caractérise par sa capacité à se développer et à avoir une profonde influence sur de nombreux aspects de notre vie quotidienne. Ses multiples avantages suscitent une vive concurrence entre de nombreuses parties rivales. Les terroristes peuvent en user pour réaliser leurs objectifs criminels, tout autant que les appareils de sécurité et d'application de la loi tels que la police pour prédire les futures attaques terroristes et les contrecarrer avant qu'elles ne se produisent.

Aujourd'hui, de nombreuses entreprises utilisent l'IA, tels que Microsoft, Google, Yahoo, Amazon, les banques et les établissements de cartes de crédit, en mettant en place leurs propres systèmes de sécurité. L'IA peut également être utilisée pour améliorer les performances et le processus décisionnel de nombreuses agences, dans la mesure où ses techniques prédictives contribuent à lutter contre les menaces terroristes et développer des contre-stratégies efficaces.

L'IA a créé un modèle virtuel dans lequel les individus interagissent via différents moyens de communication. Ce rapprochement a contribué à l'escalade jour après jour des menaces sécuritaires, ce qui nécessite de rechercher des formules et des solutions intelligentes pour comprendre les problèmes sociétaux difficiles et épineux.

Du point de vue sécuritaire, ces technologies modernes peuvent être utilisées pour intercepter les communications terroristes en les enregistrant, en les analysant et en les traitant grâce aux applications dites de « reconnaissance vocale ». Bien qu'elle ait collecté des millions d'échantillons vocaux pouvant être rapidement utilisés dans ces applications, la société «Nuance Communications» est confrontée au défi de pouvoir transcrire avec précision ces messages et communications grâce à l'IA. Cependant, plusieurs avantages sont recensés, notamment l'identification de mots ou d'expressions dans les applications de commandes vocales.

Étant donné que les terroristes tentent également de profiter de ces technologies, l'IA représente l'une des plus grandes menaces pour la sûreté et la sécurité de la société à travers l'histoire. Une étude récente a révélé que certaines organisations terroristes ont trouvé ce qu'elles cherchaient dans les technologies modernes et les outils d'IA, que ce soit pour la communication sûre et rapide entre leurs membres, ou entre elles et les recrues potentielles, ou pour échapper aux contrôles de sécurité, recruter des partisans et se procurer des armes, ou mener à bien leurs opérations criminelles en s'appuyant sur la technologie numérique ou sur le terrain.

Menaces terroristes

Le paysage des menaces terroristes émergentes grâce à l'IA évolue à un rythme très rapide. Le chercheur Sheldon Wright déclare dans son livre «Police et Technologie»: « La cybersécurité est devenue un problème de sécurité nationale » devant être réglé. Cela inclut la manière dont l'IA peut être introduite et utilisée pour lutter contre les menaces terroristes.

Les technologies modernes de toutes sortes jouent un rôle majeur dans la lutte contre les organisations terroristes. En même temps, la vie privée et les droits de l'homme doivent être protégés. La traque des terroristes ne doit pas être menée à l'aveuglette, car la technologie risque d'être une arme à double tranchant.

On ne peut pas dire qu'un système de sécurité soit totalement à l'abri des cyberattaques, surtout lorsqu'une organisation terroriste est capable d'installer des logiciels malveillants pour contrôler à distance les ordinateurs piratés et les connecter plus tard en vue de créer des réseaux d'ordinateurs infectés. Les organisations terroristes s'efforcent également de recruter des individus prêts à commettre toutes sortes d'atrocités et agissent pour cela en exploitant parfois les technologies fournies par l'IA pour amplifier l'impact de leur propagande et atteindre les éléments faibles, les recruter et en faire des extrémistes.

L'analyse la plus précise des informations à l'aide de techniques d'IA sur Internet doit être utilisée avec la plus grande efficacité par les autorités concernées pour intégrer différents types de données disponibles, depuis les discussions en ligne ou les sites de réseautage, jusqu'aux dossiers de police des terroristes présumés et les bases de données biométriques. Il est important que les autorités puissent coopérer afin de prévenir et d'arrêter les terroristes qui usent de l'IA. La coopération internationale et les lois internationales doivent être renforcées afin de faire face au réseau mondial de terroristes.

Il est nécessaire d'améliorer les technologies dédiées pour coordonner les réponses proactives locales et mondiales. L'établissement de partenariats entre les secteurs public et privé constitue un modèle potentiel de recours à l'IA pour faire face aux menaces terroristes. Le secteur privé paie pour surveiller Internet et analyser les données brutes, tandis que le public paie pour arrêter et poursuivre en justice les terroristes qui utilisent les services publics.

Lutte et prévention

Il existe de nombreuses tactiques proactives pouvant être utilisées pour lutter contre le terrorisme via des applications d'IA dans des opérations illusoires pour attraper les terroristes qui constituent désormais une menace réelle en raison de leur utilisation de plus en plus sophistiquée de l'Internet et des technologies modernes.

Les outils modernes de « gestion des connaissances » fournissent des mécanismes multiples et pratiques pour lutter contre les risques terroristes potentiels et croissants dus aux technologies de l'IA. Toutefois, le terrorisme ne peut être combattu efficacement à l'aide de ces technologies modernes que par le biais d'une bonne compréhension du cycle des données et des méthodes utilisées pour obtenir et diffuser l'information. Les autorités concernées doivent également coopérer entre elles pour activer de manière optimale les systèmes de gestion des connaissances et renforcer les partenariats inter-entreprises. Aux fins de l'échange d'informations logistiques complémentaires par le biais d'applications d'IA, le renforcement du processus décisionnel en matière de sécurité collective affaiblit les groupes terroristes et réduit leur danger grâce aux mesures proactives de coopération.

La police européenne chargée de l'application des lois (Europol) et la police internationale sont des exemples marquants d'échange d'informations par le biais de l'IA, car les structures des services spécialisés dans la lutte contre le terrorisme sont similaires, ce qui montre l'importance d'avoir des systèmes interconnectés de collecte de données, d'analyse d'informations et d'utilisation efficace de la technologie d'IA.

Il est peu probable que les enquêtes qui nécessitent de longues procédures formelles aboutissent. Ainsi, les services de police européens ont dû développer de nouvelles stratégies antiterroristes, basées sur l'IA et les technologies de l'information, telles les polices de proximité et de tolérance zéro et la police axée sur le renseignement et celle axée sur les problèmes.

De nombreux gouvernements ont réalisé d'importants investissements dans

l'infrastructure des technologies de l'information et des télécommunications. Compte tenu de la menace posée par le terrorisme numérique, il est aujourd'hui nécessaire d'adopter une approche plus globale pour élaborer des lois, des protocoles et des stratégies permettant de faire face aux énormes développements technologiques, aux défis associés à l'IA et au terrorisme, en plus d'établir des définitions concertées devant remplacer le langage vague et désuet utilisé dans les accords européens actuels.

En abordant les questions de l'IA et du terrorisme, l'idée d'interagir avec les communautés au niveau local pour recueillir des informations et des données sera réaffirmée. Cette approche se concentre sur le citoyen et met également l'accent sur l'utilisation maximale de la gestion des connaissances et de la police du renseignement afin de répondre aux exigences de la société dans la lutte contre le terrorisme.

Coopération conjointe

Le développement des technologies de l'information, des télécommunications et de l'IA accroît l'importance de la coopération conjointe entre de nombreuses agences pour utiliser ces technologies afin de réduire la menace terroriste. Il est nécessaire d'élaborer des programmes efficaces pour lutter contre le terrorisme et de commencer à échanger des informations en temps réel entre les agences de sécurité, les forces de l'ordre et les militaires par le biais de programmes intelligents. Les causes sous-jacentes de la radicalisation doivent être traitées selon des stratégies proactives. Le renforcement de la coopération en matière de sécurité et de cohésion communautaire est essentiel pour l'efficacité des contre-stratégies visant à dissuader les terroristes de commettre leurs crimes. Les communications inter-institutions sont également nécessaires pour que les services de sécurité puissent travailler ensemble de manière coordonnée et efficace à l'intérieur ou à l'extérieur des frontières nationales.

Les réseaux virtuels alimentés par l'IA ont le potentiel d'améliorer les interactions sociales, d'établir des relations et de fournir des systèmes de soutien pour se transformer en une société dotée d'un capital social. Mais pour comprendre l'IA liée au terrorisme, les gouvernements doivent élaborer des stratégies pratiques pour faire face à la menace imminente, avec des actions coordonnées, globales, flexibles et rapides qui abordent des réponses préventives à tous les niveaux, du local au mondial. Il existe des modèles policiers et analytiques qui peuvent être utiles lorsqu'ils sont appliqués dans des cadres reconnus et approuvés pour lutter contre

les organisations terroristes qui utilisent l'IA.

Il ne fait aucun doute que l'IA peut être utilisée pour combiner la capacité et le désir d'échanger des données entre les agences agissant en partenariat sécuritaire pour éliminer le terrorisme et atteindre et arrêter les terroristes, ce qui nécessite une plus grande coopération internationale et des législations appropriées, notamment avec l'intensification des menaces des gangs criminels, des terroristes, des pirates informatiques et des gouvernements hostiles souhaitant lancer des attaques contre les infrastructures critiques et les systèmes Internet profitant de la « mondialisation » et des systèmes de réseaux, outre les menaces du terrorisme usant de l'IA, pouvant mener à l'exclusion de certaines sociétés et à exacerber les préjugés.

En conclusion

L'IA ouvre la voie aux groupes terroristes et leur permet de mettre en œuvre leurs plans diaboliques. Avec la diffusion croissante des applications de l'IA et le développement sans précédent de technologies innovantes, ces groupes pourraient recourir aux nouvelles technologies et les exploiter à leurs fins terroristes. Il est donc impérieux de lutter contre ce phénomène grâce à des méthodes policières modernes, d'aider à faire face aux menaces terroristes et d'utiliser les technologies modernes disponibles pour contrecarrer les nouvelles menaces.

Comme le dit le chercheur Leon Hempel dans son livre «Surveillance Studies»: «Les questions de risque, de confiance, de sécurité et d'opportunité sont centrales». Il est donc important de tirer parti des nouvelles technologies pour garder une longueur d'avance sur les terroristes, comme il devrait y avoir un accord mondial sur les données collectées grâce à l'IA, comment les partager et avec qui, non seulement pour lutter contre le terrorisme, mais aussi pour protéger nos libertés et nos propres identités.