



المعهد المصري للدراسات
EGYPTIAN INSTITUTE FOR STUDIES

المتوردون العالميون يستخدمون الذكاء الاصطناعي أفاق جديدة للفاعلين من خارج الدولة

ترجمة: عادل رفيق

ترجمات

19 أكتوبر 2026

YIKES



TURKEY- ISTANBUL

Bahçelievler, Yenibosna Mh 29 Ekim Cad. No: 7 A2 Blok 3. Plaza D: 64
Tel/Fax: +90 212 227 2262 E-Mail: info@eis-eg.org



WWW.EIPSS-EG.ORG

f Eipss.EG t Eis_EG

المتوردون العالميون يستخدمون الذكاء الاصطناعي.. أفاق جديدة

للفاعلين من خارج الدولة

ترجمة عادل رفيق

مقدمة

في 16 يونيو 2026، قدم [سيمون ويسلر](#)، وهو صانع محتوى ومقدم برامج بريطاني شهير في قناة [WarFronts](#) التي يبتثها على موقع يوتيوب، حلقة هامة يناقش فيها الانتشار السريع للذكاء الاصطناعي وما يُحدثه من تحول جذري ليس فقط في العمليات الحكومية والعسكرية، بل أيضاً في قدرات المجموعات المتمردة والمنظمات المرتبطة بـ "الإرهاب"، أو بالجماعات الأخرى الفاعلة خارج إطار الدولة، والتي قد تقاوم احتلالاً عسكرياً، أو أنظمة مستبدة في أماكن مختلفة من العالم.

تتناول هذه الحلقة كيف بدأت جماعات مثل فروع "تنظيم الدولة الإسلامية" وجماعة "بوكو حرام" بتجربة الذكاء الاصطناعي في إنتاج الدعاية لأنشطتها، وتجنيده عناصر جديدة، والتخطيط التكتيكي، واستكشاف أعطال الأسلحة وإصلاحها، وتطوير الطائرات المسيّرة، ونشر الروايات "المؤامراتية" الخاصة بها. ورغم أن العديد من التطبيقات المبكرة للذكاء الاصطناعي كانت بدائية أو غير فعّالة، إلا أن هذه الإخفاقات لا ينبغي أن تحجب الخطر الأكبر: فتلك الجماعات المتمردة تتعلم كيفية استخدام الذكاء الاصطناعي، والتكيف مع قيوده، وتجاوز القيود الأمنية، وتبادل التقنيات الناجحة.

ويُسلّط النقاش الذي تناولته الحلقة الضوء على التوتر المتزايد بين التطبيقات العسكرية والمدنية المشروعة للذكاء الاصطناعي، وإمكانية إساءة استخدامه من قبل جهات فاعلة غير حكومية قد تكون "عنيفة". وتزايد أهمية أنظمة الذكاء الاصطناعي التجارية في استراتيجيات الدفاع الوطني، بينما تستطيع بعض المجموعات المرتبطة بـ "الإرهاب" الوصول إلى تقنيات مماثلة عبر اشتراكات زهيدة، وحلول بديلة، وشبكات افتراضية خاصة.

وتخلص هذه الحلقة إلى أن التهديد الأكبر قد لا يكمن في سلاح واحد متطور مُولّد بواسطة الذكاء الاصطناعي، بل في التأثير التراكمي للعديد من المزايا التكنولوجية الصغيرة، على غرار: إنتاج

دعاية أسرع، وتحسين عملية صنع القرار التكتيكي، وسهولة حل المشكلات التقنية، والطائرات المسيّرة ذاتية التشغيل، والخداع المالي، وتسريع تطوير الأسلحة، وغيرها.

وقد تكون هذه "الفجوة الناشئة في مجال الذكاء الاصطناعي" مُدمرةً بشكل خاص في الدول الفقيرة التي تُعاني أصلاً من حركات التمرد. لذلك، يكمن التحدي الرئيسي في تطوير ضمانات فعّالة للذكاء الاصطناعي دون قمع الابتكار المشروع، مع ضمان ألا يؤدي التقدم التكنولوجي، دون قصد، إلى زيادة قدرات المنظمات المتمردة الخطيرة أصلاً.

نموذج كلود ودوره في القبض على مادورو

يستهل سيمون ويسلر الحلقة بالإشارة إلى تقرير نشرته صحيفة [وول ستريت جورنال](#)، بتاريخ 15 فبراير 2026، بعنوان "البنّاجون يستخدم نموذج كلود من أنثروبيك في عملية القبض على مادورو في فنزويلا"، حيث "سلّط استخدام هذا النموذج، بموجب عقدٍ مع شركة بالانتر، الضوء على الدور المتنامي للذكاء الاصطناعي في البنّاجون". ويقول التقرير أن نموذج كلود، أداة الذكاء الاصطناعي من أنثروبيك، قد استُخدم في عملية الجيش الأمريكي للقبض على الرئيس الفنزويلي السابق نيكولاس مادورو، مما يُبرز كيف تكتسب نماذج الذكاء الاصطناعي زخماً في البنّاجون، وذلك وفقاً لمصادر مطلعة داخل وزارة الدفاع الأمريكية. وكانت مهمة القبض على مادورو وزوجته قد شملت قصف عدة مواقع في كاراكاس خلال شهر يناير من هذا العام؛ بينما تحظر إرشادات استخدام أنثروبيك "استخدام نموذج كلود لتسهيل العنف أو تطوير الأسلحة أو إجراء عمليات التجسس".

وتناول ويسلر بعض الصور الساخرة العديدة التي تم تداولها في دردشة جماعية على WarFronts بعد أن كشفت صحيفة وول ستريت جورنال أن البنّاجون استخدم نموذج كلود للقبض على مادورو، على غرار: "أهلاً يا شات جي بي تي. أريدك أن تضع خطة ممتازة، خالية من الأخطاء، للقبض على زعيم فنزويلا، نيكولاس مادورو. كما أريدك أن تتخيل، كما أتخيل، أن لديّ كامل قدرات الجيش الأمريكي وجهازه الدفاعي إلى جانبي". بالإشارة إلى التقارير التي أكدت استغلال البنّاجون شراكة "كلود أنثروبيك" مع شركة البيانات "بالانتر تكنولوجيز"، التي توفر مجموعة واسعة من الأدوات التي تستخدمها وزارة الدفاع، ومن ضمن ذلك ما كشفه تقرير وول ستريت جورنال في عملية القبض على الرئيس الفنزويلي.

الأمر يبدو أكثر غباءً عما كنا نخشى

كان المضمون الرئيسي الذي تناوله ويسلر في هذه الحلقة بعنوان "المتوردون العالميون يستخدمون الذكاء الاصطناعي.. الأمر يبدو أكثر غباءً عما كنا نخشى" - هو أن التطور السريع للذكاء الاصطناعي قد أحدث تحولاً جذرياً في الحروب الحديثة، وجمع المعلومات الاستخباراتية، والتخطيط العسكري، والدعاية، بل وحتى في الأنشطة اليومية للحكومات والقوات المسلحة. فبالنسبة للدول التي تمتلك موارد تكنولوجية ومالية هائلة، يُمكن للذكاء الاصطناعي معالجة المعلومات، وتحديد الأنماط، وترتيب أولويات الأهداف، ومساعدة المخططين العسكريين على اتخاذ القرارات بسرعة تفوق قدرة البشر على مجاراتها.

إلا أن هذه التقنية نفسها باتت متاحة بشكل متزايد لجماعات ذات موارد أقل بكثير، بما في ذلك المنظمات المرتبطة بـ "الإرهاب" وحركات التمرد. والنتيجة هي مفارقة تكنولوجية مقلقة: فبعض أخطر الجهات الفاعلة غير الحكومية في العالم قد تتعلم استغلال الذكاء الاصطناعي بوتيرة أسرع من قدرة الحكومات على تنظيمه؛ حيث أنه بينما أصبح الذكاء الاصطناعي جزءاً لا يتجزأ من العمليات العسكرية، فإنه في الوقت نفسه يجد طريقه إلى أيدي المنظمات "المتطرفة" و"المتطرفة". وعلى الرغم من أن العديد من التجارب المبكرة التي أجرتها تلك الجماعات والمنظمات كانت بدائية وغير موثوقة، بل وفشلت فشلاً كبيراً في بعض الأحيان، فإن تجاهلها سيكون خطأ جسيماً، باعتبار أن التكنولوجيا تتطور بسرعة، وأن تلك المنظمات التي تستخدمها تتعلم من إخفاقاتها.

لذلك، تتجاوز المسألة مجرد مشهد طريف حيث يتلقى المتوردون نصائح خاطئة من برامج الدردشة الآلية. فالذكاء الاصطناعي في نهاية المطاف يتيح لجماعات صغيرة نسبياً اكتساب قدرات كانت تتطلب سابقاً خبرات تقنية متطورة، أو منظمات ضخمة، أو موارد مالية هائلة. وقد يُساعدهم كذلك في الدعاية، وتجنيد الأنصار، وصيانة الأسلحة، والتخطيط التكتيكي، وتطوير الطائرات المسيّرة، والاحتيايل المالي، وربما تصميم أسلحة أكثر تطوراً. وفي الوقت نفسه، تواجه الحكومات معضلةً صعبة: فالقيود المشددة قد تُقلل الخطر، لكن الإفراط في التنظيم قد يُبطئ البحث العلمي المشروع ويُؤدي إلى تخلف الدول عن منافسيها الجيوسياسيين.

الذكاء الاصطناعي كأداة عسكرية

يقول ويسلر في تقريره إن الأهمية المتزايدة للذكاء الاصطناعي برزت بشكل خاص عندما ظهرت تقارير تفيد بأن البنتاجون استخدم نظام "كلود" للذكاء الاصطناعي التابع لشركة "أنثروبيك" في عملية القبض على الرئيس الفنزويلي نيكولاس مادورو. ولا يزال الدور الدقيق الذي لعبه هذا النظام غير واضح، ولم يكشف البنتاجون ولا شركة "أنثروبيك" علناً عن معلومات تفصيلية حول كيفية استخدام "كلود". ومع ذلك، أوضحت هذه الحادثة مدى توغل أنظمة الذكاء الاصطناعي في المؤسسات الحكومية والعسكرية.

ولا تقتصر علاقة البنتاجون بالذكاء الاصطناعي على عملية واحدة كهذه؛ فمن خلال شراكات مع شركات مثل "بالانتر تكنولوجيز"، يتم دمج الأنظمة المدعومة بالذكاء الاصطناعي بشكل متزايد في سير العمل العسكري والاستخباراتي. وقبل الحرب على إيران، كما ذكر في الحلقة، أفادت التقارير أن واشنطن استخدمت الذكاء الاصطناعي للمساعدة في اختيار الأهداف، وتحديد مواقعها بدقة، وترتيب أولوياتها وفقاً لأهميتها. وبعد وقوع الضربات، كان بالإمكان أيضاً استخدام أنظمة الذكاء الاصطناعي لتقييم فعاليتها والمساعدة في تحديد كيفية تنفيذ الهجمات اللاحقة.

وبالنسبة للمخططين العسكريين، تُعد هذه قدرة جذابة بشكل كبير. فالحروب الحديثة أصبحت تُنتج كميات هائلة من المعلومات: صور الأقمار الصناعية، ولقطات الطائرات المسيّرة، وبيانات الاتصالات، وتقارير الاستخبارات، والخرائط، والمعلومات اللوجستية، وملاحظات ساحة المعركة. وفي الوقت الذي قد يُصاب المحللون البشريون فيه بالإرهاق من هذا الكم الهائل من الجهد، فإن الذكاء الاصطناعي يبشّر بمعالجة هذه المعلومات بسرعة وتحديد العلاقات أو الأنماط التي قد تغيب عنهم.

لكن هذه السهولة نفسها تشكّل مشكلة أمنية كبيرة في حد ذاتها. فأنظمة الذكاء الاصطناعي المفيدة للحكومات قد تكون مفيدة أيضاً لأعدائها. والفرق يكمن في أن الحكومات تمتلك الموارد اللازمة لتطوير ذكاء اصطناعي عسكري متطور، بينما تستطيع الجماعات المسلحة الوصول بشكل متزايد إلى أنظمة الذكاء الاصطناعي التجارية بتكلفة زهيدة نسبياً. فالمنظمات المرتبطة بـ "الإرهاب" ليست بالضرورة بحاجة إلى بناء نماذج ذكاء اصطناعي خاصة بها، بل يمكنها ببساطة استغلال الأنظمة التجارية المتاحة وإيجاد طرق للالتفاف على قيودها.

الذكاء الاصطناعي بيد التنظيمات

كان أحد أوائل الأمثلة الواضحة على قيام التنظيمات المرتبطة بـ "الإرهاب" بتجربة الذكاء الاصطناعي التوليدي ما حدث بعد الهجوم الإرهابي الذي وقع في مارس 2024 على مبنى بلدية كروكوس بالقرب من موسكو. فبعد أيام قليلة من الهجوم، بدأ حساب موالٍ لتنظيم الدولة الإسلامية بنشر نشرات إخبارية مُولّدة بالذكاء الاصطناعي عبر منصة Rocket Chat، وهي منصة اتصالات لامركزية استخدمها أنصار التنظيم لسنوات.

كان الهدف الظاهر هو إنشاء ما يشبه بثاً إخبارياً احترافياً. إلا أن النتائج كانت رديئة للغاية. لم تتطابق الصور مع الأحداث الموصوفة، بل إن بعض اللقطات كانت قد نُشرت قبل سنوات. وبدلاً من إظهار حرب معلوماتية متطورة، كشفت مقاطع الفيديو عن قصور المستخدمين عديدي الخبرة الذين كانوا في طور التجربة لأدوات التكنولوجيا الجديدة.

كما ظهرت محاولة مماثلة لاحقاً لدى فرع تنظيم الدولة الإسلامية في خراسان (ISKP)، وهو فرع ينشط بشكل أساسي في أفغانستان ومنطقة آسيا الوسطى والجنوبية الأوسع. وبحسب التقارير، قام التنظيم، تحت اسم "تلفزيون خراسان"، بتجربة مُقدمين ومواد فيديو مُولّدة بالذكاء الاصطناعي. ومرة أخرى، كانت النتائج مخيبة للآمال. فقد وصفت التقارير مقاطع فيديو لم يتطابق فيها الكلام مع الإيماءات بشكل صحيح، مما أعطى انطباعاً واضحاً بأنها وسائط اصطناعية.

ومع ذلك، واصل تنظيم الدولة الإسلامية في خراسان تجاربه على هذه التقنية. بل إنه طور دورات تدريبية لتأهيل المجندين على إنتاج مواد بلغات إضافية، منها الأردية والفارسية. وكانت ردود فعل المؤيدين بحد ذاتها كاشفة. حيث لم يكن بعضهم مهتماً بالدرجة الأولى بالجودة التقنية للفيديوهات، بل تساءلوا عما إذا كان استخدام الذكاء الاصطناعي التوليدي متوافقاً مع معتقداتهم الدينية. ورداً على ذلك، حاول التنظيم تعديل عروضه التقديمية المُولّدة بالذكاء الاصطناعي عن طريق طمس وجوه مقدمي العروض الرقمية.

وأظهر هذا الجدل أمراً هاماً حول تلك المنظمات "المتطرفة": أن تبني التكنولوجيا لا يحدث بمعزل عن سياق الأيديولوجية، بل يجب تكييف التقنيات الجديدة مع البيئة الأيديولوجية والثقافية والتنظيمية للجماعة التي تستخدمها. لم تقتصر تجارب تنظيم الدولة الإسلامية على الفيديوهات فحسب، فقد نشرت منشورته "صوت

خراسان" مواداً تصف الذكاء الاصطناعي بأنه واجب ديني، ثم تراجعت عن هذا الادعاء بعد أن سخرت منه منظمات جهادية أخرى. وناقشت مقالة أخرى استخدامات يُفترض أنها جائزة للذكاء الاصطناعي، بما في ذلك توليد أفكار تجارية. ولم تكن هذه الحادثة ثورة تكنولوجية، لكنها أظهرت أن تلك المنظمات كانت تستكشف بنشاط ما يمكن أن يقدمه لها الذكاء الاصطناعي.

الذكاء الاصطناعي في الميدان

أكثر الأمثلة إثارة للقلق بشأن تحول النصائح التي يقدمها الذكاء الاصطناعي إلى تجربة ميدانية هي تلك التي وردت في التقرير الذي قدمه سيمون ويسلر تتعلّق بجماعة بوكو حرام وهجومها على منشأة عسكرية في شرق نيجيريا. فوفقاً لبحثٍ استشهد به ويسلر، واجه مقاتلو بوكو حرام خندقاً دفاعياً يُحيط بهدفهم. وبدلاً من التخلي عن الهجوم ببساطة، استشار أعضاء الجماعة أنظمة الذكاء الاصطناعي، حيث زوّدها بمعلوماتٍ حول دراجاتهم النارية والمسافة التي يحتاجون إلى قطعها.

وقد ساهمت النصائح المؤلّدة بواسطة الذكاء الاصطناعي في برنامج تدريبي غريب؛ حيث قام ميكانيكيو بوكو حرام بتعديل الدراجات النارية لتحسين تسارعها وسرعتها القصوى، ثمّ قام المقاتلون بإنشاء عوائق تدريبية تتكوّن من حفرة مملوءة بالنار والزجاج المكسور، وحاولوا القفز فوقها. وكانت النتائج كارثية، حيث لقي ثمانية عشر مقاتلاً حتفهم خلال محاولات التدريب.

للوهلة الأولى، يبدو أن هذه الحادثة تُثبت أن الذكاء الاصطناعي لا يُعني عن الخبرة البشرية. لم يُدرك برنامج الدردشة الآلي عواقب الخطة على أرض الواقع، ودفع المسلحون ثمناً باهظاً لاتباعها. ولكن هذا تحديداً هو السبب الذي يجعل هذه الحادثة لا ينبغي التعامل معها على أنها مجرد مزحة. فعلى الرغم من الخسائر الفادحة، تمكن بعض المقاتلين في نهاية المطاف من إتقان المناورة وتدريب الآخرين عليها. ونجحت المجموعة لاحقاً في مهاجمة القاعدة العسكرية.

لذا، فإن الدرس المستفاد يبدو أكثر تعقيداً من مجرد "تقديم الذكاء الاصطناعي نصائح خاطئة مثل هذه المجموعات" الإرهابية". فقد ساهم الذكاء الاصطناعي في عملية تعلم متكررة. حيث جرب المسلحون، وتكبدوا خسائر، وتكيفوا، حتى توصلوا في النهاية إلى أسلوب ناجح.

ويُعد هذا النمط بالغ الأهمية عند التفكير في الذكاء الاصطناعي وتنظيمات التمرد. فتللك المنظمات لا تحتاج بالضرورة إلى إجابات مثالية من الذكاء الاصطناعي، بل قد تحتاج فقط إلى أنظمة تقدم اقتراحات مفيدة، أو تفسيرات تقنية، أو مناهج بديلة، أو معلومات تُسرّع من عملية تعلمها.

من الأرقام إلى التكتيكات

بدأ الذكاء الاصطناعي يؤثر أيضاً على طريقة تفكير بعض الجماعات المسلحة في التكتيكات العسكرية. فقد وصف أحد المقاتلين السابقين كيف شنت مجموعته هجوماً باستخدام نحو 200 مقاتل لمجرد امتلاكها هذا العدد. وكانت النتيجة كارثية، حيث قُتل نحو 60 مقاتلاً. ووفقاً للرواية، ساعد التحليل المدعوم بالذكاء الاصطناعي المقاتلين على إدراك أن زيادة عدد الأفراد لا تضمن بالضرورة تنفيذ هجوم أكثر فعالية. ففي بعض الأحيان، تستطيع الوحدات الأصغر حجماً والأكثر تنسيقاً تحقيق نتائج أفضل مع تعريض عدد أقل من الأفراد للخطر. ويُقال إن الدرس المستفاد من ذلك هو أن عملية تضم 20 مقاتلاً منسقاً جيداً قد تكون أكثر فعالية من عملية تضم 200 مقاتل غير منسقين.

ويمثل هذا تحولاً مفاهيمياً هاماً. فليس بالضرورة أن يتكرر الذكاء الاصطناعي تكتيكاً عسكرياً جديداً كلياً ليكون مفيداً. بل يمكنه أيضاً تحسين عملية صنع القرار من خلال مساعدة القادة عديدي الخبرة على تنظيم المعلومات ومقارنة الخيارات.

وقد يكون هذا ذا قيمة خاصة للجماعات المسلحة لأن العديد منها يفتقر إلى التعليم العسكري الرسمي. ويمكن أن يعمل برنامج الدردشة الآلي كمصدر سهل الوصول إليه للحصول على توضيحات، مع أن نصائحه تبقى غير موثوقة ويجب التعامل معها بحذر شديد.

كما ورد في التقرير استخدام الذكاء الاصطناعي لمساعدة المقاتلين في تشخيص أعطال الأسلحة، وإصلاح البنادق المعطلة، والحصول على معلومات تقنية حول الأسلحة والمتفجرات. ثم تُشارك بعض هذه المعلومات داخل الشبكات المتطرفة. وهذا يخلق تأثيراً مضاعفاً خطيراً؛ فبدلاً من أن يقوم شخص واحد ذو معرفة تقنية بتعليم عدد قليل من الآخرين، يمكن توزيع المعلومات على مئات أو آلاف الأشخاص.

الدعاية والأسلحة

قد تكون الدعاية أهم من الأسلحة في بعض الأوقات. ولذلك، فقد لا يرتبط الاستخدام الأكثر أهمية للذكاء الاصطناعي بالأسلحة فقط، فلطالما اعتمدت المنظمات "المتطرفة" على الدعاية؛ فقدرتها على التجنيد والترهيب ونشر الرسائل الأيديولوجية والتأثير على الرأي العام لا تقل أهمية عن قدرتها المادية على شنّ الهجمات.

ويُخفّض الذكاء الاصطناعي التوليدي تكلفة إنتاج الدعاية بشكل كبير؛ إذ يمكن لمنظمة صغيرة نظرياً إنشاء مقاطع فيديو وصور ومقالات وترجمات وتسجيلات صوتية وتقارير إخبارية زائفة دون الحاجة إلى إدارة إعلامية احترافية ضخمة. كما يُمكن للذكاء الاصطناعي المساعدة في تكييف الرسائل لتناسب مختلف الجماهير واللغات. والأكثر إثارة للقلق هو الدعاية التي لا تدعو صراحةً إلى ممارسة "الإرهاب".

ويمكن للجماعات المتمردة إنتاج مواد مصممة لزيادة انعدام الثقة بالحكومات، وتأجيج الانقسامات الاجتماعية القائمة، والترويج لنظريات المؤامرة، واستغلال المخاوف دون الدعوة المباشرة إلى العنف. وقد يصعب على السلطات ومنصات التواصل الاجتماعي تحديد هذا المحتوى لأنه قد يبدو كتعليق سياسي عادي وليس كدعاية "متطرفة". ويجعل الذكاء الاصطناعي هذه الاستراتيجية أكثر فعالية، إذ يُمكن توليد المحتوى بسرعة كبيرة وتخصيصه لجماهير مختلفة. والهدف ليس بالضرورة إقناع الجميع بأيديولوجية معينة. فقد يكون الهدف ببساطة هو زرع عدم الثقة بالمؤسسات، والتشكيك في المعلومات الموثوقة لدى الجموع، وزيادة العداء بين الناس. ففي مجتمع مستقطب، قد يكون لذلك الفعل آثار مدمرة للغاية.

الساحل وإمكانية ظهور حركات تمرد مدعومة بالذكاء الاصطناعي

لا تقتصر هذه الظاهرة على شبكات تنظيم الدولة الإسلامية أو غرب أفريقيا. فقد درس المحللون أيضاً جماعة نصرة الإسلام والمسلمين (JNIM)، وهي منظمة مرتبطة بتنظيم القاعدة وتنشط في منطقة الساحل الأفريقي. وقد أظهرت الجماعة قدرات متطورة بشكل متزايد في استخدام الطائرات المسيّرة، وتواردت تقارير أنها وجدت طرقاً للتحايل على قيود الشركات المصنعة.

وقد بحث المحللون فيما إذا كان الذكاء الاصطناعي يُسهم في هذه التحسينات. وإذا كان الأمر كذلك، فقد يُفسر ذلك بعض النجاحات الميدانية الأخيرة لجماعة نصرة الإسلام والمسلمين، بما في ذلك العمليات المنسقة التي نُفذت بالتعاون مع جبهة تحرير أزواد (ALF) في مالي.

ومع ذلك، فمن المهم التمييز بين الأدلة المؤكدة والتكهنات. فمن المحتمل أن يُسهم الذكاء الاصطناعي في تطوير الطائرات المسيّرة والتخطيط لها وتكييفها، ولكن لا ينبغي أن يُعزى كل تحسن تكنولوجي تُحرزه منظمة متمردة تلقائياً إلى الذكاء الاصطناعي.

ومع ذلك، فإن هذا الاحتمال ذو أهمية بالغة لأن الطائرات المسيّرة التجارية منخفضة التكلفة قد أحدثت بالفعل تحولاً جذرياً في الحروب. وقد يؤدي دمج الطائرات المسيّرة مع الذكاء الاصطناعي ذي القدرات المتزايدة إلى قفزة تكنولوجية هائلة أخرى.

الذكاء الاصطناعي و"الإرهاب" في الغرب

لا يقتصر خطر استغلال الذكاء الاصطناعي على ساحات المعارك في أفريقيا والشرق الأوسط. فقد وجد الباحثون أدلة على أن أنصار تنظيم الدولة الإسلامية في الولايات المتحدة وأوروبا الغربية قد استفسروا من روبوتات الدردشة التي تعمل بالذكاء الاصطناعي عن أهداف محتملة وأساليب ممكنة لتنفيذ الهجمات. في الواقع، قد يصبح الذكاء الاصطناعي بمثابة دليل رقمي للتنظيمات "الإرهابية"، مع أنه، على عكس الوثائق الثابتة، قادر على التفاعل مع الأسئلة وتكييف المعلومات وفقاً لاحتياجات المستخدم.

وقد نجحت السلطات حتى الآن في التدخل في عدة حالات قبل إتمام الهجمات. ومن الأمثلة التي ذُكرت في النقاش، قيام السلطات الفرنسية باعتقال رجل تونسي للاشتباه في استخدامه الذكاء الاصطناعي للمساعدة في التخطيط لهجوم على متحف أو موقع يهودي في باريس. قد يكون إحباط مثل هذه الهجمات أمراً مُشجعاً، ولكنه يُسلط الضوء أيضاً على المشكلة الأساسية؛ إذ يجب على أجهزة مكافحة الإرهاب تحديد الأنشطة الخطيرة قبل تنفيذها. ومع ازدياد قدرات الذكاء الاصطناعي وسهولة الوصول إليه، قد يضطر المحققون إلى مراقبة عدد هائل من التفاعلات والتمييز بين التخطيط الخبيث الحقيقي والأسئلة المشروعة، والبحوث الأكاديمية، وكتابة القصص الخيالية، أو الفضول البريء. وهذه بالتأكيد مشكلة معقدة.

التنظيمات وضوابط الذكاء الاصطناعي

يتساءل ويسلر إذا كانت شركات الذكاء الاصطناعي التجارية تحظر المساعدة في "الإرهاب" والأسلحة والهجمات العنيفة، فكيف تتمكن تلك المنظمات المتطرفة من استخدام أنظمة الذكاء الاصطناعي؟ إحدى الإجابات على مثل هذه التساؤلات هي أنهم يبحثون بنشاط عن حلول بديلة؛ حيث تشير بعض الدراسات التي أشار إليها ويسلر في الحلقة إلى أن المدربين الأجانب زودوا قادة بوكو حرام بأجهزة الكمبيوتر المحمولة، والشبكات الافتراضية الخاصة، واشتراكات الذكاء الاصطناعي المدفوعة، وتعليمات حول كيفية إخفاء الطلبات الخطيرة.

فبدلاً من طرح معلومات محظورة بشكل علني، يمكن للمستخدمين صياغة الأسئلة في شكل تمارين أكاديمية، أو سيناريوهات خيالية، أو إشارات إلى أفلام. وإذا رفض أحد برامج الدردشة الآلية الاستجابة لطلباتهم، فإنه ينتقل ببساطة إلى برنامج آخر. وقد أدى هذا إلى خلق ما يمكن وصفه بأنه نهج لا يعتمد على النظام الأساسي، فلم يكن الهدف هو الولاء لمزود معين للذكاء الاصطناعي، لكن كان الأمر ببساطة هو العثور على نظام يجيب على التساؤلات.

ووفقاً لتلك الأبحاث، فقد قامت الفصائل المرتبطة بـ "بوكو حرام" في نهاية المطاف بتطوير وحدات مخصصة للذكاء الاصطناعي، وتم تكليف الأعضاء الموثوق بهم بمسؤولية الحفاظ على الاشتراكات والاستجابة لطلبات الأعضاء الآخرين. وشمل دورهم مواكبة الأساليب الجديدة للتحايل على قيود سلامة الذكاء الاصطناعي.

وهذا تطور بالغ الأهمية لأنه يمثل التعلم المؤسسي، حيث لم تعد المجموعة تعتمد على المقاتلين الأفراد الذين يقومون بإجراء تجارب عشوائية على روبوتات الدردشة. لقد كانت تعمل على تطوير قدرة داخلية مخصصة لاستغلال الذكاء الاصطناعي. ولم تمتد الدراسة التي وثقت هذه الممارسات إلا حتى نهاية عام 2024. ومنذ ذلك الحين، أصبحت أنظمة الذكاء الاصطناعي أكثر قوة إلى حد كبير.

حواجز السلامة للذكاء الاصطناعي

استثمرت شركات الذكاء الاصطناعي بكثافة في تحسين آليات الأمان الخاصة بها. ومع ذلك، لا يزال الباحثون المستقلون يكتشفون نقاط ضعف في تلك الأنظمة. فقد ذكرت إحدى الدراسات التي أشار إليها ويسلر إلى أن بعض التوجيهات الخطيرة قد تتجاوز أنظمة الأمان بمجرد إعادة صياغتها؛ حيث أظهر الباحثون أن تغيير بنية الطلب –

على سبيل المثال، تحويله إلى قصيدة – قد يدفع بعض الأنظمة إلى الاستجابة لطلبات كان من الممكن رفضها لولا ذلك.

وعلى الرغم من أن الشركات عملت لاحقاً على معالجة هذه الثغرات، إلا أن الدرس الأهم يبقى قائماً، وهو أن أنظمة الأمان ليست ثابتة. ففي كل مرة يُغلق فيها المطورون ثغرة، يمكن للمستخدمين البحث عن ثغرة أخرى. حيث أفاد تقرير صادر عن منظمة التكنولوجيا ضد الإرهاب (Tech Against Terrorism) باختبار أنظمة الذكاء الاصطناعي باستخدام توجيهات مبنية على سيناريوهات إرهابية واقعية. حيث رفضت الأنظمة الإجابة على حوالي 57% فقط من التوجيهات بشكل إجمالي.

وكانت نسبة الرفض أعلى بالنسبة للأسئلة المتعلقة بالمتفجرات، حيث بلغت حوالي 80%، لكنها كانت أقل بكثير بالنسبة للأسئلة المتعلقة بالأسلحة الكيميائية المرتجلة. وحتى دون الخوض في التفاصيل التقنية لهذه المواضيع الخطيرة، فإن النتيجة مثيرة للقلق، حيث: أمان الذكاء الاصطناعي ليس موثقاً به تماماً بعد.

وتزداد المشكلة تعقيداً بسبب طبيعة المنافسة الشديدة في صناعة الذكاء الاصطناعي. حيث تتسابق الشركات لتطوير أنظمة أكثر كفاءة، وجذب العملاء، والمنافسة دولياً. وقد تُصبح إجراءات السلامة جزءاً آخر من هذا السباق التنافسي، ولكن يبقى الضغط قائماً دائماً لجعل النماذج أكثر فائدة وأقل تقييداً.

جيل المتمردين القادم

تكمن أخطر الاحتمالات في الجيل القادم من المتمردين المدعومين بالذكاء الاصطناعي؛ فقد حذر المحللون من أن الذكاء الاصطناعي قد يُسهّل تمويل الإرهاب من خلال تسهيل الاحتيال والخداع والتلاعب. كما قد يُساعد الذكاء الاصطناعي الجماعات التي تُجري تجارب على الطباعة ثلاثية الأبعاد، ومكونات الطائرات المسيّرة، وقطع الغيار، وغيرها من المعدات.

ويُثير هذا احتمال مستقبل تستخدم فيه منظمة متمردة الذكاء الاصطناعي لتصميم مكون، ثم تقوم ورشة عمل آلية صغيرة بتصنيعه، ليتم دمج المعدات الناتجة في طائرة مسيّرة أو نظام آخر. ويمثل هذا السيناريو انخفاضاً كبيراً في الحواجز التكنولوجية التي تواجه الجهات الفاعلة غير الحكومية.

وهناك أيضاً قلق بشأن الأسلحة الكيميائية والبيولوجية. فقد أفاد باحثون بأن بعض المتمردين أبدوا اهتماماً بأسلحة تُسبب خسائر بشرية فادحة. وبالتأكيد لا يعني هذا أن الأسلحة الكيميائية أو البيولوجية المتطورة ستظهر قريباً في كل صراع بين المتمردين، فتطوير مثل هذه الأسلحة يتطلب أكثر بكثير من مجرد طرح سؤال على برنامج دردشة آلي. لكن الجمع بين الذكاء الاصطناعي المتاح، والمعلومات عبر الإنترنت، وتقنيات التصنيع منخفضة التكلفة، والطائرات المسيّرة، والبرمجيات المتطورة باستمرار، قد يُقلل تدريجياً من الحواجز التي حمت المجتمعات تاريخياً من أنواع معينة من الهجمات. ومثل هذا الاحتمال يستحق اهتماماً جاداً في هذا السياق.

هل بإمكان الحكومات إيقاف ذلك؟

يقول ويسلر إنه في هذه المرحلة، يتبادر إلى الذهن سؤال بديهي: لماذا لا تقوم الحكومات بإجبار شركات الذكاء الاصطناعي ببساطة على جعل أنظمتها تمتنع عن توفير معلومات خطيرة؟ والجواب ببساطة أيضاً هو أن المشكلة أعقد من ذلك بكثير. حيث لا تستطيع الحكومات السيطرة الكاملة على المعلومات الموجودة على الإنترنت.

إن معظم المعارف المتعلقة بالأسلحة والهندسة والكيمياء والطب والحوسبة والتكنولوجيا العسكرية ذات استخدام مزدوج بطبيعتها. فالمعلومات التي قد تفيد شخصاً "إرهابياً" قد تفيد أيضاً مهندساً أو باحثاً أو طبيباً أو مُصنّعاً أو طالباً شرعياً. وإذا أصبحت القيود مفرطة، فقد يلجأ المستخدمون الشرعيون إلى أنظمة أقل خضوعاً للرقابة.

وهناك أيضاً مشكلة تتمثل في المنافسة الدولية. حيث تنظر الحكومات بشكل متزايد إلى الذكاء الاصطناعي كتقنية استراتيجية تُضاهي الأجيال السابقة من التكنولوجيا العسكرية. فإذا أبطأت دولة ما تطويره بينما سارعت أخرى في ذلك، فإن الدولة الأولى تُخاطر بالتخلف اقتصادياً وعسكرياً؛ وهذا يُحفز بقوة على مواصلة الاستثمار في تطوير إمكانات الذكاء الاصطناعي.

سباق الذكاء الاصطناعي العسكري

تُعد الولايات المتحدة من أكبر المشاركين في سباق الذكاء الاصطناعي العسكري. ويشير التقرير الذي قدمه ويسلر إلى طلب البنتاجون ما يقارب 54 مليار دولار لأنظمة مستقلة تعمل بالذكاء الاصطناعي. ويظهر هذا الإنفاق مدى تجاوز الذكاء الاصطناعي العسكري مرحلة التجريب ودخوله حيز التخطيط الاستراتيجي.

لكن هناك مفارقة واضحة، فالشركات التي تُطوّر أنظمة ذكاء اصطناعي متطورة للحكومات غالباً ما تكون هي نفسها الشركات التي يُمكن للأفراد حول العالم، بمن فيهم ذوو النوايا الخبيثة، الوصول إلى منتجاتها التجارية. ومع تحسين الشركات لنماذجها، قد تُزوّد خصومها، دون قصد، بأدوات أكثر قوة.

والولايات المتحدة ليست وحدها في هذا الشأن. فقد أدمجت الصين الذكاء الاصطناعي في استراتيجيتها للتحديث العسكري، بما في ذلك تطبيقات تطوير الأسلحة، والتصنيع، وأنظمة القيادة. كما أولت روسيا اهتماماً بالغاً بالذكاء الاصطناعي. وكان الرئيس الروسي فلاديمير بوتين قد جادل بأن الدولة التي تُسرّع في تبني الذكاء الاصطناعي في الشؤون العسكرية ستحقق مزايا هائلة في ساحة المعركة. وناقش مسؤولون دفاعيون روس الذكاء الاصطناعي، والروبوتات، وأنظمة القيادة الآلية، والطائرات المسيّرة، باعتبارها مكونات أساسية للتحديث العسكري.

وبالمثل، أنشأت الهند أيضاً مؤسسات متخصصة في الذكاء الاصطناعي العسكري، وطوّرت نيودلهي، بحسب التقارير، عشرات المنتجات الدفاعية القائمة على الذكاء الاصطناعي، بما في ذلك أنظمة الروبوتات ذاتية التشغيل، والأمن السيبراني، والمراقبة. والمحصلة النهائية هي سباق تسلح عالمي في مجال الذكاء الاصطناعي، وهذا ما يجعل التنظيم الدولي الشامل في هذا الشأن أمراً بالغ الصعوبة.

الفجوة في الذكاء الاصطناعي

قد تكون العواقب وخيمة بشكل خاص في الدول الفقيرة؛ حيث تندلع العديد من حركات التمرد في مناطق تعاني حكوماتها أصلاً من محدودية الموارد، وضعف المؤسسات، ونقص القدرات الاستخباراتية، وصعوبة التضاريس. وقد تجد هذه الحكومات صعوبة في مواكبة التنظيمات "الإرهابية" حتى بدون الذكاء الاصطناعي.

أما الآن، فإنها أصبحت تواجه خصوماً قادرين على الوصول إلى تكنولوجيا تجارية متطورة دون الحاجة إلى تطويرها بأنفسهم. ويخلق هذا ما يسميه الباحثون "فجوة الذكاء الاصطناعي" بين الدول الغنية في الشمال العالمي والدول الفقيرة في الجنوب العالمي.

ويكمن الخطر في أن هذه الفجوة قد لا تقتصر على فصل الحكومات عن بعضها البعض، بل قد تفصلها أيضاً عن الجماعات المتمردة العاملة داخل حدودها. وقد تفتقر الحكومة إلى المال اللازم لبناء أنظمة ذكاء اصطناعي متطورة،

بينما تستطيع منظمة "إرهابية" شراء اشتراكات في أدوات تجارية واستخدامها على الفور. وهذا أحد أكثر جوانب المشكلة إثارة للقلق.

لطالما تطلّب التفوق التكنولوجي بنية تحتية ضخمة، بينما من المحتمل أن يقلّل الذكاء الاصطناعي من هذه المتطلبات. فقد تتمكن منظمة صغيرة تضمّ عدداً قليلاً من الأعضاء ذوي المهارات التقنية من استغلال أدوات طوّرتها شركات تُقدّر قيمتها بمليارات الدولارات.

المفارقة الكبرى

تقدّم هذه المسألة في جوهرها مفارقة عميقة؛ فقد أصبح الذكاء الاصطناعي من أهم التقنيات للأمن القومي، حيث تستثمر الحكومات مبالغ طائلة لجعل جيوشها أكثر ذكاءً وسرعةً واستقلالية. وفي الوقت نفسه، تتعلم المنظمات المرتبطة بـ "الإرهاب" والمتمرتدة كيفية استغلال هذه الثورة التكنولوجية.

ويؤكد ويسلر أنه غالباً ما تكون النماذج الأولى في الاستفادة من الذكاء الاصطناعي مثيرة للسخرية. وقد تحتوي الدعاية المؤلّدة بالذكاء الاصطناعي على صور قديمة تم تداولها من قبل. وقد يستخدم مقدمو البرامج الرقمية إيماءات غير طبيعية وغير متسقة. وقد تُوصي برامج الدردشة الآلية بتكتيكات قتالية عبثية كما ذكرت التقارير. وقد تتكبد العناصر الإرهابية خسائر فادحة أثناء محاولتهم اتباع نصائح الذكاء الاصطناعي. لكن هذه الإخفاقات جميعاً لا ينبغي في نهاية المطاف أن تؤدي إلى التراخي في مواجهة هذا الخطر.

فتلك المنظمات تتعلم من أخطائها. إنها تُجرّب، وتكيف، وتبادل المعلومات، وتنتقل بين المنصات، وتُدرب أعضائها بشكل مستمر، وتحفظ بالدروس الناجحة وتتجاهل غير الناجحة. ويُجسّد مثال بوكو حرام هذا الأمر خير تجسيد. فقد لقي ثمانية عشر مقاتلاً حتفهم أثناء محاولتهم تنفيذ تدريب غريب بمساعدة الذكاء الاصطناعي، ومع ذلك، تعلمت المنظمة في نهاية المطاف ما يكفي لتنفيذ هجوم ناجح. إن الأمر الأكثر أهمية ليس درجة الذكاء التي يتميز بها الذكاء الاصطناعي بحد ذاته، بل قدرة المؤسسة على استخدام هذه التقنية كجزء من عملية تعلم متكررة. ومن المرجح أن تزداد أهمية ذلك مع تطور نماذج الذكاء الاصطناعي.

الخلاصة

لا يعني ظهور التمرد المدعوم بالذكاء الاصطناعي أن التنظيمات المرتبطة بـ "الإرهاب" على وشك امتلاك أسلحة خارقة لا يمكن إيقافها، ولا يعني أيضاً أن كل منظمة إرهابية أصبحت فجأة متطورة تقنياً. فمعظم الجماعات المتطرفة لا تزال تعاني من قيود مالية وبشرية ولوجستية واستخباراتية وتدريبية، فضلاً عن مشاكل تنظيمية أساسية.

لكن الذكاء الاصطناعي يغير بالتأكيد مسار الأمور. فهو يخفض تكلفة اكتساب المعرفة، ويسرع وتيرة التجارب، ويسهل إنتاج الدعاية، ويساعد في الترجمة وتجنيد العناصر الجدد، ويعين المقاتلين عديمي الخبرة على فهم المواضيع التقنية، ويمكنه تحسين التخطيط التكتيكي وقدرات الطائرات المسيّرة، كما يمكنه تضخيم المعلومات المضللة على نطاق غير مسبوق.

لذلك، قد لا يكمن الخطر الأكبر في سلاح واحد مذهل يعمل بالذكاء الاصطناعي، بل في آلاف التحسينات الصغيرة نسبياً التي تجعل المنظمات المتمردة أكثر قدرة وتمكناً. وفي هذا السياق، تواجه الحكومات مهمة بالغة الصعوبة، إذ يجب عليها منع أنظمة الذكاء الاصطناعي من أن تصبح أدوات للإرهاب، مع الحفاظ على حقها المشروع في الوصول إلى المعلومات والابتكار. في الوقت نفسه، يتعين على الدول التنافس مع دول أخرى تستثمر بكثافة في الذكاء الاصطناعي لأسباب اقتصادية وعسكرية. إن الولايات المتحدة والصين وروسيا والهند وغيرها من القوى الكبرى لا تملك حافزاً يُذكر للتخلي عن سباق الذكاء الاصطناعي. إذ تعتقد حكوماتها أن الريادة التكنولوجية قد تُحدد مستقبل القوة العسكرية والجيوسياسية. ونتيجة لذلك، من المرجح أن يبقى التنظيم الدولي صعباً.

وفي غضون ذلك، قد تكون الدول الأكثر تضرراً من التمرد هي الأقل قدرة على مواكبة تلك التطورات. وهذه هي الأهمية الحقيقية للفجوة الناشئة في مجال الذكاء الاصطناعي. فالفجوة التكنولوجية بين الدول الغنية والفقيرة قد تتحول إلى فجوة أمنية، بينما قد تُضيّق التكنولوجيا نفسها الفجوة بين الحكومات المتطورة والمنظمات المتمردة البدائية نسبياً.

نعم، قد تبدو التجارب المبكرة ساذجة؛ وقد تكون الدعاية المؤلدة بالذكاء الاصطناعي في البداية رديئة للغاية؛ وقد تنتهي النصائح الميدانية التي تقدمها أنظمة الذكاء الاصطناعي أحياناً بكارثة. لكن تجاهل هذه التطورات لمجرد أن

بعض المجموعات المرتبطة بـ "الإرهاب" يستخدمون الذكاء الاصطناعي بشكل سيئ حالياً إنما يُغفل النقطة الأهم، وهي أنهم يتعلمون، وكذلك تتطور التكنولوجيا.

لذلك، فإن السؤال المحوري ليس ما إذا كان بإمكان المتمردين استخدام الذكاء الاصطناعي. فهم قادرون على ذلك بالفعل؛ إنما السؤال هو ما إذا كانت الحكومات وشركات التكنولوجيا والمؤسسات الدولية قادرة على تطوير ضمانات فعّالة بالسرعة الكافية لمنع التجارب البدائية الحالية لتلك التنظيمات من أن تتحول إلى قدرات متطورة في الغد القريب؛ وقد بدأ السباق لتحقيق ذلك بالفعل.

