التقييم الاستراتيجي لتوظيف الذكاء الاصطناعي في الاستراتيجيات الدولية لمكافحة الإرهاب: دراسة تحليلية

أ.م.د طارق محمد ذنون الطائي *

عد الذكاء الاصطناعي احد المتغيرات المهمة في البيئة الاستراتيجية الامنية الدولية. اذ قاد الى ان يكون مجالاً رئيسا للتفاعل بين الأجهزة الأمنية الرسمية للدول والجماعات الإرهابية، و ذو مسارات متعددة. وفقاً لما تقدم، يهدف البحث إلى تقييم توظيف الذكاء الاصطناعي في استراتيجيات مكافحة الارهاب الدولية من خلال التعريف بالذكاء الاصطناعي ومديات استخدامه في المجالات الامنية، ومدعّمة بالنماذج والنظريات ذات الصلة، فضلا عن تشخيص التحديات في عملية توظيفه، والفرص التي يمكن ان يوفرها. وعلى هذا الاساس، يتجسد السؤال الرئيس في الاتي: الى أي مدى يتم توظيف الذكاء الاصطناعي في استراتيجيات مكافحة الارهاب من قبل الدول الفاعلة؟. اذ ان لكل دولة رؤيتها في عمليات توظيفه. فالولايات المتحدة تعطي الاولوية للامن القومي الأمريكي على حساب جوانب حقوق الانسان، بينما يحاول الأوروبيون الموازنة المعقدة بين المتطلبات الأمنية، وحقوق الانسان، بينما تمتلك الصين رؤيتها الخاصة المستندة الى نظامها الشمولي. كما ان توظيف الذكاء الاصطناعي يتضمن جانبين: أولهما: البعد الإيجابي المتمثل بتوفير قاعدة معلوماتية كبيرة ، ثانيهما: البعد السلبي المتمثل بحرية الوصول الى بيانات جميع الافراد. وفي الختام فان الذكاء الاصطناعي يمكن لجميع الأطراف استخدامه، فهو سيكون متاحاً لأجهزة الدولة بجميع تصنيفاتها، وفي الوقت نفسه، يكون متاحاً للحركات المتطرفة التي تستهدف خصومها.

الكلمات المفتاحية: الذكاء الاصطناعي، مكافحة الإرهاب، الولايات المتحدة وأوروبا، المعلومات، الخصوصيات الفردية.

Strategic Assessment of the employment of Artificial Intelligence in International Counter-Terrorism Strategies: An analytical study

Assist Prof Dr Tareq Mohammed Dhannoon Al Taie

Artificial intelligence is one of the key variables in the international security strategic environment, which has led to it being a major area of interaction between official state security agencies and terrorist groups, with multiple trajectories, both negative and positive. Accordingly, the research aims to evaluate the employment of artificial intelligence in international counter-terrorism strategies by defining artificial intelligence and its security, supported by relevant models and theories, as well as diagnosing the challenges of its use and the opportunities it can provide. Therefore, the central research question is: To what extent is AI employed in counter-terrorism strategies by active states? In this context, state security agencies can no longer afford to disregard AI in identifying extremist behaviour patterns before they develop into real threats. The United States prioritises American national security at the expense of human rights, while Europeans attempt a complex balance between security requirements, individual privacy, and human rights. China, on the other hand, has its own vision based on its totalitarian system, which controls the movement of society. The strategic assessment of employing artificial intelligence in combating terrorism confirms that it cannot be avoided: First, the positive aspect, it is a large information base. Second, the negative aspect, which is the freedom to access the data of all individuals. In conclusion, artificial intelligence can be used by all parties. It will be available to state agencies of all classifications and to extremist movements that target their opponents.

Keywords: Artificial intelligence, counterterrorism, United States and Europe, information, individual privacy.

** جامعة الموصل/ كلية العلوم السياسية، tareq-mohammed@uomosul.edu.iq

المقدمة

يعد الذكاء الاصطناعي ركيزة رئيسة من مرتكزات التحول في ادراك التهديدات اللامتماثلة في البيئة الاستراتيجية الامنية العالمية في القرن الحادي والعشرين. اذ لم يعد مسألةً ثانوية بالنسبة لصناع القرار في الدول، وانما بدأ يشغل مكانة مهمة ومتزايدة في الفكر الاستراتيجي لهم. كما ان عمليات التوظيف لم تعد تقتصر على البعد المدني، وانما تخطى ذلك الى البعد الأمني، فضلاً عن انه أصبح ذو تأثيرات متعددة الجوانب للفواعل التي تعمل على توظيفه سواء كانت من الدول أم الفواعل المدنية من غير الدول، ام الفواعل العسكرية من غير الدول، لا بل بدأت تداعياته السلبية تتوسع، لأنه من الصعوبة بمكان التحكم بتفاعلاته وتداعياته، رغم اختلاف إمكانيات واهداف كل فاعل، فقد قاد ذلك الى ان تكون عمليات توظيف الذكاء الاصطناعي غير محدده وواضحة المعالم.

أهمية البحث:

تكمن أهمية البحث في محاولة تقديم مقاربات محددة عن الذكاء الاصطناعي، ومديات توظيفه من قبل الدول في عمليات مكافحة الإرهاب، والعمل على تحليل البيئة الأمنية التي يعمل فيها الذكاء الاصطناعي، وتوضيح الفاعلين الذين يعملون على توظيف الذكاء الاصطناعي في خدمة اهدافهم، فضلا عن تقديم وتحديد التحديات التي تواجه عمليات توظيف الذكاء الاصطناعي في عمليات مكافحة الإرهاب، والفرص المتاحة امام الفواعل التي توظفه، والعمل على تقديم تقييم استراتيجي ورؤية شاملة حول التجارب العالمية في عمليات مكافحة الإرهاب من خلال تقديم نماذج في عمليات مكافحة الإرهاب.

إشكالية البحث:

تتجلى في تعدد الرؤى حول مديات تأثير الذكاء الاصطناعي في عمليات مكافحة الإرهاب العالمي، فهنالك من يرى بانه يؤثر بشكل كبير في الحد من الإرهاب العالمي نتيجة ما يوفره من قدرات معلوماتية قادرة على الكشف عن العمليات الإرهابية قبل وقوعها، والأخر يرى بان تأثيره محدوداً نتيجة كونه سلاح ذو حدين، وانه أداة يمكن لجميع الفواعل استخدامها، فالغلبة لمن يحسن توظيفها، ولا تتعلق بفاعل دون اخر، في هذا السياق، يحاول البحث معالجة هذه الإشكالية. من هنا يتجذر السؤال الرئيس: ما هو مدى وفاعلية توظيف الذكاء الاصطناعي في عمليات مكافحة الإرهاب؟ ووفقاً لما تقدم، تتبلور الأسئلة الفرعية في الاتي: ماهية الذكاء الاصطناعي بجانبية المدني والعسكري؟ كيف تعمل الفواعل على توظيفه في مجال الفعل ورد الفعل ضد بعضها البعض؟، ما هو التقييم الاستراتيجي الشامل لتوظيف الذكاء الاصطناعي في عمليات مكافحة الإرهاب؟، ويتفرع التساؤل الاخير الى جانبين: التحديات التي تواجه الدول في توظيف الذكاء الاصطناعي في عمليات مكافحة الإرهاب؟ والفرص المتاحة امامها لكي تكون اكثر فاعلية في مواجهة الفواعل المهددة للأمن؟.

فرضية البحث:

تكمن فرضية البحث في فكرة مفادها ان تأثير الذكاء الاصطناعي بدأ يتعاظم في مختلف مجالات الامن لاسيما في عمليات مكافحة الإرهاب العالمي، ولم يعد توظيفه يقتصر على الأجهزة الأمنية الرسمية للدول، وانما تعدى ذلك الى ان يتم توظيفه من قبل الفواعل العسكرية من غير الدول التي تمارس العنف في مختلف مناطق العالم، وعلى الرغم من التحديات التي تواجه الدول في عملية توظيفه في مواجهة التهديدات الأمنية التي تواجهها في الحروب الهجينة التي تشنها الجماعات المتطرفة، فانه قدم لمؤسسات الدول مزايا مهمة مكنتها من الكشف والتعقب وتحجيم التهديدات قبل وقوعها، لا بل قدم لها ادوات ابتكارية من خلال تغذيتها بالمعلومات اللازمة لضمان فاعلية عملياتها.

منهج البحث:

تقتضي الضرورة العلمية تبني مجموعة من المناهج العلمي بوصفها الأداة التي يمكن من خلالها معالجة الإشكالية واثبات الفرضية التي سيقت في اطار الدراسة. اذ تم الاعتماد على المنهج الوصفي لوصف الروئ الفكرية المتعلقة بالأفكار حول الذكاء الاصطناعي، ومنهج التحليل النظمي الذي يستند على المدخلات والمخرجات، بهدف مناقشة المسارات التي ستقود اليها عملية التوظيف من قبل الدول.

هيكلية البحث:

لقد حتمت الضرورة العلمية والهدف العام تقسيم الدراسة الى ثلاثة مباحث. ناقش المبحث الأول الترابط بين الذكاء الاصطناعي والإرهاب، اذ انقسم الى ثلاث مطالب، درس الاول: المدخل المفاهيمي والنظري، بينما حاول الثاني سبر غور الذكاء الاصطناعي، والتغيير في أدوات مكافحة الإرهاب. بينما درس المبحث الثاني التحليل الاستراتيجي الشامل للبيئة الامنية للذكاء الاصطناعي ومكافحة الإرهاب، والذي توزع على ثلاث مطالب، ناقش الأول جدلية العلاقة بين المعلومات والذكاء الاصطناعي، وجذر الثاني التحديات التي يفرضها الذكاء الاصطناعي في مجال مكافحة الإرهاب، بينما حاول الثالث تأصيل الفرص التي يوفرها الذكاء الاصطناعي في مجال مكافحة الإرهاب. وأخيرا حلل المبحث الثالث مآلات التوظيف الدولي للذكاء الاصطناعي في عمليات مكافحة الإرهاب، والذي توزع بدوره على مطلبين، قارب المطلب الاول النماذج الدولية في توظيف الذكاء الاصطناعي في المجالات الأمنية ومكافحة الإرهاب، بينما وضع المطلب الثاني المسارات المستقبلية لتوظيف الذكاء الاصطناعي في استراتيجيات مكافحة الإرهاب.

المبحث الأول: الترابط بين الذكاء الاصطناعي والإرهاب

يعد الذكاء الاصطناعي تحولاً استراتيجيا كبيراً في سياق الحرب على الإرهاب. فعلى الرغم من ان مكافحة الإرهاب مرت بمراحل زمنية مختلفة، وشهدت توصيفات متنوعة، وتم توظيف أدوات مختلفة لمكافحته من قبل الدول، واتخذت تلك الأدوات اشكال متعددة، فإن عمليات مكافحة الإرهاب للدول في القرن الحادي والعشرين دخلت عصر التكنومعلوماتية والذكاء الاصطناعي متعدد الابعاد والتداعيات. وعلى هذا الأساس، فان الضرورة العلمية، تقتضي تحديد مجموعة من المداخل المفاهيمية والمقاربات الفكرية التي تشكل الأساس المنطقي للتعاطي مع مكنونته.

المطلب الأول: المدخل المفاهيمي والنظري

الضرورة العلمية تقتضي مناقشة مجموعة من المفاهيم التي تمثل الأساس العلمي المنظم لعملية الايغال الفكرية في مكنونة البحث وجوهرة. وعلى هذا الأساس، يعد تعريف الإرهاب من المداخل المهمة في سياق دراسة وتحليل الذكاء الاصطناعي وعلاقته بمكافحة الإرهاب كون المجال الرئيس للدراسة.

اولاً: الترابط المعرفي بين المفاهيم

تُعرّف الأمم المتحدة الإرهاب بأنه "أعمال إجرامية تهدف أو تُحْدَث لإثارة حالة من الرعب لدى عامة الناس، أو مجموعة من الأشخاص، أو أشخاص معينين لأغراض سياسية". بينما تتجسد عمليات مكافحة الإرهاب في الآتي: الممارسات والتقنيات والاستراتيجيات المستخدمة لمكافحة الإرهاب أو منعه، بما في ذلك الجهود المبذولة لتحديد التهديدات أو الأعمال الإرهابية وردعها والتصدي لها. وتكاملاً مع ما سبق، يتم تحذير التطرف بانه: المعارضة الصريحة أو الفعلية للقيم الأساسية، بما في ذلك الديمقراطية،

وسيادة القانون، والحرية الفردية، والاحترام المتبادل والتسامح مع مختلف الأديان والمعتقدات"[1]

وتكاملاً مع ما سبق، "يتجسد الذكاء الاصطناعي في انه مجال متعدد التخصصات، يُصنف عادةً كفرع من فروع علوم الحاسوب، ويتناول النماذج والأنظمة التي تُحاكي وظائف الذكاء البشري، كالتفكير والتعلم. ومع تطور الذكاء الاصطناعي وتحسينه، تزداد قدرته على محاكاة السلوكيات البشرية المعقدة، مما يُعزز فائدته في تطبيقات الأمن والدفاع. ومن أبرز التطورات في هذا المجال الذكاء الاصطناعي التوليدي، وهو شكل من أشكال الذكاء الاصطناعي الذي يُنتج نصوصًا وصورًا وملفات صوتية وبيانات اصطناعية بناءً على المدخلات التي يقوم بها المستخدم. كما تُنتج نماذج الذكاء الاصطناعي التوليدي مخرجات إبداعية أخرى، مما يجعلها أدوات قيّمة في المجالات المتنوعة، تنتقل من إنتاج الوسائط إلى استراتيجيات مكافحة الإرهاب[2]. فضلاً عن ذلك، يشير الذكاء الاصطناعي إلى أنظمة الحاسوب القادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا، مثل الإدراك البصري، والتعرف على الكلام، واتخاذ القرارات، وترجمة اللغات"[3].

وفي هذا السياق، فان "التطورات المتسارعة في مجال الذكاء الاصطناعي تُحدث تحولاً جذرياً في جوانب عديدة من المجتمع في مختلف القطاعات. إلا أن ازدياد تطور تقنيات الذكاء الاصطناعي وسهولة الوصول إليها يُنذر بمخاطر غير مسبوقة، لا سيما عند استغلالها من قبل جهات متطرفة كالمنظمات الإرهابية. ويُشكل احتمال تعزيز الذكاء الاصطناعي لقدرات الإرهابيين تهديداً خطيراً للأمن العالمي، ما يستدعي اهتماماً عاجلاً من صانعي السياسات وخبراء الأمن والباحثين الأكاديميين على حد سواء"[4]. وهنا لابد من الإشارة بان الإرهاب يمكن ان يمارس من قبل فرد، او جماعة، او منظمة، او دولة.

ثانياً: المقاربات الفكرية والاسس النظرية

يُعدّ التصدي للتحديات التي يفرضها الإرهاب المدعوم بالذكاء الاصطناعي أمرًا بالغ الأهمية. "فكما يوضح فيلدشتاين، فان الذكاء الاصطناعي يزود الجماعات الإرهابية بأدوات فعّالة في عمليات نشر أيديولوجيتها، وتجنيد ألاتباع، والتخطيط للهجمات بسرعة عالية ونطاق واسع بشكل غير مسبوقين. اذ تتمتع أنظمة الذكاء الاصطناعي بقدرة عالية على التكيف والتوسع، ما يُتيح للجماعات الارهابية إمكانية تضخيم نطاق وتأثير الأنشطة الإرهابية، الأمر الذي يجعل تطوير تدابير مضادة فعّالة أمرًا ضروريًا. وتُفضي هذه الديناميكية إلى ظهور شكل جديد من الحرب غير المتكافئة، ويكتسب الإرهابيون فيها مزايا استراتيجية تُمكنهم من تقويض أساليب مكافحة الإرهاب التقليدية، وزعزعة موازين القوى العالمية. فضلاً عن ذلك، يُفاقم غياب الأطر القانونية الشاملة والمبادئ التوجيهية الأخلاقية التي تُنظم عمليات توظيف الذكاء الاصطناعي في الأمن القومي هذه التحديات. كما تثير عمليات عسكرة الذكاء الاصطناعي لأغراض إرهابية تساؤلات عميقة حول مستقبل الصراع وطبيعة الحرب نفسها[5]. وفي هذا السياق، اكد إيلون ماسك، مؤسس شركة تسلا، من أن الصعود الوشيك للذكاء الاصطناعي قد يكون "أكثر خطورة من الأسلحة النووية"[6].

وعلى هذا الأساس، تنطلق الأسس النظرية للبحث من المقاربات النظرية التي قدمها مجموعة من المفكرين لعل في مقدمتهم هورويتز. اذ يرى الاتي: "يُغيّر الذكاء الاصطناعي طبيعة الحرب، ويُطمس الحدود الفاصلة بين السلام والصراع، ويُنشئ ميادين جديدة للتنافس، مثل الفضاء الإلكتروني وبيئة المعلومات، وتعاظم احتمالية نشوب الحروب غير المتكافئة المدفوعة بالذكاء الاصطناعي، كما يمكن للفواعل من غير الدول أن تتحدى الهيمنة

العسكرية للدول الوطنية، مما تستلزم إعادة تقييم النماذج الأمنية القائمة للمؤسسات الامنية. ونتيجة لما تقدم من افتراضات، ونظرًا لطبيعة التحديات المتعددة الأوجه التي يفرضها الإرهاب المدعوم بالذكاء الاصطناعي، فإن اتباع المنهج الشامل والمتعدد التخصصات أمر ضروري لمعالجة هذه القضية الملحة"[7]. وبسبب التقدم التكنولوجي المتسارع، قد تكون البشرية على وشك الدخول في مرحلة حرجة من مسيرتها. وعلى الرغم من ان التقنيات التحويلية الجذرية، مثل أنظمة النانو والذكاء الاصطناعي، تتيح فرصًا ومخاطر غير مسبوقة. وقد يتحدد مستقبلنا، بل ووجودنا بكيفية تعاملنا مع هذه التحديات، تبرز الحاجة إلى فهم أعمق لديناميكيات الانتقال من مجتمع انساني إلى مجتمع "ما بعد الانسانية"[8].

المطلب الثاني: الذكاء الاصطناعي والتغيير في أدوات مكافحة الارهاب

يعد الذكاء الاصطناعي أحد أهم مظاهر التغيرات والتحولات المستمرة. ونتيجةً لذلك، "أصبح التفاعل بين الذكاء الاصطناعي والأمن الوطني موضوعاً لتقييم المخاطر والتهديدات بالنسبة للدول. ورغم عدم وجود إطار واضح ومتكامل حتى الآن، فمن الواضح أن الدول تراقب عن كثب وتُقيّم بحذر الآثار الحالية والمستقبلية للذكاء الاصطناعي. ولا يزال تأثير الذكاء الاصطناعي على القدرات العسكرية أحد أهم الشواغل المتعلقة بالأمن الوطني. اذ ترتبط الآثار المباشرة وغير المباشرة للذكاء الاصطناعي في الممارسات الأمنية التقليدية بشكل متزايد، وبالمصالح الحيوية للدول. وفي الوقت نفسه، يكتسب الذكاء الاصطناعي أهمية متزايدة في السياق الأوسع للصراعات الجيوسياسية بين الدول"[9].

وفي هذا السياق، فإن "استخدام الجماعات الإرهابية للتكنولوجيا ليس بالأمر الجديد، فقد ادت التكنولوجيا دورًا محوريًا في افعالها. ومع ذلك، ومع التطورات الأخيرة في مجال الذكاء الاصطناعي والذكاء الاصطناعي التوليدي، بدأت بعض الجماعات الإرهابية تأخذ بنظر الاعتبار "فوائد" هذه التقنيات. وتتجلى مزايا الذكاء الاصطناعي التوليدي في توظيفه لأغراض خبيثة، بدءًا من التجنيد التفاعلي وصولًا إلى تطوير الدعاية والتأثير في سلوك الأفراد عبر منصات التواصل الاجتماعي. اذ توفر التطورات التكنولوجية الحديثة آفاقًا واسعة وإمكانيات لا حصر لها، وهي إمكانيات تحاول الجماعات الإرهابية استغلالها لصالحها"[10].

كما "يُعدّ استغلال الإرهابيين لوسائل التواصل الاجتماعي حاليًا من أبرز الطرق التي يستخدمونها لتوظيف الذكاء الاصطناعي للوصول إلى الجمهور الواسع، ونشر الدعاية بهدف التطرف والتجنيد. كما تُتيح منصات التواصل الاجتماعي للمنظمات الإرهابية تنسيق هجماتها. كما إنّ إخفاء الهوية وسهولة الوصول إلى وسائل التواصل الاجتماعي تُتيحان عمليات لا مركزية بشكل اكبر، مما يُصعّب على قوات مكافحة الإرهاب رصدها. فضلاً عن ذلك، قد تُضخّم خوارزميات وسائل التواصل الاجتماعي التي تُشجّع التفاعل المحتوى المتطرف دون قصد، مما يعرض الآخرين للخطابات ذات الطابع الإرهابي. وبذلك، تُصبح وسائل التواصل الاجتماعي ساحة معركة يسعى فيها كلٌّ من الإرهابيين وقوات مكافحة الإرهاب إلى استغلال البيانات الشخصية وحمايتها. ويُبيّن ذلك الضرر المحتمل الذي تُسبّبه هذه الديناميكية من خلال الاستطلاعات والمقابلات مع منظمات الأمن القومي وإنفاذ القانون والمجتمع المدني، وذلك لفهم أفضل لكيفية إدراك مختلف الجهات الفاعلة الاجتماعية للتهديد الذي يُمثّله استخدام الإرهابيين للذكاء الاصطناعي"[11].

فضلاً عن ذلك، "تُتيح أدوات الذكاء الاصطناعي، فرصةً كبيرة لأتمتة جهود مكافحة التطرف باستخدام العديد من التقنيات التي سبق ذكرها. فعلى

سبيل المثال، من خلال عملية من مرحلتين، يُمكن للأجهزة الأمنية تدريب نماذج التعلم الآلي على منهجية مكافحة التطرف لتحديد التدخلات المعرفية التي توقف أو تعكس عملية التلقين المتطرف. وبفضل هذه المعلومات، يُمكن لنماذج التعلم الآلي تحليل الدعاية المتطرفة، وتحديد نقاط الضعف في الرسائل، ثم توليد رسائل مضادة موثوقة على نطاق واسع"[12].

المبحث الثاني: التحليل الاستراتيجي الشامل للبيئة الامنية للذكاء الاصطناعي ومكافحة الارهاب

تعد المعلومات الركيزة الأساسية في الذكاء الاصطناعي. فعلى الرغم من أهميتها الحيوية لأي تفاعل امني، فإنها بدأت تشغل مكانة مهمة في القرن الحادي والعشرين، لا بل تعاظمت مع ظهور الذكاء الاصطناعي وتعاظم فاعلية في مكافحة الإرهاب وتوظيفه في المعالجات الأمنية. من هنا فان التحليل الاستراتيجي لتعاظم تأثير الذكاء الاصطناعي في البيئة الاستراتيجية الأمنية ولاسيما مكافحة الإرهاب، يحتم تقسيم المبحث وفق المطالب الاتية:

المطلب الأول: جدلية العلاقة بين المعلومات والذكاء الاصطناعي في مجال مكافحة الارهاب

يمكن وصف تطبيق التحليلات التنبؤية لمكافحة الإرهاب، بأنه "الهدف المنشود" لقوات الأمن، إذ يمكّنها من تجاوز النهج التقليدي القائم على رد الفعل تجاه الإرهاب، والتحول إلى نهج استباقي، وذلك من خلال توقع الأنشطة الإرهابية المستقبلية والتدخل قبل وقوع أي هجوم. ولتحقيق ذلك، يحتاج نموذج الذكاء الاصطناعي إلى كميات هائلة من البيانات الآنية المتعلقة بسلوك الإرهابي أو المشتبه به. ومن خلال تحليل هذه البيانات، يمكن لهذا النموذج، على سبيل المثال، التنبؤ بالأنشطة المستقبلية المحتملة لهؤلاء الأفراد. ونظرًا للنمو الهائل الذي شهده العقد الماضي في كمية البيانات المتعلقة بسلوك الأفراد على الإنترنت، لا سيما على وسائل التواصل الاجتماعي، فقد ازداد الاهتمام باستكشاف كيفية استخدام بيانات وسائل التواصل الاجتماعي التي تم جمعها، والتي تتناول سلوك الأفراد على الإنترنت، للتنبؤ بالأنشطة الإرهابية"[13].

كما ان "الاستخبارات مفتوحة المصدر هي منهجية مهمة لجمع البيانات المتاحة وتحليلها وتفسيرها. تتنوع مصادر الاستخبارات مفتوحة المصدر بين وسائل الإعلام (الصحف المطبوعة، والتلفزيون، وغيرها)، والإنترنت (المنشورات الإلكترونية، والمدونات، ومواقع التواصل الاجتماعي الأخرى)، والبيانات الحكومية العامة، والمنشورات المهنية والأكاديمية، والبيانات التجارية، أو ما يُعرف أحيانًا بـ"الأدبيات الرمادية" (التقارير الفنية، وبراءات الاختراع، والنشرات الإخبارية، وغيرها). اذ تساعد أدوات الاستخبارات مفتوحة المصدر في تصفح المواد وتحليلها وعرضها بصريًا، بدءًا من البحث عن كلمات مفتاحية محددة وصولًا إلى تتبع تفاعلات الحسابات. وتُعد استخبارات وسائل التواصل الاجتماعي فرعًا من فروع الاستخبارات مفتوحة المصدر، وتركز على جمع المعلومات الاستخباراتية من وسائل التواصل الاجتماعي. في هذه الحالة، وتُمكّن أدوات استخبارات وسائل التواصل الاجتماعي المؤسسات من تحليل المحادثات، والاستجابة للإشارات الاجتماعية، وتجميع نقاط البيانات الاجتماعية في اتجاهات وتحليلات ذات مغزى"[14].

فضلاً عن ذلك، "تكمن القيمة المضافة لأنظمة الذكاء الاصطناعي الناشئة في تقليل العبء المعرفي المرتبط بالمستويات التكتيكية والعملياتية لمكافحة الإرهاب. فالقدرة على استهلاك ومعالجة وتلخيص كميات هائلة من المعلومات، بغض النظر عن نوع البيانات، ستُبسط عملية صنع القرار وتُهيئ الحكومات بشكل أفضل للاستجابة للإرهاب. ومع مرور الوقت، يُمكن أتمتة معظم عمليات

مكافحة الإرهاب باستخدام مجموعة من منصات الذكاء الاصطناعي. ويكمن التحدي الذي يواجه الحكومات في كيفية بناء استراتيجيات تستفيد من هذه القدرات الجديدة. ولتحقيق ذلك، يجب عليها أولاً فهم نقاط القوة والضعف في الذكاء الاصطناعي، مع إدراك وجود وظائف معينة لا يُمكن تنفيذها إلا من قِبل البشر، والتي تقع في المقام الأول على المستوى الاستراتيجي"[15].

وفي هذا السياق، "تجلى مفهوم "الاستخدام الخبيث للذكاء الاصطناعي" لوصف الأفعال التي تُؤدي عمدًا إلى عواقب وخيمة. ففي عام(٢٠١٨)، قام فريق من المؤلفين البارزين من مختلف التخصصات والمنظمات لاسيما في ذلك معهد مستقبل الإنسانية بجامعة أكسفورد، ومركز دراسة المخاطر الوجودية بجامعة كامبريدج، ومؤسسة الحدود الإلكترونية، ومركز الأمن الأمريكي الجديد، بدراسة الاستخدام الخبيث للذكاء الاصطناعي من قِبل الدول والمجرمين والإرهابيين. وقدّر تقريرهم، الذي حمل عنوان "الاستخدام الخبيث للذكاء الاصطناعي: التنبؤ والوقاية والتخفيف"، نموًا سريعًا في الاستخدام الخبيث لهذه التقنية خلال العقد القادم. ورأى المؤلفون بأن الاستخدام الخبيث للذكاء الاصطناعي يُشكّل تهديداً على صعيد الأمن السيبراني والأمن المادي والأمن السياسي. فالتهديدات السيبرانية تعد مجالًا متزايد الأهمية نظرًا لنقاط الضعف الكامنة في الفضاء السيبراني والطبيعة غير المتكافئة للتهديدات التي تُشكّلها الهجمات السيبرانية. فهي من منظور مكافحة الإرهاب، تشمل التهديدات المرتبطة بالاحتيال، وبرامج الفدية، وهجمات الحرمان من الخدمة الموزعة، فضلاً عن تشويه المواقع الإلكترونية. فضلاً عن ذلك، يتزايد القلق بشأن إساءة استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات، ولا سيما الإنترنت ووسائل التواصل الاجتماعي، لارتكاب أعمال إرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها"[16].

وتكاملاً مع ما سبق، "حظي الذكاء الاصطناعي باهتمام عالمي كبير كأداة قادرة على معالجة كميات هائلة من البيانات، واكتشاف الأنماط والروابط فيها التي لا يراها الإنسان، مما يُعزز الفعالية والكفاءة في تحليل المعلومات المعقدة. وباعتباره تقنية متعددة الأغراض، يمكن الاستفادة من هذه المزايا في مجال مكافحة الإرهاب. وفي ضوء ذلك، يتزايد اهتمام أجهزة إنفاذ القانون ومكافحة الإرهاب عالميًا باستكشاف كيفية إطلاق العنان للإمكانات التحويلية للذكاء الاصطناعي"[17]. وهو ما مثل تحولاً كبيرا ومتعدد الاتجاهات، وانتج تحديات وفرص في الوقت نفسه.

المطلب الثاني: التحديات التي يفرضـها الذكاء الاصطناعي في مجال مكافحة الارهاب

تتمثل التحديات الرئيسة التي تواجه "توظيف الذكاء الاصطناعي في مجال مكافحة الإرهاب في عدم توفر كميات هائلة من البيانات المطلوبة أو صعوبة الوصول إليها. كما يشير التشخيص الدقيق لواقع الإرهاب بأن الحوادث لا تحدث بشكل منتظم، وغالبًا ما تكون الأحداث وحالات التطرف فريدة من نوعها. اذ توجد العديد من قواعد البيانات مفتوحة المصدر حول الإرهاب والتي يمكن استخدامها لأغراض تدريب الخوارزميات، مثل قاعدة بيانات الإرهاب العالمية، والتي تجمع معلومات تاريخية عن أكثر من (200,000) حادث إرهابي على مستوى العالم منذ عام(1970). ورغم أن هذه المصادر قيّمة للغاية، لاسيما فيما يتعلق بالتنبؤ بأنواع الهجمات الإرهابية المحتملة في المستقبل، والمناطق المستهدفة، والأسلحة المستخدمة، فإن تطبيق النماذج الموضحة في هذا التقرير يتطلب بيانات أكثر تحديدًا وتتعلق بأفعال الإرهابيين الأفراد أو المشتبه بهم، مثل بيانات وسائل التواصل الاجتماعي. ونظرًا لأن معظم هذه البيانات غير منظمة، فسيكون من

الضروري بذل جهد كبير لإعدادها لكي يتم فيما بعد توظيفها. ويتجلى تحدي اخر في ان أحد الحلول الممكنة للتغلب على نقص بيانات "العالم الحقيقي" هو استخدام "البيانات المعززة بالادلة"، أي البيانات الاصطناعية التي تُنتجها الشبكات التنافسية العامة (GANs) لأغراض تدريب الخوارزميات. ومع ذلك، لا تزال هناك حاجة إلى مزيد من البحث لاستكشاف البيانات في مجال مكافحة الإرهاب"[18].

فضلاً عن ما تقدم، و"نظراً لعدم القدرة على التنبؤ بالسلوك الانساني والوضع الراهن للتقدم التكنولوجي، فمن المرجح أن يظل تطبيق الخوارزميات للتنبؤ بالسلوك على المستوى الفردي ذا قيمة محدودة للغاية. وفي هذا السياق، أشار خبراء حقوق الإنسان ومنظمات المجتمع المدني إلى العديد من المخاوف الأخلاقية المتعلقة بالتمييز في الأحكام والمعاملة. كما أن الكميات الهائلة من البيانات المتعلقة بالفرد والتي تعد ضرورية لكي تعمل الخوارزمية بدقة، تثير مخاوف بشأن إمكانية المراقبة الجماعية غير المبررة"[19].

وكما هو الحال مع الحرب الالكترونية، "يُمثل الذكاء الاصطناعي ثورة تكنولوجية جديدة، اذ لا توجد له مفاهيم أو تعريفات مُقابلة في القانون او العرف الدولي. فعلى سبيل المثال، لا تزال هناك تحديات جسيمة بشأن إمكانية تطبيق المفاهيم الأساسية التقليدية لقانون الحرب لاسيما التفريق بين المدنيين والمقاتلين، والمبادئ التي تطبق في النزاعات المسلحة، على الذكاء الاصطناعي والمنصات غير المأهولة والتي يحدث فيها القتال، وكيفية تطبيقها. ويُقدم الإصدار الثاني من دليل تالين للحرب الالكترونية، الذي جمعه الباحثون المتخصصون في القانون من المجتمع الدولي، بعض التوجيهات في هذا الشأن. ومع ذلك، لا يزال النقاش مستمراً حول قوانين ولوائح الذكاء الاصطناعي التي هي بحاجة إلى مزيد من التعمق. وتكاملاً مع ما تحذر، وقبل تحديد معيار الاستخدام العسكري للذكاء الاصطناعي، فانه لا يُمكن استبعاد لجوء الدول إلى استغلال الثغرات والمناطق الرمادية في القواعد لتقويض السلام والاستقرار الإقليميين. وسيؤدي التطبيق العسكري للذكاء الاصطناعي في نهاية المطاف إلى قضايا أخلاقية تتعلق بالصراع بين الإنسان والآلة. فهل ينبغي للإنسانية أن تُسلم مصيرها لآلات تفوق ذكاءها ذكاءً؟ وهل يُمكن للآلات أن تحل محل البشر في صنع القرار، بل وتحديد المسار النهائي للحضارة الإنسانية؟ بمجرد أن يُصبح استخدام الذكاء الاصطناعي واسع النطاق في المجال العسكري، ستُصبح هذه المعضلات حتمية"[20].

وعلى هذا الأساس، فإن "الاستخدامات المتنوعة للذكاء الاصطناعي في سياق عمليات مكافحة الإرهاب قد تنتهك العديد من الحقوق الأساسية، بما في ذلك الخصوصية وحماية البيانات؛ والمساواة وعدم التمييز؛ وحرية التعبير، وتكوين الجمعيات، والتجمع السلمي، وممارسة الشعائر الدينية؛ والمشاركة السياسية؛ والحرية الشخصية؛ والأمن الشخصي؛ والحياة؛ وحقوق الفئات الضعيفة والمهمشة والمحرومة. كما أن عمل وسلامة المدافعين عن حقوق الإنسان معرضة للخطر"[21].

وتكاملاً مع ما تقدم، "أظهر استطلاع رأي أجراه مركز الأمم المتحدة لمكافحة الإرهاب التابع لمكتب الأمم المتحدة لمكافحة الإرهاب ومعهد الأمم المتحدة لأبحاث الجريمة والعدالة، من خلال مركز الذكاء الاصطناعي والروبوتات التابع له، بان هنالك مخاوف مماثلة. فمن بين(27) ممثلًا عن الحكومات والقطاعات الصناعية والأكاديمية والمنظمات الدولية والإقليمية، رأى (44%) منهم بأن الاستخدام الخبيث للذكاء الاصطناعي لأغراض إرهابية "محتمل جدًا"، بينما رأى(56%) أنه "محتمل إلى حد ما". والجدير بالذكر أنه لم يرَ أي من المشاركين في

الاستطلاع أن الاستخدام الخبيث للذكاء الاصطناعي بهذه الطريقة "غير محتمل"[22].

فضلاً عن ذلك، لا تزال العديد من "أنظمة الذكاء الاصطناعي في مراحل التطوير أو التجريب أو الاختبار، ولم تثبت قدراتها بشكل حقيقي. وثمة خطر حقيقي يتمثل في أن يبالغ مؤيدو الذكاء الاصطناعي، بمن فيهم الشركات التي تغذي طفرة الاستثمار العالمي الحالية في هذا المجال، في تقدير فوائده، ويعملوا على التقليل من شأن تكاليفه ومخاطره. ونظرًا لأن عدد الإرهابيين الفعليين في معظم المجتمعات ضئيل للغاية، فإن القيود الجسيمة على البيانات قد تحول دون الاستقراء المفيد لغرض الكشف عن التهديدات المستقبلية، لا سيما عند التنبؤ بسلوك الأفراد. كما أن السرية المتعلقة بالملكية الفكرية والأمن القومي المحيطة بتطوير الذكاء الاصطناعي ونشره، قد تحجب هذه التقنية عن التدقيق المستقل للتحقق من فعاليتها ومخاطرها، بما في ذلك المؤشرات المتعلقة بمعدلات الإنذارات الكاذبة وحالات الفشل في اكتشاف المخاطر، فضلًا عن الرقابة التشغيلية الفعالة، لا بل ان بعض تقنيات أمن الذكاء الاصطناعي قد تكون محجوبة تماماً عن العامة وغير معروفة لهم. كما ان التحدي الأكبر يتمثل في انه لا تتوافر بيانات كافية حول مدى توظيف أنظمة الذكاء الاصطناعي من قبل سلطات مكافحة الإرهاب وإنفاذ القانون على مستوى العالم، وأنواع الأنظمة المستخدمة، ومدى فعاليتها بشكل موضوعي، وما هي انتهاكات الحقوق والأضرار الأخرى التي تسببها، وما هي الحدود بين الأمن والحرية"[23].

كما "يتجسد الاستخدام الخبيث للذكاء الاصطناعي في مجموعة من التحديات التي تدفع الى توظيفه لأغراض ارهابية، أولهما: ان الذكاء الاصطناعي اصبح متاحاً للجميع، وعلى الرغم من ان العديد من الخوارزميات مفتوحة المصدر، إلا أن خطر الاستخدام الخبيث المحتمل يزداد بنفس القدر بفعل إمكانية لجوء هذه الجماعات إلى الاستعانة بمصادر خارجية لاسيما في المجال الاقتصادي والذي تستخدمه الجماعات الإجرامية، اذ "يُحرك الاقتصاد الرقمي الخفي من خلال توفير مجموعة واسعة من الخدمات التجارية التي تُسهل ارتكاب أي نوع تقريبًا من الجرائم الإلكترونية". ثانيهما: قابلية الذكاء الاصطناعي للتوسع من حيث الحجم والنطاق، مما يقود الى ضرورة الاستعداد والدفاع ضد الجمات الفردية والجماعية مثل تهديد أسراب الطائرات المسيرة التي تحلق بشكل متزامن. ثالثهما: عدم التكافؤ المتأصل في مجال مكافحة الإرهاب، ويتجسد ذلك في مقولة مهمة: علينا أن نكون محظوظين في كل مرة، بينما يكفيهم أن يكونوا محظوظين مرة واحدة". ويمكن ملاحظة هذا التفاوت في التحديات التي تواجهها جهات مكافحة الإرهاب والإرهابيون فيما يتعلق باستخدام الذكاء الاصطناعي، يتطلب الأمر دراسة متأنية لاستخدامه بما يضمن مراعاة الحريات المدنية وحقوق الإنسان الأساسية. ومع ذلك، من المرجح ألا تُولي الجهات الخبيثة، كالجماعات والأفراد الإرهابيين، اهتماماً كبيراً لهذه المخاوف، مما يُسهّل عليهم استخدام الذكاء الاصطناعي في جوانب عديدة رابعهما: تزايد اعتماد المجتمع على البيانات والتكنولوجيا، وعلى موثوقية البيانات لضمان استمرارية عمله بما في ذلك البنى التحتية الحيوية مثل مقدمي الرعاية الصحية، ومزودي الطاقة، والمنشآت البيولوجية والنووية. ورغم ما يوفره هذا من مزايا عديدة، إلا أنه يزيد في الوقت نفسه من احتمالية تعرض أنظمة الذكاء الاصطناعي للهجمات الإلكترونية التي تستخدم الذكاء الاصطناعي، أو للهجمات التقليدية التي تستهدف هذه الأنظمة داخل هذه البنى التحتية أو البيانات التي تعمل عليها"[24]. وعلى الرغم من التحديات الكبيرة التي ترافق تعاظم توظيف الذكاء الاصطناعي، فانه

يتضمن العديد من الفرص التي أسهمت معطيات مكافحة الإرهاب.

المطلب الثالث: الفرص التي يوفرها الذكاء الاصطناعي في مجال مكافحة الارهاب

على الرغم من "توضيح مخاطر الذكاء الاصطناعي في أعلاه، إلا أنه يُمكن أن يؤدي دورًا مهما في دعم جهود مكافحة الإرهاب بطرقٍ مُتعددة. وأحد تطبيقاته هو المراقبة والرصد، اذ يُمكنه من تحليل مقاطع الفيديو المباشرة لرصد السلوكيات أو الأشياء المشبوهة في الأماكن العامة، مما يُساعد السلطات على الاستجابة السريعة للتهديدات المحتملة. وفيما يتعلق بمكافحة الدعاية المتطرفة واستئصال التطرف، فانه يُمكن لأدوات الذكاء الاصطناعي الكشف تلقائيًا عن المحتوى المتطرف وإزالته من المنصات الإلكترونية، مما يحد من انتشار الدعاية الإرهابية. كما يُمكنه ذلك من دعم برامج القضاء على التطرف من خلال تحديد الأفراد المعرضين للخطر وتحليل سلوكياتهم عبر الإنترنت"[25].

ومع ذلك، فانه "بإمكان التحليلات التنبؤية المساهمة في مكافحة الإرهاب، ولكن بطريقة مختلفة. فبدلاً من مراقبة الأفراد عبر الإنترنت والتنبؤ بسلوكهم، يمكن استخدام نماذج تنبؤية تستند إلى إحصاءات من مصادر عبر الإنترنت، والتي تم إخفاء هوية أصحابها تماماً أو على الأقل استخدام أسماء مستعارة لحماية خصوصية المستخدم، لتحديد الاتجاهات أو التنبؤ بالسلوك المستقبلي للمتطرفين. ويمكن أن يكون هذا التحليل القائم على البيانات المجمعة فاعلاً لدعم أجهزة الأمن والاستخبارات في تحديد أولويات الموارد القليلة كدعم عملياتي، واتخاذ قرارات استراتيجية، أو تقديم تحذيرات للسلطات المختصة. اذ تسهم التحليلات التنبؤية في خلق رؤى عميقة حول بنية شبكة الجماعات الإرهابية، والتنبؤ بالانقسامات، ووضع سياسات تهدف إلى الحد من الهجمات"[26].

وفي هذا السياق، "يُعد التحليل التنبؤي مجالًا آخر لعملية توظيف الذكاء الاصطناعي. فمن خلال تحليل الأنماط في البيانات التاريخية، ونشاط وسائل التواصل الاجتماعي، ومصادر المعلومات الاستخباراتية الأخرى، يُمكن للذكاء الاصطناعي التنبؤ بالهجمات الإرهابية المحتملة. فهو قادر على تقييم سلوك الأفراد أو الجماعات لتحديد علامات التطرف والتدخل قبل وقوع الهجمات. وفيما يتعلق بتحليل البيانات وجمع المعلومات الاستخباراتية، فان الذكاء الاصطناعي يدمج مجموعات من البيانات الضخمة من مصادر متعددة مثل لقطات المراقبة، والمنصات الرقمية، والمعاملات المالية لتوفير رؤى شاملة. كما يستخدم عمليات معالجة اللغة لفهم وتحليل واعتراضات الاتصالات والمحتوى الإلكتروني، بحثًا عن التهديدات المحتملة. كما يمكن للذكاء الاصطناعي أيضًا تحسين الكفاءة التشغيلية في مكافحة الإرهاب. فهو قادر على تحسين تخصيص الموارد للعمليات، وضمان نشر الأفراد والمعدات بفعالية. كما يمكنه تزويد صانعي القرار ببيانات وتوصيات آنية، مما يعزز من فعالية استراتيجيات مكافحة الإرهاب. مع ذلك، من الضروري التذكير بأن أي تدابير مضادة تُنفذ يجب أن تُحقق توازنًا دقيقًا بين حماية رفاهية المجتمع والحفاظ على التبادل الحر للأفكار والابتكار، وهما سمتان للمجتمعات الديمقراطية"[27].

فضلاً عما تأصل من فرص، "تتمثل احدي استخدامات الذكاء الاصطناعي الأخرى في مكافحة الإرهاب عبر الإنترنت في توظيف تقنيات الذكاء الاصطناعي للمساعدة في تحديد الأفراد المعرضين لخطر التطرف في المجتمعات الإلكترونية، وذلك لتيسير التحقيق والتدخل المناسبين، وهي ظاهرة متزايدة الأهمية على الإنترنت. كما أنها ظاهرة يستحيل رصدها باستخدام أساليب إنفاذ القانون التقليدية. وبينما يُعدّ التطرف ظاهرة

اجتماعية معقدة، ومساره شخصي للغاية، وغالبًا ما يكون سياسيًا، فإن تقنيات التعلّم الآلي، يمكن أن تُقدّم دعمًا قيّمًا لأجهزة إنفاذ القانون ومكافحة الإرهاب، فضلًا عن الجهات الفاعلة الأخرى ذات الصلة بالمجتمع كالأخصائيين الاجتماعيين. ويمكن استخدام معالجة اللغة الطبيعية، على سبيل المثال، لتحديد الكلمات المفتاحية التي قد تُشير إلى حالة التطرف في الحسابات على وسائل التواصل الاجتماعي، أو مدى تأثر الفرد بالخطابات الإرهابية على الإنترنت. كما يُمكن أن يكون من المفيد التعرّف على أنماط سلوكية مُحددة للأفراد، مثل استهلاك أو البحث عن محتوى إرهابي أو متطرف، وهو ما يتوافق مع مؤشرات التطرف"[28].

المبحث الثالث: مآلات التوظيف الدولي للذكاء الاصطناعي في عمليات مكافحة الإرهاب

لم يعد الذكاء الاصطناعي ضمن الاطار النظري، وانما بدأ يدخل تدريجياً في عمليات التوظيف الحقيقي لدى الدول والفواعل من غير الدول سواء كانت المدنية أم العسكرية، واصبح يشغل مكانة مهمة في الاستراتيجيات الدولية بجوانبها كافة الأمنية والعسكرية، لا بل شرعت الدول في توظيفها في الحروب التكنومعلوماتية وعمليات مكافحة الإرهاب وفق رؤيتها الخاصة بها وتعريفها الخاص لماهية الارهاب. وفي هذا السياق، فان الايغال في عملية سبر غور التوظيف الاستراتيجي الدولي للذكاء الاصطناعي في عمليات مكافحة الإرهاب يتطلب استعراض مجموعة من النماذج الدولية التي تمتلك خبرة في هذا المجال، ومن ثم الانتقال الى بحث مألات التوظيف المستقبلية بهدف معرفة المسارات المستقبلية.

المطلب الأول: النماذج الدولية في توظيف الذكاء الاصطناعي في المجالات الأمنية ومكافحة الارهاب

لقد اصبح الذكاء الاصطناعي في مجاله الأمني احد الأهم الأدوات الأمنية غير التقليدية التي توظفها القوى الدولية الفاعلة في البيئة الاستراتيجية الأمنية الدولية لاسيما في تعزيز الامن القومي لها ومواجهة التهديدات التي تعدها ارهابية بفعل امتلاك الذكاء الاصطناعي، وما تملكه من قدرة كبيرة على تجميع وتحليل البيانات وتحليلها بوقت قياسي ومن ثم التنبؤ بالتهديدات قبل وقوعها. وتعد الولايات المتحدة والصين وأوروبا من الفواعل الدولية الرائدة في هذا المجال كونها تمتلك البنى التحتية التكنولوجية المتقدمة والتي تمكنها من توظيفها بشكل فاعل ولكن لكل منهما استراتيجيته ورؤيته الخاصة به.

اولاً: الولايات المتحدة

أصدرت الحكومة الأمريكية في السنوات الأخيرة "سلسلة من الوثائق حول استراتيجية الذكاء الاصطناعي. اذ تؤكد هذه الوثائق على استخدام الابتكار التكنولوجي للحفاظ على التفوق العسكري الأمريكي في المستقبل، وهو ما يُعرف باستراتيجية التعويض الثالث. كما تشير هذه الوثائق إلى أنه لا توجد تقنية أخرى تُضاهي تأثير الذكاء الاصطناعي والتقنيات الذكية على العمليات العسكرية الأمريكية، سواءً تم استُخدامها في الاستشعار عن بُعد، أم شبكات القيادة والسيطرة، أم العمليات، أم شبكات الدعم اللوجستي. وانطلاقًا من هذه الأولويات، عملت الحكومة الأمريكية في حزيران من عام (2017) في الحد من استثمارات الصين في الذكاء الاصطناعي داخل الولايات المتحدة. وفي هذا السياق، وانطلاقًا من خصائص ومزايا تقنية الذكاء الاصطناعي، سعى الجيش الأمريكي إلى الريادة في اقتراح مفهوم عملياتي جديد للحرب الخوارزمية، يرتكز على تقنيات التعلم الآلي والتعلم العميق"[29].

اذ يرى صناع القرار في الولايات المتحدة بانه "يمكن من خلال رقابة المحتوى تعزيز جهود مكافحة الإرهاب من خلال استخدام أنظمة البيانات الضخمة وتحليل الشبكات الاجتماعية التي تفحص الشبكة وتحدد

مراكز ثقل الجماعات الإرهابية. وبالاستناد إلى أساليب الاستخبارات التقليدية لتحليل الروابط، سيُمكّن نهج تحليل الشبكات الاجتماعية، المدعوم بخوارزميات الذكاء الاصطناعي، من فحص الشبكات على نطاق واسع لرسم خرائط المجتمعات، وتحديد الجهات الفاعلة الرئيسية فيها، وتحديد مراكز الثقل التنظيمية. ووفقاً لذلك تُحدد هذه الطريقة سرعة الانتماءات الجديدة كمؤشرات للتحليل، والجهات الفاعلة المهيمنة للمراقبة أو الاستهداف، ووظائف العدو وهياكله الهرمية داخل التنظيم الإرهابي، مما يُتيح تطوير وتنفيذ حملات إعلامية أو نفسية لمواجهة انتشار الأيديولوجيات العنيفة" [30].

وفي هذا السياق، "جمعت الولايات المتحدة على مدى العشرين عامًا الماضية كميات هائلة من البيانات المتعلقة بمكافحة الإرهاب ودراسته. فمنذ عام(٢٠١٨)، اتخذت الحكومة الأمريكية خطوات جادة لدمج وتوسيع نطاق استخدام علوم البيانات والتعلم الآلي والذكاء الاصطناعي في منظومة الأمن القومي، سعيًا منها إلى إحداث تغيير جذري، والابتكار، والاستعداد لمستقبل يعتمد على الذكاء الاصطناعي. مما اوجد علاقة بين مخزون الولايات المتحدة الهائل من بيانات والإرهاب، والقوة التحويلية لعلوم البيانات والذكاء الاصطناعي. اذ يرى احد الكتاب بان هنالك حاجة الى خمس ركائز: أولهما: إعادة الاستثمار في بيانات الإرهاب الأساسية وتطويرها، ثانيهما: الاستفادة الاستراتيجية من المواد التي تم الحصول عليها، ثالثهما: تطوير بيانات مكافحة الإرهاب واستخدامها بشكل أفضل، رابعهما: ممارسة دمج البيانات، خامسهما: أتمتة المهام التحليلية الأساسية وغيرها، وتعزيز البيانات"[31].

وتكاملاً مع ما سبق، "تُعدّ التغييرات التي تم اجراؤها في وزارة الدفاع الأمريكية (البنتاغون) من الأهمية بمكان. فمنذ عام(2018)، أصدر البنتاغون استراتيجيته للذكاء الاصطناعي(2018)، واستراتيجيته للتحديث الرقمي(2019)، واستراتيجيته للبيانات (2020). وفي عام (2018)، أعلنت وكالة مشاريع البحوث الدفاعية المتقدمة عن "استثمار لسنوات متعددة تبلغ قيمتها ملياري دولار في برامج جديدة تحت مسمى حملة "الذكاء الاصطناعي القادم"، مع التركيز على مجالات رئيسة". واكتسبت هذه الجهود والاستثمارات هيكلًا تنظيميًا من خلال إنشاء مركز الذكاء الاصطناعي المشترك التابع لوزارة الدفاع، وهو كيان أُنشئ ليكون نقطة ارتكاز لتنفيذ استراتيجية البنتاغون للذكاء الاصطناعي. في العام نفسه. كما اتخذت قيادة العمليات الخاصة الأمريكية (SOCOM) خطوة تنظيمية مماثلة من خلال إنشاء مكتب بيانات القيادة التابع لها، والذي صُمم "للإشراف على تحويل القوى العاملة، فضلاً عن توفير نقطة اتصال للتواصل مع الصناعة، وحوكمة البيانات، والتركيز على البيانات في عمليات صنع القرار لتطوير القدرات". كما تتابع وحدة الابتكار الدفاعي بشكل فاعل عدد من مشاريع الذكاء الاصطناعي لتحسين عمليات الأعمال في وزارة الدفاع"[32].

وتجذيراً لما تقدم، "يتولى قسم مكافحة الإرهاب التابع لشعبة الأمن القومي في وزارة العدل الأمريكية مسؤولية دمج جهود إنفاذ القانون والمبادرات التشريعية والاستراتيجيات المتعلقة بها بمكافحة الإرهاب الدولي والمحلي. وعلى المستوى التكتيكي، تعمل فرق العمل المشتركة لمكافحة الإرهاب التابعة لمكتب التحقيقات الفيدرالي (JTTF) كخط دفاع أول ضد (الإرهاب) من خلال دمج المحققين والمحللين وفرق الاستجابة للأزمات على المستويين المحلي والفيدرالي. وبفضل المعلومات والتحليلات والقرائن الاستقصائية، تستطيع فرق العمل المشتركة لمكافحة (الإرهاب) استخدام

الذكاء الاصطناعي والتعلم الآلي لتعزيز أنشطة المراقبة القانونية، بما في ذلك المراقبة السلبية، والمراقبة النشطة للأهداف، والتعرف على الوجوه، والتحقق من الهوية، ودمج أجهزة استشعار المتعددة الأوجه، وتسجيل البيانات عبر تقنية سلسلة تقنية لربط السجلات المالية للمتطرفين من خلال التشفير. وبموجب الصلاحيات الممنوحة لها بموجب الباب (50) من قانون الولايات المتحدة، تستفيد وزارة العدل من أدوات محددة مثل التراخيص الصادرة بموجب قانون مراقبة الاستخبارات الأجنبية، في تعظيم فعالية الجهود الاستقصائية والتحليلية، بما في ذلك المراقبة الإلكترونية والتفتيش المادي للأشخاص المتورطين في الإرهاب الدولي ضد الولايات المتحدة"[33].

وعلى هذا الأساس، "جمعت الولايات المتحدة كمية هائلة من المعلومات خلال عمليات مكافحة الإرهاب التي نُفذت منذ أحداث الحادي عشر من أيلول عام(2001). في مقال نُشر في مجلة (Joint Forces Quarterly) عام(2020)، بين بأن الجيش الأمريكي يمتلك "أكثر من(300) تيرابايت من المواد القابلة للاستغلال المجمعة (CEM)، والتي جُمعت من جميع أنحاء العالم". اذ يشمل هذا الأرشيف المتنوع من المواد أدلة جنائية وبيانات من أجهزة الكمبيوتر، ومحركات الأقراص الصلبة الخارجية، والهواتف المحمولة، فضلاً عن المواد المادية مثل الكتب، والكتيبات، والمذكرات، والرسائل، وأنواع أخرى من المراسلات الشخصية التي تم استعادتها. كل هذه البيانات، التي أطلق عليها الجيش الأمريكي اسم "المواد القابلة للاستغلال المجمعة (CEM)" أو أدلة ساحة المعركة، كانت حاسمة في مساعدة من يقومون بمكافحة الإرهاب على تحديد مواقع أهداف إرهابية جديدة وتعزيز فهم ديناميكيات الجماعات الإرهابية الداخلية وفق وجهة النظر الامريكية، مثل أولويات القادة، والعلاقات بين الجماعات، والتحديات التنظيمية، والتفاصيل البيروقراطية المرتبطة بإدارة الشبكات الإرهابية. بذلك فان المواد القابلة للاستغلال المجمعة (CEM) أهمية بالغة[34].

ووفقاً للاستراتيجية القومية الأمريكية لمكافحة الإرهاب، "لا يزال الإرهابيون المتطرفون يشكلون التهديد العابر للحدود الرئيسي للولايات المتحدة ومصالحها القومية. وقد أظهرت المنظمات الجهادية العالمية البارزة، وعلى رأسها (داعش) وتنظيم القاعدة، مسلحة بأيديولوجية متطرفة عنيفة، نية وقدرة على شن هجمات ضد الأراضي الأمريكية، ولا تزال تهدد المصالح الأمريكية في جميع أنحاء العالم. ومن الجدير بالذكر أن التهديد الإرهابي في الولايات المتحدة يتسم بديناميكية وانتشار متزايدين، حيث يستغل عدد متزايد من الجماعات والشبكات والأفراد التوجهات العالمية، بما في ذلك ظهور وسائل اتصال أكثر أمانًا، وتوسع وسائل التواصل الاجتماعي والإعلام الجماهيري، واستمرار حالة عدم الاستقرار في مناطق عديدة"[35].

والاستكشاف الشامل للمقاربات الامريكية لتوظيف الذكاء الاصطناعي في مكافحة الإرهاب تؤكد بانه "مع التحوّل في الاهتمام الاستراتيجي والموارد الحيوية نحو التنافس بين القوى العظمى، يجب أن تبقى استراتيجية مكافحة الإرهاب الأمريكية ذات أهمية كبرى، مع التركيز بشكل خاص على توظيف التقنيات الناشئة وتجديد العلاقات مع القطاع الخاص والمجتمع الدولي لمواكبة الأساليب الحديثة التي توظفها المنظمات المتطرفة العنيفة. ويعدّ التنبؤ عنصرًا رئيساً في أي استراتيجية فعّالة لمكافحة الإرهاب، إذ يتطلب مرونةً وتنسيقًا شاملًا لمنع الهجمات العنيفة في المستقبل. ورغم وجود مخاطر معروفة في تطبيق التطورات التكنولوجية في إنفاذ القانون والأنشطة الاستخباراتية، فإن أنظمة الذكاء الاصطناعي التنبؤية تُتيح فرصةً لزيادة سرعة وكفاءة وفعالية أنشطة مكافحة الإرهاب،

سواءً من حيث التصدي للتطرف عبر الإنترنت أم قدرة المتطرفين على تصدير الإرهاب على نطاق عالمي. والهدف النهائي لهذه الاستراتيجية المتقدمة هو الحدّ من تطرف وتعبئة المتطرفين عبر الإنترنت، وضمان خفض الهجمات الإرهابية العنيفة ضد الولايات المتحدة وشركائها الدوليين"[36].

كما انهم يرون بانه "يمكن استخدام المعلومات الحقيقية بوصفها سلاح في حملات التأثير الخارجي. إذ يُمكن للجهات الخبيثة تقويض المؤسسات الديمقراطية عبر القرصنة الإلكترونية وتسريب المعلومات(الحقيقية). وقد تُؤدي عملية الكشف الانتقائي عن المعلومات المخترقة إلى انعدام الثقة وتقويض الحوار الوطني المدني. ومع تزايد الانقسام والتشرذم في المشهد المعلوماتي الأمريكي، يُعدّ الشعور السائد بانعدام الثقة في النظام مكسبًا لمعارضي الديمقراطية، اذ تشمل أساليب تقويض التماسك بهذه الطريقة الاحتيال الموجه للحملات الانتخابية وتسريب المعلومات. ويتسم التصيد الاحتيالي الموجه بمحاولات خداع الهدف لحمله على كشف معلومات أو تثبيت برامج ضارة من خلال انتحال صفة طلب مشروع عبر البريد الإلكتروني. ومن المرجح أن يستمر التصيد الرقمي مثل الهجوم الإلكتروني الذي استهدف رئيس حملة المرشحة الرئاسية الامريكية هيلاري كلينتون، جون بوديستا، والمؤتمر الوطني الديمقراطي عام(2016)، ليستهدف المرشحين وموظفيهم، لابل حتى مسؤولي الانتخابات. وعلى هذا الأساس، فانه من خلال مساعدة عملية معالجة المعلومات المدعومة بالذكاء الاصطناعي، سيصبح من الصعب التمييز بين هذه الهجمات والطلبات والاستفسارات المشروعة. ولذلك فإن القدرة على تنفيذ عمليات التصيد الاحتيالي الآلي على نطاق واسع ستزيد من احتمالية نجاح المهاجم"[37].

وفي العقد الثالث من القرن الحادي والعشرين، "تخوض الولايات المتحدة صراعًا واسع النطاق يتطلب حلولًا من الجهات الفاعلة الرئيسة لاسيما القطاع التكنولوجي الخاص والحكومة الأمريكية. ويرى الخبراء الامريكيون بانه لا يمكنهم إهدار الدروس الرقمية والتنظيمية والاستراتيجية المستفادة من قرابة عقدين من مكافحة الإرهاب. إن التعلم من النجاحات المحددة في قطاع التكنولوجيا وجهود الحكومة الأمريكية في مكافحة الإرهاب سيُحسّن استجابة الولايات المتحدة الجماعية لتحديات التضليل الرقمي في المستقبل. وينبغي على الجهات الفاعلة في القطاعين الخاص والعام مراعاة خمسة دروس مهمة في مكافحة الإرهاب: أولهما: تحسين الأساليب التقنية لتحديد محتوى حملات التأثير الأجنبي؛ وثانيهما: زيادة التعاون بين الشركات؛ وثالثهما: بناء شراكات بين الحكومة وقطاع التكنولوجيا من خلال تبادل المحللين بين القطاعين العام والخاص؛ ورابعهما: الحفاظ على الوضع الهجومي وتخصيص الموارد اللازمة لإبقاء الخصم في موقف دفاعي؛ وخامسهما: الاستفادة من خبرات حلفاء الولايات المتحدة"[38].

ووفقاً لوجهة النظر الامريكية "تُعدّ هذه الخطوات مؤشرات هامة على التقدم الذي يتم تحقيقه. اذ توفر وثائق وخطط استراتيجية البيانات والذكاء الاصطناعي التي نشرتها الحكومة الأمريكية الإطار العام لكيفية نيتها، أو تأملها، في المضي قدمًا في مجال البيانات والذكاء الاصطناعي. وقد استُكمل ذلك برؤية قدمها خبراء مخضرمون، مثل الفريق المتقاعد روبرت آشلي، الرئيس السابق لوكالة استخبارات الدفاع، حول الوجهة التي ينبغي أن تقود إليها أو التي يُحتمل أن تقود إليها هذه التغييرات، فعلى سبيل المثال، وفقًا للمقاربات التي يقدمها روبرت آشلي فانه "في المستقبل يجب أن تكون الاستفادة من البيانات المستسقاة من مواد العدو التي تم الاستيلاء عليها، والكميات الهائلة من

المعلومات المتاحة للجمهور، وتبني الاستخبارات مفتوحة المصدر والبنى التحتية المفتوحة، جزءًا رئيساً من كل عملية عسكرية مستقبلًا". وبينما تتطلع الولايات المتحدة إلى المستقبل وتعمل على كيفية "تحسين" حجم عمليات مكافحة الإرهاب، فإنها تحتاج أيضًا إلى خطة أكثر تحديدًا لكيفية استخدامها ودمجها والاستفادة منها بشكل كامل من كميات البيانات الهائلة المتعلقة بالإرهاب ومكافحته التي جمعتها وصنفتها وأنشأتها على مدى العشرين عامًا الماضية. تُعد تلك الكميات الهائلة من البيانات مورداً فريد من نوعه على المستوى الاستراتيجي وإذا ما تم استغلاله بطرق ذكية واستراتيجية، فسوف يساعد الولايات المتحدة على مواصلة التعلم ونقل المعرفة عبر الأجيال، وتتبع تطورات الإرهاب المستقبلية، وتحديد الفرص الجديدة لمكافحة الإرهاب، واكتساب الكفاءة التحليلية"[39]. وعلى هذا الأساس، تعد الولايات المتحدة الدولة الرائدة الأولى في العالم التي توظف الذكاء الاصطناعي في عملياتها الخارجية نتيجة القدرات الهائلة التي تمتلكها والانفاق الكبير للأموال على الابتكار الذي يعد الأساس لهيمنتها على قاعدة المعلومات والبيانات العالمية.

ثانياً: الاتحاد الأوروبي

يمثل قانون الذكاء الاصطناعي للاتحاد الأوروبي، "الذي تم اعتماده حزيران من عام(2024)، أول إطار اوروبي متعدد الجنسيات ينظم عملية تطوير ونشر الذكاء الاصطناعي. ووفقاً للرؤية الاوروبية، فانه لإعطاء الأولوية لسلامة المستخدمين وحقوقهم الأساسية، يصنف القانون أنظمة الذكاء الاصطناعي بناءً على مستويات المخاطر المحتملة: محظورة، عالية المخاطر، محدودة المخاطر، المخاطر المتدنية. واستناداً لذلك، فعلى مستوى المخاطر التي يشكلها الذكاء الاصطناعي ، تُطبق اللوائح بشكل حازم لحماية المستخدمين. وقد حظي هذا النهج المتعلق بسلامة المستخدمين بتأييد واسع، لا بل ووُصف بأنه يدعم نهجًا "محوره الإنسان" في تنظيم الذكاء الاصطناعي. وفي سياق منع التطرف العنيف، يبرز الذكاء الاصطناعي كأداة معقدة ومتعددة الأوجه. فقد استخدمت الجماعات الإرهابية الذكاء الاصطناعي لتجنيد الأعضاء، وإنتاج ونشر الدعاية، بل وقد تستخدمه لتنفيذ الهجمات. وفي الوقت نفسه، تبنت الوكالات الحكومية في جميع أنحاء الاتحاد الأوروبي إمكانات الذكاء الاصطناعي في تعزيز التدابير الأمنية من خلال العمل الشرطوي التنبؤي، والتنبؤ بالجريمة، والتقييم الآلي للمخاطر، والتحليل الجنائي. كما أحدثت تقنيات الذكاء الاصطناعي تحولًا جذريًا في كيفية عمل أنظمة العدالة الجنائية، وتحسين الأمن، ورفع كفاءة وسرعة القضاء، فضلاً عن كونها فعّالة من حيث التكلفة، ويُنظر إليها أيضاً كوسيلة للحد من انتهاكات الحقوق والحريات"[40].

كما يعد مشروع "نظام الكشف المبكر والإنذار الفوري للمحتوى الإرهابي على الإنترنت (RED-Alert)، المموّل من الاتحاد الأوروبي، مثالًا حيوياً على مدى اهتمام الاتحاد الأوروبي في توظيف الذكاء الاصطناعي لمكافحة الإرهاب، فهي أداة تهدف إلى الكشف عن المراحل المبكرة للتطرف مع مراعاة أعلى معايير الخصوصية والأمان. اذ يستخدم(RED-Alert) في معالجة اللغة الطبيعية، وتحليل الشبكات الاجتماعية، ومعالجة الأحداث المعقدة لاسيما جمع ومعالجة وعرض وتخزين البيانات الإلكترونية المتعلقة بالجماعات الإرهابية، بما في ذلك المراحل المبكرة للتطرف بناءً على محتوى وسائل التواصل الاجتماعي. ويدعم الذكاء الاصطناعي البحث عن الكلمات المفتاحية أو المواضيع المعروفة في المحتوى الذي لم يُحدد بعد على أنه ذو صلة. فضلاً عن ذلك، يتضمن عملية إخفاء هوية البيانات وإظهارها، وتتكيف مع العمليات التنظيمية لأجهزة إنفاذ القانون، ويرى الأوروبيون بان الذكاء

الاصطناعي يعد مجالاً واعداً عند البيانات الحساسة. واختُتم مشروع(RED-Alert) في أواخر عام (2020)، اذ أشارت وكالات إنفاذ القانون المشاركة في تجربة المنصة على أنها تُقدم تحسناً ملحوظاً مقارنةً بالأدوات التي تستخدمها حالياً. ومع ذلك، من المهم الإشارة إلى أن المنصة استُخدمت فقط في مرحلة تجريبية، ومن ثم فإن قابليتها للتشغيل خارج بيئات الاختبار لا تزال غير غامضة"[41].

وعلى المستوى القانوني، "تحظر المادة 5(1)(ح) من قانون الذكاء الاصطناعي للاتحاد الأوروبي في الصفحة(52)، استخدام تقنيات التعرف البيومتري الفوري في الأماكن العامة، وذلك مراعاةً لحقوق الإنسان. ومع ذلك، تستثني المادة حالتين هامتين تحديدًا في مجال مكافحة الإرهاب. أولًا، يُسمح باستخدام هذه الأدوات لمنع "تهديد حقيقي وراهن أو تهديد حقيقي ومتوقع بوقوع هجوم إرهابي". ويُمكّن استخدام هذا النظام، الذي أثار جدلًا واسعًا، أجهزة إنفاذ القانون من تحديد هوية الأفراد من خلال مسح وتحليل ملامح الوجه، أو طريقة المشي، أو غيرها من المؤشرات البيومترية، ومقارنة هذه البيانات البيومترية بالبيانات المخزنة في قاعدة البيانات المرجعية. والجدير بالذكر أنه يمكن استخدام هذه الأنظمة دون موافقة الأفراد الخاضعين للمراقبة. ونتيجة لذلك أصدر المقرر الخاص للأمم المتحدة المعني بمكافحة الإرهاب وحقوق الإنسان تحذيرات "شديدة اللهجة" بشأن إمكانية أن يؤدي هذا النوع من المراقبة البيومترية غير المقيدة إلى تغيير جذري في الخصوصية وتقويض الثقة في العمليات الديمقراطية، مؤكدًا على أهمية الضمانات الشفافة. فضلاً عن ذلك، فإن استخدام الذكاء الاصطناعي لمراقبة وسائل التواصل الاجتماعي بحثًا عن علامات التطرف أو مؤشرات أخرى على نشاط إرهابي مُحتمل قد يُؤدي إلى استهداف الأفراد بشكل غير عادل بناءً على نشاطهم على الإنترنت. وقد يُؤدي إلى تأثير مُثبِّط، حيث يُحجم الأفراد عن التعبير عن آرائهم. ويُعدّ هذا الأمر إشكاليًا بشكل خاص في سياق مكافحة الإرهاب، اذ يصعب التمييز بين التعبير المشروع والتحريض على العنف" [42].

فعلى سبيل المثال، "يعمل مشروع البحث "نظام الرصد ومنصة نقل التطرف" (MOTRA)، الممول من الحكومة الألمانية، حاليًا على تطوير أداة رصد شاملة لتحليل البيانات المجمّعة لرصد التطورات المجتمعية المهمة.، والهدف من ذلك هو الكشف عن التغيرات في المواقف، والتي يُمكن أن تُشكّل مؤشرًا مبكرًا على النشاط الإجرامي. اذ يُمكّن الرصد المنهجي من تحديد وتصنيف الاتجاهات الجديدة بسرعة أكبر، ويُشكّل أساسًا للتنبؤات التي تُتيح وضع سياسة أمنية قائمة على الأدلة، وفعّالة في قمع التهديدات والوقاية منها. مع ذلك، لا يزال تصميم المنهجية والتكنولوجيا قيد التطوير، ولذا فإن المعلومات المتاحة محدودة. وكما تُبيّن هذه الأمثلة، يُمكن للتكنولوجيا المدعّمة بالذكاء الاصطناعي أن تُفيد في دعم المحللين لتحديد نقاط الضعف المحتملة للتطرف عبر الإنترنت. ومع ذلك، يجب التأكيد على أن التقييمات الآلية لنقاط الضعف للتطرف تُثير مخاوف أخلاقية بالغة الأهمية. فضلاً عن ذلك، يجب القول بأن التكنولوجيا لا تزال بعيدة كل البعد عن أن تُغني عن عمل خبراء الأمن المتمرّسين. وفي ضوء ذلك، من المهم الإقرار بأنه حتى لو كانت التكنولوجيا في حالة مُتقدّمة تُتيح استخدامها بثقة وموثوقية، فإن أنشطة كهذه في المجال الوقائي لا تُوفّر بالضرورة دائمًا مُبرّرًا لتدخّل جهات إنفاذ القانون"[43].

وتركيزاً لما تقدم، يعتقد الناشطون في المجال الأوروبي بانه "على الرغم من أن أدوات الذكاء الاصطناعي لم تنتشر بعد على نطاق واسع في مكافحة الإرهاب، إلا أن تطويرها اصبح يتقدم بشكل سريع. وتُرسّخ اللوائح الجديدة الصادرة

على المستوى الأوروبي إطاراً لتطوير الادوات الجديدة، وتُستخدم أساساً لأغراض التنبؤ والتحقيق في إجراءات المحاكمة. وتتسم بعض الأحكام بتساهل ملحوظ، لا سيما في سياق مكافحة الإرهاب، مما يُشكّل خطراً على حقوق الإنسان، لاسيما الحق في الخصوصية والحق في محاكمة عادلة. ورغم وجود آليات رقابية، فإن احتمالية إساءة استخدام هذه الأدوات وتطبيق هذه الاستثناءات على نطاق واسع قد يُقوّض النهج الذي يركز على الإنسان والذي يهدف القانون إلى تعزيزه.. لذلك ومع استمرار تطور أدوات الذكاء الاصطناعي وتوسعها في مجال مكافحة الإرهاب، ستتطلب فعالية اللوائح وحماية حقوق الإنسان تدقيقاً مستمراً من الحكومات"[44].

ثالثاً: الصين

أحدثت التطورات السريعة التي "شهدتها الصين في مجال الذكاء الاصطناعي تحولاً جذرياً في المشهد العالمي، مما كان له تداعيات عميقة على الأمن والاستقرار الاقتصادي والقيم الديمقراطية. فبينما يمتلك الذكاء الاصطناعي إمكانات هائلة للابتكار والكفاءة، إلا أنه في ظل الاستخدام الاستبدادي الذي تمارسه الصين، أصبح أداة للمراقبة الجماعية والرقابة والتضليل والتوسع العسكري الاقتصادي. اذ توظف الصين الذكاء الاصطناعي كسلاح لترسيخ سلطتها والتأثير على الخطاب العالمي، تكما تجبر شركات الذكاء الاصطناعي الصينية على الامتثال لأوامر الحزب الشيوعي الصيني"[45].

وفي هذا السياق،" يُعدّ استخدام الصين لتقنيات الذكاء الاصطناعي لاستهداف الاقليات من أبرز الأمثلة الموثقة على الاستبداد الخوارزمي القائم على الذكاء الاصطناعي. ففي شينجيانغ، تُستخدم أنظمة المراقبة والتنبؤ بالجريمة القائمة على الذكاء الاصطناعي لمواجهة هذه الأقليات. ومن خلال جمع كميات هائلة من البيانات، تستطيع السلطات رصد المعارضين المحتملين قبل ارتكاب أي عمل فعلي. وتُسهّل العديد من مبادرات جمع البيانات عمليات المراقبة ، بما في ذلك برنامج "العيون الحادة" للمراقبة الحضرية، ومنصة العمليات المشتركة المتكاملة التي ترصد السلوكيات التي تُعتبر مؤشراً على عدم الاستقرار الاجتماعي المحتمل. وتُقيّد شبكة المراقبة الواسعة هذه حرية مواطني الإيغور وشعورهم بالأمان، وتؤدي إلى فرض رقابة ذاتية عليهم. وقد احتجزت السلطات مواطنين من الإيغور في معسكرات إعادة تأهيل بناءً على نتائج تحليلات غامضة تعتمد على الذكاء الاصطناعي. وقد انتقد صحفيون استقصائيون ومنظمات حقوقية وبعض الحكومات الغربية والمنظمات الدولية بشدة الحكومة الصينية لمعاملتها للإيغور المسلمين. وعلى الرغم من الضغوط الدولية، بما في ذلك العقوبات الاقتصادية، لا تزال شبكة المراقبة في شينجيانغ قائمة. إن خطر تبني دول أخرى لتكنولوجيا المراقبة الصينية يثير مخاوف بشأن الاستخدام الواسع لأساليب الصين في السيطرة الاجتماعية"[46].

فضلاً عن ذلك، على الصعيد الداخلي، "طورت الصين نظام مراقبة متطورًا للغاية يعتمد على الذكاء الاصطناعي، مستخدمةً تقنيات التعرف على الوجوه، والتنبؤ بالجريمة، وتتبع البيانات البيومترية لمراقبة مواطنيها وقمع المعارضة. ويتحكم "جدار الحماية العظيم" – وهو آلية رقابة مدعومة بالذكاء الاصطناعي – في تدفق المعلومات، مُشكلاً الرأي العام ومعززًا سلطة الحزب الشيوعي الصيني. والتلاعب بحملات التضليل المدعومة بالذكاء الاصطناعي بالروايات المحلية التي تؤثر على وسائل الإعلام الدولية، دافعةً برسائل مؤيدة لبكين في حين تقمع الآراء المعارضة .أما خارج حدودها، فتمتد استراتيجية الصين في مجال الذكاء الاصطناعي إلى المجالات العسكرية والاقتصادية والجيوسياسية. ويعمل جيش التحرير الشعبي

الصيني على تطوير أنظمة حرب ذاتية التشغيل مدعومة بالذكاء الاصطناعي، وقدرات حرب إلكترونية، وأدوات تحليل استخباراتي، مما يجعل الصين لاعبًا رئيسياً في ديناميكيات الصراعات الحديثة. وفي الوقت نفسه، وظفت الصين الذكاء الاصطناعي في الاقتصاد العالمي لأتمتة الصناعة، والتحكم في سلاسل التوريد، والتلاعب بالأسواق المالية، مما رسخ مكانتها كقوة مهيمنة في قطاعات أشباه الموصلات، والمعادن الأرضية النادرة، والتمويل الرقمي. من خلال دمج الذكاء الاصطناعي في مبادرة الحزام والطريق، كما وسعت الصين نفوذها الرقمي والاقتصادي في جميع أنحاء الدول النامية، حيث قامت بتضمين بنية تحتية مدفوعة بالذكاء الاصطناعي تضمن الاعتماد طويل الأجل على التكنولوجيا الصينية"[47].

كما "تُسرّع الصين جهودها لدمج الذكاء الاصطناعي في العمليات العسكرية، ساعيةً إلى تحقيق تفوق حاسم على الولايات المتحدة في حال نشوب صراع مستقبلي في المحيط الهادئ مع منافستها الاستراتيجية، كما هو الحال في تايوان. ويقول محللون إن بكين تهدف إلى تعزيز قدرات جيش التحرير الشعبي الصيني، باستخدام الذكاء الاصطناعي لتحسين الوعي الميداني واتخاذ القرارات، مع الاستفادة من التطورات في القطاعات المدنية لتطبيقها عسكريًا عبر مسارها الراسخ للتكامل بين القطاعين المدني والعسكري. وقد حللت دراسة نشرها مركز الأمن والتكنولوجيا الناشئة بجامعة جورجتاون في سبتمبر/أيلول الماضي أكثر من 2800 عقد متعلق بالذكاء الاصطناعي لجيش التحرير الشعبي الصيني خلال الفترة(2023-2024)، كاشفةً عن مئات العقود الممنوحة لمؤسسات مدنية. وتتراوح هذه العقود بين تطوير الخوارزميات وأنظمة المركبات ذاتية القيادة. وقد فازت جامعة شنغهاي جياو تونغ وحدها بعدة عقود دفاعية متعلقة بأنظمة الذكاء الاصطناعي، من بينها عقد لتطبيق مفهوم طورته الجامعة، وهو عبارة عن "شبكات قتل" آلية، حيث يمكن للأسلحة المنتشرة في مناطق القتال البحرية التكيف مع الظروف المتغيرة. وذكرت صحيفة وول ستريت جورنال أن مشروعًا آخر تضمن نظامًا لتتبع الأهداف سريعة الحركة عبر طبقات متعددة من نماذج الذكاء الاصطناعي"[48].

المطلب الثاني: المسارات المستقبلية لتوظيف الذكاء الاصطناعي في استراتيجيات مكافحة الإرهاب

اثبتت التجربة العملية لتوظيف الذكاء الاصطناعي في الاستراتيجيات الدولية لمكافحة الإرهاب بانه بدأ يسهم اسهاماً فاعلاً في إعادة تشكيل ادراك الدول لعمليات مكافحة الإرهاب، لاسيما من خلال الانتقال من الاستجابة المعتمدة على ردة الفعل والفعل الجزئي الى الاستجابة القائمة على التنبؤ المسبق بفعل الوصول الى المعلومات بشكل كبير ورصد الأنماط الفكرية المتطرفة مما يقود الى الوصول الى النوايا المخططة قبل تحولها الى فعل واقع. وعلى الرغم مما تقدم، تثير هذه المسألة العديد من التحديات المتمثلة في الخصوصية والجوانب الأخلاقية وانتهاكات حقوق الانسان وغيرها.

وفق هذا السياق، "يتزايد إدراك إمكانية تسخير الذكاء الاصطناعي وإساءة استخدامه في الأنشطة الإرهابية، إذ بات أداةً إضافيةً في ترسانة الإرهاب لإدارة عملياته التنظيمية والتجنيد والتمويل. لذا، يجب على صانعي السياسات والمشرعين وأجهزة إنفاذ القانون والمجتمع المدني التعاون الوثيق لوضع استراتيجيات فعّالة لمواجهة إساءة استخدام الكيانات الإرهابية للذكاء الاصطناعي. وسيتطلب الأمر مزيدًا من اليقظة ومجموعة من الآليات، مثل مبادرات أصحاب المصلحة المتعددين، والتشريعات، والسياسات التي تُعزز الرقابة على منصات التواصل الاجتماعي وأدوات توليد المحتوى المدعومة بالذكاء

الاصطناعي، فضلًا عن استخدام أدوات الكشف الآلي، لرصد العمليات الإرهابية المعززة بالذكاء الاصطناعي واحتوائها"[49].

يمثل "دمج الذكاء الاصطناعي في جمع المعلومات الاستخباراتية تحولاً جوهرياً في قدرات مكافحة الإرهاب، إذ يعزز بشكل كبير القدرة على جمع ومعالجة وتحليل كميات هائلة من البيانات للكشف عن التهديدات. وقد أدى النمو المتسارع في الاتصالات الرقمية والأنشطة الإلكترونية وتزايد ترابط أنظمة المعلومات إلى توليد كميات غير مسبوقة من البيانات تتجاوز القدرات التحليلية التقليدية. مما قد يمكّن الأجهزة الأمنية من تحديد الأنماط والتهديدات المحتملة بسرعة وكفاءة وفعالية أكبر. وتحديد الارتباطات والأنماط السلوكية التي قد تغيب عن المحللين البشريين، من خلال تقنيات التعلم الخاضع للإشراف، اذ يمكن تدريب أنظمة الذكاء الاصطناعي على ملفات تعريف إرهابية معروفة ومنهجيات هجومية. ويمكن توجيه هذه الجهود لتحسين رصد التطرف عبر الإنترنت، والتجنيد، والتخطيط العملياتي للهجمات الإرهابية. وتُستخدم هذه القدرات في ما يُعرف بتحليل المشاعر، اذ يتم الاستفادة من الخوارزميات لتقييم النبرة العاطفية للاتصالات، مما قد يُشير إلى تحولات نحو النوايا الإرهابية أو الأيديولوجيات المتطرفة العنيفة. ويدعم ذلك عملية تحليل الشبكات المدعومة بالذكاء الاصطناعي من خلال رسم خرائط للهياكل التنظيمية المعقدة، مما يُساعد في تحديد العُقد الرئيسة داخل الشبكات الإرهابية والكشف عن الروابط الخفية بين الأفراد والجماعات"[50].

كما "يُعيد الذكاء الاصطناعي تشكيل البيئة المعلوماتية الامنية العالمية، والمشهد الأمني، وأساليب تواصل المجتمعات وتعبئتها وحوكمتها، بوتيرة متسارعة. وبينما يُتيح الذكاء الاصطناعي فرصًا هائلة لتعزيز جهود منع ومكافحة التطرف العنيف المؤدي إلى الإرهاب، فإنه يُستغل أيضًا بشكل فاعل من قِبل الجهات الإرهابية لتسريع إنتاج الدعاية، وتضخيم المعلومات المضللة، وتذليل العقبات أمام التخطيط العملياتي. وتؤدي هذه الرؤية الى بلورة أهمية دراسة آثار الذكاء الاصطناعي على حقوق الإنسان في مجال منع ومكافحة التطرف العنيف، بما في ذلك كيفية استغلاله لنشر خطابات تمييزية تُحفز التجنيد والتطرف المؤدي إلى العنف"[51].

وبحسب "تقرير للأمم المتحدة الذي صدر عام(2021)، اعتقد(44%) من الخبراء الذين شملهم الاستطلاع بأن استخدام الإرهابيين للذكاء الاصطناعي لأغراض خبيثة أمرٌ مرجحٌ للغاية، بينما اعتقد(56%) منهم أنه مرجحٌ إلى حدٍ ما. ولم يرَ أي خبيرٍ من بين المشاركين في الاستطلاع أن ذلك أمر مستبعد. ولتقييم المخاطر الأكثر تحديدًا المرتبطة بالنماذج منخفضة المستوى والذكاء الاصطناعي التوليدي، تجدر الإشارة إلى دراسة أجرتها لجنة الاتصالات والرقمنة في مجلس اللوردات البريطاني عام (2024). اذ شملت الدراسة مقابلات مع(41) خبيرًا، وتحليل(900) صفحة من الأدلة المكتوبة، وعقد اجتماعات مع شركاتٍ مختلفة، بما في ذلك شركات التكنولوجيا والبرمجيات. وصنّف التقرير المخاطر وفقًا للجدول الزمني، والأثر الاقتصادي، وعدد الوفيات والإصابات الناجمة عن استخدام الذكاء الاصطناعي مع النماذج منخفضة المستوى"[52].

وتحذيراً لما تقدم، يمكن للذكاء الاصطناعي أن يُغير طبيعة العمليات الإرهاب واسلوبها سواء من الذين يقومون بها أم الذين يتعرضون لها بثلاث طرق رئيسة[53]:

1: تعزيز العمليات المعلوماتية :يمكن لمنصات الذكاء الاصطناعي في مجال عمليات المعلومات أن تؤدي دورًا محوريًا في صياغة وتعزيز العمليات المعلوماتية. في العام

الماضي، أفادت مبادرة "التكنولوجيا ضد الإرهاب"، التي أطلقتها الأمم المتحدة بأن الجهات الإرهابية والمتطرفة العنيفة قد بدأت بالفعل في استخدام أدوات الذكاء الاصطناعي التوليدي لتحسين أساليبها الحالية في إنتاج ونشر الدعاية، وتشويه السرديات، والتأثير في الرأي العام. وتُعدّ تقنية التزييف العميق (Deepfakes) أحد أنواع الوسائط الاصطناعية الناتجة عن أدوات الذكاء الاصطناعي التوليدي. والتي يمكنها أن تُحاكي أشخاصًا أو أشياءً أو أحداثًا معينة، وتبدو حقيقية. مما يُسهّل الأنشطة غير القانونية والخطيرة. فعلى سبيل المثال، قامت مؤسسة إعلامية مرتبطة بتنظيم القاعدة بنشر معلومات مضللة ودعاية بدت وكأنها مُنتجة باستخدام تقنية التزييف العميق. في شباط من عام (2024)، فحصت دراسة ما يقارب (286) محتوى مُنشأ أو مُحسّن بواسطة الذكاء الاصطناعي، أنشأته أو شاركته حسابات لداعش عبر أربع منصات رئيسية للتواصل الاجتماعي. تبين بانها مواد مُعده بواسطة الذكاء الاصطناعي. اذ سمح الذكاء الاصطناعي للمؤيدين بإنشاء محتوى إبداعي وفعال، بل وتجاوز فلاتر إنستغرام وفيسبوك وأصبحوا بارعين في التحايل على قيود إنشاء المحتوى. كما طوروا مهارة عالية في تجاوز ضوابط مراقبة المحتوى على منصات التواصل الاجتماعي. وهذا يُشير بقوة إلى ضرورة تعزيز الضوابط الحالية على كل من أدوات إنشاء الصور المدعومة بالذكاء الاصطناعي ومنصات التواصل الاجتماعي.

2: التجنيد: في هذا السياق، قد يستخدم الإرهابيون أدوات الذكاء الاصطناعي لتحليل المرشحين وتحديد المجندين المحتملين الذين يستوفون معاييرهم. ويمكن استخدام أدوات الذكاء الاصطناعي التوليدية لتخصيص الرسائل والمحتوى الإعلامي للمجندين المحتملين. وأفادت دراسة للأمم المتحدة بوجود مخاوف بشأن أدوات(OpenAI) فيما يتعلق بقدراتها على "التنميط الدقيق والاستهداف الدقيق، وتوليد نصوص تلقائية لأغراض التجنيد". ووجدت الدراسة نفسها بأن الذكاء الاصطناعي قد يُستخدم في عملية استخراج البيانات لتحديد الأفراد المعرضين للتطرف، مما يُمكّن من نشر المعلومات أو الرسائل الإرهابية بدقة. فعلى سبيل المثال، قد يرسلون رسائل مُخصصة للمجندين المحتملين، مثل أولئك الذين يبحثون غالبًا عن "محتوى عنيف على الإنترنت المدعومة بالذكاء الاصطناعي. وقد تم إثبات ذلك في تجربة عندما تم "تجنيد" مُراجع تشريعات مكافحة الإرهاب في المملكة المتحدة بواسطة روبوت الدردشة.

3: التمويل: تُعنى آليات مكافحة تمويل الإرهاب بتتبع تدفق الأموال من مصادرها، سواء كانت قانونية أو غير قانونية، إلى الإرهابيين. وتشمل هذه الآليات جهات معنية متعددة، بما في ذلك برامج مكافحة غسل الأموال. ذا يُعدّ برنامج "اعرف عميلك" (KYC) أحد الأساليب القياسية التي تستخدمها المؤسسات المالية لمكافحة غسل الأموال، لا سيما عند فتح حساب مصرفي عبر الإنترنت. اذ تشترط مكالمة فيديو مباشرة للتحقق من هويته الزبون. ويمكن تزييف العملية، مما يسمح للإرهابيين بفتح حسابات وهمية وتسهيل تمويل أنشطتهم. فقد أجرى تقرير صادر عن شركة (Sensity.ai) المتخصصة في كشف الاحتيال دراسةً حول أشهر مزودي خدمات التحقق البيومتري، ووجد بأن "الغالبية العظمى منهم عُرضة بشدة لهجمات التزييف العميق". ومن ثم ، يُمكن للإرهابيين تجاوز إجراءات التحقق الأمني المدمجة في منصات "اعرف عميلك"، والتهرب من آليات مكافحة تمويل الإرهاب، ومن ثم تحويل الأموال بطرق غير مشروعة. كما استُخدمت تقنية التزييف الصوتي العميق تحويل الأموال بطرق غير مشروعة. كما يُمكن لهذه التسجيلات خداع الناس لحملهم على التخلي

عن أموالهم أو معلوماتهم الحساسة، وتحويل الأموال بطرق غير مشروعة عن طريق توليف صوت يُشبه إلى حد كبير صوت المستخدم المصرّح له. كما تُعدّ العملات المشفرة مصدرًا آخر لتمويل الإرهاب. ففي عام(2022)، أفادت بلومبيرغ أن خبيرًا قانونيًا في مكافحة الإرهاب تابعًا للأمم المتحدة قد صرّح بأنه "يتم رصد المزيد من حالات استخدام العملات المشفرة في تمويل الإرهاب ". وقد اشتبه في استخدام العملات المشفرة في تمويل تفجيرات باريس عام (2015) وسريلانك عام(2019). ويمكن للإرهابيين استغلال هذه الادوات لإجراء صفقات أكثر ربحية في العملات الرقمية، ومن ثم زيادة أرباحهم.

ويشير تحليل الدكتورة سارة لومان الى الاتي: " أن التأثيرات ستكون ذات تحولاً كبيراً. ويتطلب الإرهاب دورة مستمرة من التطرف والتجنيد وتوفير الموارد لدعم العمليات الناجحة. وهنا، يُمكن للذكاء الاصطناعي إنشاء محتوى إرهابي ومضاعفة تأثيره عندما تتفاعل البرامج الآلية وغيرها من البرامج مع البشر. كما يُمكن للإرهابيين استغلال استخدام المجتمع المدني والحكومات للذكاء الاصطناعي لمهاجمة نقاط الضعف التي لم تكن لتوجد لولا تقنيات الذكاء الاصطناعي. كما يمكن للارهابيين استخدام نماذج اللغة الكبيرة في الخدمات اللوجستية العسكرية والمدنية، مثل التلاعب بقوائم الشحن لتسهيل العمليات الإرهابية. وكما تُلاحظ لومان "إن الجهات الخبيثة، كما هو الحال مع الحكومات، تعتمد على الشركات مثل مايكروسوفت و(OpenAI) للحصول على قدرات الذكاء الاصطناعي. يؤدي ذلك إلى توسيع نطاق الجهات التي يعتمد عليها الإرهابيون للحصول على الدعم، ليشمل جهات تربطها علاقات بمكافحة الإرهاب"[54].

تؤثر "الدعاية الإلكترونية بشكل كبير في منظومة المعلومات الحالية ونقاط الضعف فيها. تتميز هذه المنظومة بسهولة الوصول إلى منصات التواصل الاجتماعي، مما يسمح لجهات مجهولة والية بنشر المحتوى الزائف أو المضلل أو شديد التحيز دون مساءلة تُذكر. اذ اكتشف معهد ماساتشوستس للتكنولوجيا عام(2018)، بأن "الكذب ينتشر على نطاق أوسع وأسرع وأعمق" من الحقيقة على تويتر، ويمكن للتضخيم أن يزيد من إدراك الأهمية في أذهان العامة. علاوة على ذلك. كما أن تضخيم القصص الضارة أو المشتتة للانتباه حول مرشح سياسي عبر "مزارع المتصيدين" يمكن أن يُغير المعلومات التي تصل إلى الجمهور. ويؤثر في النقاشات السياسية، لا سيما عندما يقترن بإخفاء الهوية والذي يقلل من إمكانية تحديد المصدر وإمكانية المساءلة[55]. فضلا عن ذلك، تُساعد نماذج التعلم الآلي (LLMs) الإرهابيين على أتمتة وترجمة الدعاية، ومعرفة كيفية ارتكاب الاعمال الاجرامية أو الانضمام إلى الجماعة المتطرفة بسرعة أكبر. ويمكن تدريب هذه النماذج على نشر خطاب الكراهية، كما حدث مع نموذج(LLaMA) التابع لشركة(Meta) على منصة(chan 4)، والذي تم توظيفه من قبل مستخدمو اليمين المتطرف بعد أسبوع واحد فقط من إطلاق(Meta) لهذا النموذج الجديد للذكاء الاصطناعي. ويمكن تدريب النموذج على إنشاء روبوتات دردشة تعمل على الترويج لخطاب الكراهية، وكراهية الأجانب، ومعاداة السامية، والسلوك العنيف، على الرغم من وجود الفلاتر المختصة بحجب خطاب الكراهية وما يتمتع به من مميزات الأمان"[56].

وعلى الرغم من "أن تطوير الذكاء الاصطناعي قد جلب فوائد وتطورات كبيرة للعديد من المجالات، إلا أنه أوجد أيضًا تهديدات اجتماعية جديدة لا بد من معالجتها. اذ تشمل هذه التهديدات انتشار المعلومات المضللة، وانتهاك الخصوصية، واحتمالية فقدان الوظائف، واستخدام الذكاء الاصطناعي في الأنشطة الإرهابية. وللحد من هذه

التهديدات، يمكن تطبيق العديد من المقترحات والحلول"، ومنها ما يلي[57]:

أولاً: تشديد الرقابة: يُعد تشديد الرقابة من أكثر الطرق فعالية للحد من التهديدات الاجتماعية التي يُشكلها الذكاء الاصطناعي. ينبغي على الحكومات والمنظمات العمل معًا لوضع مبادئ توجيهية ولوائح واضحة لتطوير الذكاء الاصطناعي واستخدامه. وهذا من شأنه أن يُساعد في منع انتشار المعلومات المضللة، وحماية خصوصية الأفراد، والحد من استخدام الذكاء الاصطناعي لأغراض خبيثة.

ثانياً: التثقيف والتوعية: من الحلول المهمة الأخرى زيادة التثقيف والتوعية بالذكاء الاصطناعي وآثاره الاجتماعية المحتملة. ويمكن تحقيق ذلك من خلال البرامج التعليمية، وحملات التوعية العامة، والتغطية الإعلامية. فمن خلال تثقيف الناس حول المخاطر والفوائد المحتملة للذكاء الاصطناعي، يُمكن للأفراد والمنظمات اتخاذ قرارات أكثر وعيًا بشأن استخدامه.

ثالثاً: الاعتبارات الأخلاقية: بالإضافة إلى ذلك، ينبغي مراعاة الاعتبارات الأخلاقية عند تطوير الذكاء الاصطناعي واستخدامه. وتشمل هذه الاعتبارات التحيز والتمييز، والشفافية والمساءلة، واحتمالية إضرار الذكاء الاصطناعي بالقيم والمصالح الإنسانية. ومن خلال إعطاء الأولوية للاعتبارات الأخلاقية، يمكن للمنظمات والأفراد العمل على ضمان تطوير الذكاء الاصطناعي واستخدامه بمسؤولية وبشكل مفيد.

رابعاً: التعاون: يُعد التعاون بين الحكومات والمنظمات والأفراد أمرًا بالغ الأهمية للحد من المخاطر الاجتماعية التي يُشكلها الذكاء الاصطناعي. فمن خلال العمل المشترك، يمكن لأصحاب المصلحة تبادل المعلومات والموارد والخبرات لتطوير حلول واستراتيجيات فعّالة لمعالجة الآثار الاجتماعية للذكاء الاصطناعي.

خامساً: تطوير التدابير المضادة: أخيرًا، من المهم تطوير تدابير مضادة للتصدي للاستخدام المحتمل للذكاء الاصطناعي في الأنشطة الإرهابية. ويشمل ذلك الاستثمار في البحث والتطوير للكشف عن استخدام الذكاء الاصطناعي لأغراض خبيثة ومنعه، بالإضافة إلى العمل على تطوير استراتيجيات استجابة فعّالة في حال وقوع هجوم إرهابي مدعوم بالذكاء الاصطناعي.

تكثيفاً لما تجذر، "كيف ستبدو عمليات مكافحة الإرهاب في عصر الذكاء الاصطناعي؟ . يمكن القول بانه لا يوجد نهج واحد يناسب الجميع في مكافحة الإرهاب، فالظروف المحلية هي التي تحدد المتطلبات، سواء أكانت تركز على مكافحة التطرف أم على التدابير المضادة العنيفة. وينطبق المنطق نفسه على مكافحة الإرهاب المدعومة بالذكاء الاصطناعي. فمن الناحية النظرية، يمكن للذكاء الاصطناعي والتعلم الآلي أن يُدمج في أي نشاط لمكافحة الإرهاب، لاسيما مكافحة التطرف، والاستخبارات، والعمليات المباشرة. وتوفير المعلومات والمعلومات المضادة"[58].

لقد "تكيّفت الحركات المتطرفة حول العالم مع النماذج الرقمية الجديدة للقرن الحادي والعشرين، وتعلموا استخدام تكنولوجيا المعلومات والاتصالات، لاسيما الفضاءات الإلكترونية والتطبيقات التفاعلية المتعددة، ومنصات التواصل الاجتماعي، لتحقيق أهدافهم المتمثلة في نشر الفكر والدعاية القائمة على التحريض، وتجنيد الاعضاء الجدد، وتوفير الدعم المالي والتكتيكات العملياتية، وإدارة المجتمعات الإلكترونية الداعمة في مناطق أخرى من العالم، اذ تلعب وسائل التواصل الاجتماعي والمحتوى المحلي المصمّم خصيصًا لتلبية المظالم المحلية والمتاح باللغات المحلية دورًا بالغ الأهمية في التطرف والتجنيد"[59]. وفي الختام، لم يعد بإمكان الفواعل الأمنية سواء الدول ام من غير الدول اهمال

الذكاء الاصطناعي بوصفه الأداة الأهم في عالم القرن الحادي والعشرين. وعلى الرغم من التحديات التي يُشكلها، فهو فرصة تقنية لا نظير لها اذا ما احسنت أجهزة الدول من استخدامه ومأسسة سلوكها في مواجهة التهديدات الارهابية التي تواجه المجتمعات، بالشكل الذي يوازن بين الامن وخصوصية الافراد وحقوق الانسان وفق الضوابط القانونية والدستورية.

الخاتمة

يعد الذكاء الاصطناعي احد الابتكارات المهمة في القرن الحادي والعشرين. فقد اسهم في تغيير عملية الاستجابة من الاستجابة التقليدية الى الاستجابة التي تتصف بقدرة كبيرة على التنبؤ بفعل الأدوات التقنية التي يوفرها في عمليات تحليل المعلومات الأمنية. اذ يتسم بتحول نوعي في تجميع المعلومات ومعالجتها بسرعة كبيرة وتوفير القدرة على التنبؤ لدى الدول وبناء الاستراتيجيات الأمنية لمواجهة التحديات التي تحاول تهديد الامن والاستقرار والتفاعلات الاقتصادية والاجتماعية فيها. وفي هذا السياق، لم يعد بإمكان الأجهزة الأمنية للدول ومؤسسات الدول لاسيما الأمنية والاقتصادية والاجتماعية التخلي عنه في عمليات جمع المعلومات عن المهددات الأمنية المسبقة واتخاذ الإجراءات الفاعلة لمواجهة التهديدات الإرهابية. كما انه مكن أجهزة الدول من معرفة أنماط السلوك المتطرفة قبل تحولها الى تهديدات إرهابية من خلال تحليل الخطابات التي تحرض على العنف وتحديد مصدرها ومعالجتها.

ترتبط عمليات توظيف الذكاء الاصطناعي بمدى التقدم التكنولوجي لدى الدول. والدول الرائدة في هذا المجال هي الولايات المتحدة والدول الأوروبية والصين. لكل دولة رؤيتها في عمليات توظيف الذكاء الاصطناعي المستندة الى طبيعة فهما وادراكها للمهددات التي تواجهها. فالولايات المتحدة لديها معاييرها المزدوجة وتعريفها الخاص بها فيما يتعلق بالإرهاب وتعمل عليه، وتعطي الاولوية للامن القومي الأمريكي على حساب جوانب حقوق الانسان، بينما يحاول الأوروبيون الموازنة المعقدة بين المتطلبات الأمنية وخصوصيات الافراد وحقوق الانسان، وهنالك العديد من الرؤى المتناقضة في هذا المجال، بينما لدى الصين رؤيتها الخاصة المستندة الى نظامها الشمولي الذي يتحكم بحركة المجتمع بجميع جوانبه، ويمثل الذكاء الاصطناعي أداة داعمة للهيمنة الشمولية التي تعطي الأولوية للأمن على حساب حماية خصوصية الافراد.

تؤكد الحقائق العلمية بان التقييم الاستراتيجي لتوظيف الذكاء الاصطناعي في العمليات الأمنية يتضمن جانبين رئيسيين لا يمكن تجاوزهما: أولهما: البعد الإيجابي المتمثل بتوفير قاعدة معلوماتية كبيرة عن حركة المجتمعات وتفاعلاتها المجتمعة والاقتصادية والأمنية، ويعمل على اجراء تحليل الي معقد للبيانات الهائلة وتقاطعها وتحديد مصادر الخطابات التحريضية ونوايا وخطط الجماعات التي تستهدف امن الدول والتنبؤ بها واتخاذ الإجراءات الأمنية قبل وقوعها. وتتمثل الجوانب الإيجابية في القدرة على التبؤية المستقبلية، وتجفيف المنابع المالية لشبكات تمويل الإرهاب، والتوظيف التكنولوجي في عمليات كشف هوية الفاعلين عن طريق الطائرات بدون طيار، وتتبع الكلمات والمفردات في الخطابات التي تحرض على العنف ومعالجتها.

ثانيهما: البعد السلبي الذي يتجسد في ان اتاحة الوصول الى بيانات جميع الافراد في أي وقت دون اذن وتخويل يؤدي الى انتهاك خصوصيات الافراد وانتهاك الحريات وحقوق الانسان التي تكفلها الأعراف والقوانين والدساتير في الدول الديمقراطية. وفق هذا السياق، فان التحدي الأهم الذي يواجه الدول في ها المجال هو كيفية الحفاظ على التوازن بين توظيف الذكاء الاصطناعي في مواجهة التهديدات الأمنية وضمان عدم انتهاك

خصوصيات الافراد وحقوق الانسان. ويتركز ذلك في صعوبة التقييم القانوني لمدى قانونية القرار الذي اتخذه الذكاء الاصطناعي بناء على الخوارزميات والمعلومات التي تم اتخاذها فيه، وهو ما يؤدي الى غياب المسألة في حالة وقوع الخطأ. والاهم من ذلك، ان الذكاء الاصطناعي يمكن لجميع الأطراف استخدامه، فهو سيكون متاحاً لأجهزة الدولة بجميع تصنيفاتها، وفي الوقت نفسه، يكون متاحاً للحركات الإرهابية التي تستهدف مؤسسات الدول ومجتمعاتها.

المصادر

[1]-Farber, S. (2025). AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security. Journal of Strategic Security, 18(3), p320.(320–344). https://www.jstor.org/stable/48838030

[2] -Anthony Pfaff and others, (2025), The Weaponization of AI: The Next Stage of Terrorism and Warfare, edited by dr. C. Anthony pfaff, Centre of Excellence Defence Against Terrorism, Ankra, p9.

[3]-Farber, S. op.cit. p320.

[4]-Ibid, p320.

[5] -Ibid,p320-320.

[6] -CNBC news Agency, AI potentially 'more dangerous than nukes,' Musk warns, 4-8-214. https://www.cnbc.com/2014/08/04/ai-potentially-more-dangerous-than-nukes-musk-warns.html?utm_source=chatgpt.com

[7] -Farber, S.op.cit,p320-320.

[8] -Nick Bostrom, (2002) Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards, the Journal of Evolution and Technology, Vol. 9, No. 1, p1.

[9]-DİNGİL, H. (2025). Reshaping National Security and the Future of Warfare in the Age of Competitive Artificial Intelligence [Review of Artificial Intelligence and the Future of Warfare: The USA, China, and Strategic Stability; Four Battlegrounds: Power in the Age of Artificial Intelligence; The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories, by J. Johnson, P. Scharre, M. Raska, & R. A. Bitzinger]. Insight Turkey, 27(2), p414. (413–421). https://www.jstor.org/stable/48829621

[10]-Clarisa Nelu, (2024), Exploitation of Generative AI by Terrorist Groups, The International Centre for Counter-Terrorism, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[11]-Major András József Uveges, (2025), Terrorist Use of Artificial Intelligence-Driven Social Media, in "The Weaponization of AI: The Next Stage of Terrorism and Warfare", edited by dr. C. anthony pfaff, Centre of Excellence Defence Against Terrorism, Ankra, p43.

[12]-Wall, C. (2025). The Ghost in the Machine: Counterterrorism in the Age of Artificial Intelligence. Studies in Conflict & Terrorism, p9. (1–27). https://doi.org/10.1080/1057610X.2025.2475850.

[13] -United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism. (2021), Countering terrorism online with artificial intelligence: An overview for law enforcement and counter-terrorism agencies in South Asia and South-East

Asia, United Nations.p24. https://www.un.org/counterterrorism/sites/default/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf

[14] -Ibid .p23.

[15]-Wall, C. op.cit, p19.

[16] -A Joint Report by UNICRI and UNCCT, (2021), Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes , United Nations Office of Counter-Terrorism, New York, p21.

[17] -United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism. (2021), op.cit, p7.

[18] -Ibid .p18.

[19] - Ibud.p24.

[20] -Tianjiao, J. (2019). The impact of military artificial intelligence on warfare. In L. Saalman (Ed.), The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives, p52. (pp. 51–53). Stockholm International Peace Research Institute. http://www.jstor.org/stable/resrep24532.15

[21]-United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. (2025, December). Protecting human rights while using artificial intelligence to counter terrorism: Position paper. Office of the United Nations High Commissioner for Human Rights, p2.
https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/un-sr-ct-ai-position-paper-dec-2025.pdf

[22] - A Joint Report by UNICRI and UNCCT, (2021), Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes , United Nations Office of Counter-Terrorism, New York, p11-12.

[23] -United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. op.cit. p2.

[24] - A Joint Report by UNICRI and UNCCT, (2021), Algorithms and terrorism: the malicious use of artificial intelligence for terrorist purposes , United Nations Office of Counter-Terrorism, New York, p11.

[25] -Clarisa Nelu, (2024), Exploitation of Generative AI by Terrorist Groups, The International Centre for Counter-Terrorism, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[26] -United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism. op.cit .p24.

[27] - Clarisa Nelu, op.cit , https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[28] - United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism. Op.cit.p26.

[29] -Cuihong, C. (2019). The shaping of strategic stability by artificial intelligence. In L. Saalman (Ed.), The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives, p54-55.(pp. 54–77). Stockholm International Peace Research Institute. http://www.jstor.org/stable/resrep24532.16

[30] -Davis, A. L. (2021). Artificial Intelligence and the Fight Against International Terrorism. American Intelligence Journal, 38(2), p67. (63–73). https://www.jstor.org/stable/27168700

[31] -Don Rassler, (2021), Commentary: Data, AI, and the Future of U.S. Counterterrorism: Building an Action Plan, in “Discordance in the Iran Threat Network in Iraq”, edited by H.R. McMaster, Combating Terrorism Center U.S. at West Point, New york, p31.

[32] -Don Rassler, op.cit, p32.

[33] -Davis, A. L. op.cit , p69.

[34] -Don Rassler, op.cit, p36.

[35]-Davis, A. L.op.cit , p64.

[36]-Ibid, p63.

[37]-Frederick, K. (2019). The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight. Center for a New American Security, p6.

http://www.jstor.org/stable/resrep20399

[38] -Ibid, p1.

[39]-Don Rassler, op.cit, p32.

[40] -Jade Briend, (2025), The EU's AI Act: Implications on Justice and Counter-Terrorism, Centre for Statecraft and National Security (CSNS), The Global Network on Extremism and Technology, King's College London, London, https://gnet-research.org/2025/03/10/the-eus-ai-act-implications-on-justice-and-counter-terrorism/,

[41] - United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism.op.cit.p26.

[42]-Jade Briend, op.cit, https://gnet-research.org/2025/03/10/the-eus-ai-act-implications-on-justice-and-counter-terrorism/,

[43] -United Nations Interregional Crime and Justice Research Institute, & United Nations Office of Counter-Terrorism. Op. cit.p27.

[44]-Jade Briend, op.cit, https://gnet-research.org/2025/03/10/the-eus-ai-act-implications-on-justice-and-counter-terrorism/,

[45] -M. Dane Waters,(2025), China's Use of AI and its Negative Impact on the World, The Henry Jackson Society, London, p5.

[46] -Rasma Kaskina and Angelina Cvetkovska, (2024), Executive summary: Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights, Brussels, European Union, p2.

[47] - M. Dane Waters,op.cit, p5.

[48]-See: How China Is Using AI To Win Future Wars, (2026), Newsweek , News Article, https://www.newsweek.com/how-china-using-ai-win-future-wars-11304436.

[49] -Asha Hemrajani,(2024, August) The Use of AI in Terrorism, RSIS Commentary, No: 124, S. Rajaratnam School of International Studies, NTU Singapore, p4.

[50] -United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. Op.cit. P4.

[51] -From Principles to Practice: Special Dialogue on Artificial Intelligence and Preventing and Countering Violent Extremism ,(2026), United Nations Headquarters, New York, p1.

[52]-Sarah Lohmann, (2025), National Security Impacts of Artificial Intelligence and Large Language Models, in "The Weaponization of AI: The Next Stage of Terrorism and Warfare", edited by dr. C. anthony pfaff, Centre of Excellence Defence Against Terrorism, Ankra, p26.

[53] -Asha Hemrajani,(2024, August) The Use of AI in Terrorism, RSIS Commentary, No: 124, S. Rajaratnam School of International Studies,op.cit, p1-4.

[54] -Sarah Lohmann, op.cit, p23.

[55]-Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). National security –related application of artificial intelligence. In Artificial Intelligence and International Security, p5. (pp. 3–13). Center for a New American Security.

http://www.jstor.org/stable/resrep20430.3

[56]-Sarah Lohmann, op.cit, p28.

[57]-Yaser Esmailzadeh and Ebrahim Motaghi, (2024), International Terrorism and Social Threats of Artificial Intelligence, Journal of Globalization Studies. Volume 15, Number 1 , p178.

[58]-Wall, C. op.cit , p8. (1–27). https://doi.org/10.1080/1057610X.2025.2475850.

[59] -A Joint Report by UNICRI and UNCCT, op.cit, p12.