رأي | بقلم الرائد الإداري
جورج مفرّج

الذكاء الإصطناعي، الشركات الخاصة ومستقبل القوّة العسكرية

اعاد الذكاء الاصطناعي صياغة اساليب خوض الحروب والحفاظ على الامن ليشكل قوة حاسمة في ساحة المعركة. من الطائرات المسيرة الذاتية التشغيل وانظمة المراقبة المتطورة الى الشرطة التنبؤية والدفاع السيبراني، اصبح الذكاء الاصطناعي محوريا في الاستراتيجيات العسكرية والامنية الحديثة.

تعتمد الحكومات على شركات التكنولوجيا الخاصة لتوفير البيانات والخوارزميات والبنية التحتية السحابية، مما طمس الحدود بين سلطة الدولة وسلطة الشركات. تكشف الدراسات من اوكرانيا وغزة وغيرهما، كيف يعزز الذكاء الاصطناعي جمع المعلومات الاستخباراتية واتخاذ القرارات والعمليات الهجومية. مع ذلك، فان تأثيره المتزايد يثير تساؤلات اخلاقية وقانونية واستراتيجية ملحة في شأن الامن العالمي.

• استقاء البيانات لاستخلاص الدروس: يستخدم الذكاء الاصطناعي في ساحة المعركة للمراقبة والاستهداف ودعم اتخاذ القرار. تستفيد الحكومات من البيانات التي تجمع في مناطق الحرب من خلال الطائرات من دون طيار والاقمار الصناعية وغيرها لتدريب انظمة الذكاء الاصطناعي، وتعتبرها كنزا ثمينا للتعلم الالي.

انتجت الحروب بين الجيوش المتقدمة بيانات قتالية هائلة، لا سيما الحرب بين روسيا واوكرانيا. تستخدم الحكومة الاوكرانية الذكاء الاصطناعي لتوجيه الطائرات من دون طيار آليا، ولمسح صور المواقع العسكرية الروسية بمساعدة شركات خاصة. ان شركة Palantir واحدة من هذه الشركات، فهي تجمع المعلومات الاستخباراتية من الاقمار الصناعية والطائرات من دون طيار والمصادر المفتوحة لعرض خيارات الاستهداف، وتعتبر نفسها "مسؤولة عن معظم عمليات الاستهداف التي قادتها اوكرانيا"، وفقا لرئيسها التنفيذي اليكس كارب. لا تقتصر تحليلات برامج بالانتير للذكاء الاصطناعي على ذلك، بل تتعداها لتشمل جمع ادلة جرائم الحرب وتفكيك الالغام الارضية وغيرها.

تستفيد بالانتير من هذه البيانات والتحليلات لتطبيقها في ميادين اخرى. فقد اعلنت بريطانيا في ايلول 2025 عن شراكة دفاعية مع بالانتير تتضمن استضافتها للمقر الاوروبي للشركة التي ستشارك في تطوير "قدرات مدعومة بالذكاء الاصطناعي تم اختبارها بالفعل في اوكرانيا"، وستستخدمها "لدمج المعلومات الحساسة" ووضع خطط هجومية سريعة.

على المستوى الاستراتيجي، تساعد هذه التكنولوجيات القادة على محاكاة المعارك لاستباق نتائج الخطط العسكرية وتبني الافضل بينها.

• المراقبة وجمع المعلومات الاستخباراتية: ينتشر الذكاء الاصطناعي بشكل واسع في مجال الاستخبارات والمراقبة. تستخدم الحكومات تقنيات التعلم الآلي لغربلة البيانات الضخمة (صور الاقمار الصناعية، وسائل التواصل الاجتماعي، الخ) وتحويلها الى معلومات استخباراتية عملية. على سبيل المثال، يشير تحليل اجراه المعهد الملكي للخدمات المتحدة RUSI للحرب الاسرائيلية على غزة، الى ان حجم بيانات الاستشعار والاتصالات هائل لدرجة ان "الذكاء الاصطناعي عادة ما يشارك" في عملية الاستهداف الاولية، مستخدما تقنية التعرف على الانماط لتحديد الاهداف. بعد المعالجة المسبقة، تستطيع نماذج التعلم الآلي تحديد البنية التحتية العسكرية، تتبع المقاتلين او الابلاغ عن السلوكيات المشبوهة بشكل أسرع بكثير من قدرة المحللين البشريين.

تنخرط شركات التكنولوجيا الخاصة بشكل كبير في هذا المجال. توفر شركات مثل Maxar وPlanet Labs عمليات مسح عالية الدقة للاقمار الصناعية، بينما تستخدم قوات مسلحة اخرى منصتي Gotham وFoundry التابعتين لشركة Palantir، واللتين بنيتا في الاصل لمحللي وكالة المخابرات المركزية والبنتاغون، لدمج المعلومات الاستخبارية.

ايضا، وجد تقرير صادر عن مؤسسة كارنيغي عام 2019 ان أكثر من نصف الدول المتقدمة تستخدم انظمة مراقبة قائمة على الذكاء الاصطناعي. تغذي الاستخدامات المدنية الوعي العسكري. تنشئ كاميرات المراقبة التجارية، قواعد بيانات التعرف على الوجه وانظمة تحديد مواقع الهواتف المحمولة، مصادر هامة للمخابرات. في اوكرانيا، افادت التقارير ان شركة Clearview AI الخاصة للتعرف على الوجه منحت القوات الاوكرانية امكان الوصول الى صور حوالي 230 ألف جندي روسي، مما ساعد في تحديد هوية المتسللين الى اراضيها.

أضف الى ذلك، تراقب حكومات عدة وسائل التواصل الاجتماعي لتحقيق مكاسب تكتيكية، فتستخدم وحدات مكافحة الارهاب الأميركية مثلا ادوات الذكاء الاصطناعي للكشف عن الاحاديث التي تنم عن تطرف وتنذر بمخاطر، الا ان ذلك يثير تحديات جمة تتعلق بالخصوصية.

• الحرب السيبرانية: يلعب الذكاء الاصطناعي دورا متناميا في الهجوم والدفاع السيبرانيين. تستخدم الوحدات السيبرانية العسكرية التعلم الآلي لشن الهجمات وتعزيز الشبكات. على سبيل المثال، كشفت القيادة السيبرانية الاميركية في عام 2024 عن خارطة طريق تَعد بـ"دمج الذكاء الاصطناعي في كل جوانب العمليات السيبرانية".

تتضمن الخطة تحليلات تعتمد على الذكاء الاصطناعي للكشف عن عمليات تسلل العدو بشكل اسرع واتمتة الاستجابات الدفاعية. عمليا، يدعم الذكاء الاصطناعي خبراء الانترنت لتحديد نقاط الضعف البرمجية.

على الصعيد الهجومي، يساهم الذكاء الاصطناعي في تصميم برامج ضارة أكثر فعالية وحملات تصيد الكتروني موجه. في هذا الإطار، حذرت دراسة اجرتها Rand Corporation من ان الوكالات الروسية "تستغل الذكاء الاصطناعي لتحسين التجسس الالكتروني وتعزيز دقة الهجمات".

توفر شركات الأمن السيبراني الخاصة جزءا كبيرا من هذه التقنية. تستخدم منتجات مثل DarkTrace (المملكة المتحدة) وCrowdStrike (الولايات المتحدة) التعلم الآلي لتحديد سلوك الشبكة "الطبيعي" والابلاغ عن "الشذوذ" او عزله تلقائيا. الى جانب الجيش، تدافع شركات التكنولوجيا الكبرى ايضا عن البنية التحتية الحيوية. في حرب اوكرانيا، سارعت مايكروسوفت وامازون وغوغل الى نقل البيانات الحكومية لتأمين خوادم السحابة Cloud وتحييد برامج الفدية Ransomware، مما ساعد في صد الهجمات الالكترونية الروسية وحافظ على استمرارية تشغيل الانظمة المدنية.

• الشرطة التنبؤية: يثير التنبؤ بالجرائم المدار بالذكاء الاصطناعي الجدل، لكنه منتشر في دول عدة. تفحص انظمة الشرطة التنبؤية تقارير الجرائم التاريخية، شبكات التواصل الاجتماعي وغيرها من البيانات لتحديد بؤر الجريمة المحتملة او مرتكبيها. بموجب صفقة سرية عام 2012، زودت شركة بالانتير شرطة نيو اورلينز ببرنامج جمع وحلل قواعد بيانات العصابات والسجلات الجنائية وبيانات وسائل التواصل الاجتماعي، ليخلص الى تصنيف حوالى 3900 فرد خطرين. كما تعاقد جهاز الامن الدنماركي عام 2016 مع شركة بالانتير لتنفيذ مشروع مدته سبع سنوات "لتحديد الارهابيين المحتملين" عبر التحليلات التنبؤية.

باعت شركات اخرى مثل Axon، IBM، PredPol/Geolitica وShotSpotter ادوات تنبؤ بالجرائم تعمل بالذكاء الاصطناعي لشرطة الولايات المتحدة والاتحاد الاوروبي، بما في ذلك انظمة لتحديد اولويات الدوريات او كاميرات المراقبة.

توضح هذه الادوات كيف تؤثر شركات التحليلات الخاصة على الامن الداخلي. في الاراضي الفلسطينية المحتلة مثلا، افادت تقارير بأن وحدات اسرائيلية تستخدم خوارزميات لغربلة بيانات المراقبة المجمعة على مدى سنوات، مثل اعتراض الهواتف المحمولة ومنشورات مواقع التواصل الاجتماعي وغيرها، ولاعداد قوائم للمشتبه بهم، وهو شكل محفوف بالمخاطر من اشكال الشرطة التنبؤية اثار انتقادات دولية.

بينما تشيد الوكالات بمكاسب الكفاءة اي بتوزيع الشرطة حيث يتوقع وقوع الجريمة، يحذر المنتقدون من التحيز والغموض. ففي شيكاغو عام 2016، قام نظام تنبؤي بتمييز احياء الاقليات العرقية بشكل غير متناسب، مما دفع مسؤولي المدينة الى ايقاف البرنامج. مع ذلك، تواصل اجهزة الامن عالميا الشراكة مع شركات التكنولوجيا لتطوير عمل الشرطة.

• الاسلحة الذاتية التشغيل والروبوتات: يبقى الحديث عن الاسلحة الذاتية التشغيل والمنصات الروبوتية سواء في البر والبحر والجو، وغالبا ما تكون مجهزة بالذكاء الاصطناعي للملاحة ولاتخاذ قرار بالاشتباك. تنتج شركة Anduril غواصة "القرش الشبح" الذاتية التشغيل المتميزة بتكلفتها المنخفضة لاستغنائها عن طاقم بشري وهيكل ضغط عال، وقدرتها على الغوص الى اعماق تفوق بكثير الغواصات التي تقودها اطقم بشرية، اضافة الى صعوبة كشفها.

تشكل الروبوتات البرية المجهزة بكاميرات واسلحة دفعا كبيرا للجيوش في المعارك. استخدمت اسرائيل في عدوانها هذه الروبوتات، اضافة الى طائرات مسيرة صغيرة مسلحة. طورت شركة Roboteam الاسرائيلية وسيلة Robox للدفاع عن بقعة ما، وهي مجموعة روبوتات برية واستطلاعية وطائرات مسيرة معززة بالذكاء الاصطناعي تدمج بين اجهزة الاستشعار وانظمة الملاحة.

ايضا، طورت الصين مراكب ذاتية القيادة مثل الزورق Liaowangzhe II وطائرات من دون طيار ومسيرة ومركبات صاروخية مصممة لتهديد حاملات الطائرات، تعمل بأنظمة الذكاء الاصطناعي.

اما روسيا، فبنت مركبات برية ذاتية التشغيل، من بينها الدبابة الروبوتية Marker التي تحدد اولويات الهجوم عبر التعرف على صور دروع الناتو وتتخذ قرارات اطلاق النار.

كذلك، تستثمر الولايات المتحدة في الطائرات المقاتلة والطائرات المسيرة الذاتية التشغيل. يحول برنامج "تطوير القتال الجوي" التابع لوكالة مشاريع البحوث الدفاعية المتقدمة DARPA مقاتلات 16F الى طائرات مسيرة بالذكاء الاصطناعي للمعارك الجوية. حتى شركات التكنولوجيا المدنية مثل Anduril، Boston Dynamics وElbit وغيرها تشارك في هذا المجال، حيث تكيف الذكاء الاصطناعي لدعم استقلالية المركبات العسكرية.

يشير كل ما سبق الى اندلاع سباق تسلح عالمي، مدعوم بشكل متزايد بالذكاء الاصطناعي التجاري. من القارة الاميركية الى بحر الصين الجنوبي، ومن دوريات الشرطة الى الاستطلاع الفضائي، توفر شركات التكنولوجيا الخاصة الخوارزميات ومنصات البيانات والاجهزة التي تحرك حروب القرن الحادي والعشرين وأمنه.

كما يثير استخدام الذكاء الاصطناعي في المعارك مخاوف اخلاقية ويطرح اشكاليات تتعلق بالمحاسبة، اذ لا يمكن توزيع المسؤولية بين مصنع الالة ومبرمجها ومشغلها.

لن يتوقف العقد المقبل على الميزانيات العسكرية فحسب، بل على ابتكارات الشركات التكنولوجية، فهل دخلنا مرحلة تحول ميزان القوة نحو الشركات الخاصة؟ وهل ستتمكن المجتمعات ضمان الاستخدام الاخلاقي لهذه التقنيات؟