الذكاء الاصطناعي
تحول في استراتيجية إسرائيل العسكرية
(3)
هزيمة إيران

عبد المهدي مطاوع

لم يقتصر استخدام إسرائيل للذكاء الاصطناعي على حرب غزة أو لبنان، بل امتد ليكون العمود الفقري لاستراتيجية الردع التي تبنتها لتحييد التهديد الوجودي الذي تمثله إيران بالنسبة لها، من الاغتيالات إلى الحرب الإلكترونية والدفاع الصاروخي. ومن ثم كان المُضاعف للقوة الذي تسعى إسرائيل من خلاله إلى سد الفجوة الجغرافية والديموغرافية مع إيران. ومع ذلك، فإن اعتمادها المتزايد عليه قد يرفع المخاطر إلى مواجهة إقليمية شاملة، يحكمها سباق تسلح خفي، تتفاقم معه الأزمة من خلال خوارزميات سريعة قد تفوق قدرة البشر على احتوائها، مما قد يهدد بإطلاق العنان لعواقب إنسانية وسياسية لا رجعة فيها.

مما لا شك فيه أن انتقال إيران من استراتيجية الحرب بالوكالة إلى الردع المباشر، منذ 7 أكتوبر 2023م، فاقم من حدة تهديداتها لإسرائيل، وهو الأمر الذي رأت فيه إسرائيل دليلاً على عدوانية «محور المقاومة الإسلامية» المدعوم من طهران، فلجأت إلى تطوير واستخدام أدوات الذكاء الاصطناعي لمواجهتها على عدة جبهات متوازية. ليس فقط كأداة تكتيكية بل كعنصر مركزي في استراتيجية الردع الاستخباراتية والعسكرية متعددة المراحل. نشير غليها بإيجاز على النحو التالي:

أولا: مرحلة المراقبة والتحليل الاستباقي:

1) **تحديد البنية التحتية النووية والإستراتيجية**: استخدمت إسرائيل خوارزميات الذكاء الاصطناعي لتحليل (petabytes) بيانات الأقمار الصناعية وصوره؛ لاكتشاف وتتبع أي أنشطة مشبوهة بمنشآت إيران النووية وبمستودعات الذخيرة ومخازن الصواريخ الموجودة تحت الأرض وفي باطن الجبال، ومنصات إطلاقها الثابت منها والمتحرك. خاصة أن هذه الخوارزميات لديها القدرة على كشف أنماط حركة التربة الدقيقة، وأي تغير في درجة حرارتها واستشعار حركة المركبات، التي قد تشير إلى مواقع سرية أو أي تقدم في برنامج إيران النووي
2) **تحليل شبكة التمويل والتهريب**: تولت أنظمة الذكاء الاصطناعي تحليل الشبكات المالية العالمية، وأنماط الشحن البحري؛ لكشف محاولات إيران تهريب مكونات عسكرية، أو

تكنولوجيا مزدوجة الاستخدام، أو قيامها بعمليات غسيل الأموال لدعم حماس، وحزب الله اللبناني، وأنصار الله باليمن. مما مكنها من فرض حصار استخباراتي على إيران أكثر ذكاءً وفعالية.

ثانيا: مرحلة الهجومي/ الردعي:

يُشتبه بشكل مؤكد قيام إسرائيل، غالباً بالتعاون مع حلفاء، باستخدام ذكاء اصطناعي متقدم لتطوير هجمات إلكترونية معقدة ضد البنية التحتية الحساسة ومنشآت إيران الاستراتيجية، حيث وجهت ضربات في العمق السيبيري والفيزيائي. باستخدام الذكاء الاصطناعي، من خلال الخطوات التالي:

1) **اكتشاف الثغرات أوتوماتيكيا**: إذ تم مسح الأنظمة الإيرانية؛ لاكتشاف نقاط الضعف بسرعة قياسية.
2) **تطوير فيروسات مخصصة**: تصميم برمجيات خبيثة، مثل برنامج (Stuxnet)الشهير المنسوب إليها، تتكيف مع دفاعات الشبكة المستهدفة وقادرة على التسبب بأضرار فيزيائية بالمنشآت النووية والصناعية.
3) **تسييل الهجمات على نطاق واسع**: إدارة هجمات (DDoS)متطورة وتنسيقها ضد الأهداف بشكل متزامن.
4) **التخطيط للضربات الجوية المحتملة**: فقد تحول الخيار العسكري ضد منشآت إيران النووية لحقيقة وكان الذكاء الاصطناعي عاملاً حاسماً. استخدمت فيه أنظمة المحاكاة (Wargaming) المدعومة بالذكاء الاصطناعي لمحاكاة آلاف السيناريوهات، وتحديد مسارات مشابهة للطيران، ونقاط الضعف في الدفاعات الإيرانية، وتوقع ردود الفعل، بهدف زيادة فرص النجاح وتقليل المخاطر.

ثالثا: مرحلة بناء سور حديدي رقمي

1) **الدفاع الصاروخي المتكامل**: يعد الضربات الإيرانية المباشرة باستخدام الصواريخ الباليستية والفرط صوتية والمسيرات، تحول قلق إسرائيل إلى شعور بتهديد وجودي. هنا، اندمجت أنظمة الذكاء الاصطناعي لتشكل درعاً دفاعيا، مثل أنظمة «سهم» و«حيتس» التي تعتمد على خوارزميات التعلم الآلي في المعالجة الفائقة السرعة لبيانات الرادار، والتمييز بين الرؤوس الحربية والطعم، وحساب نقطة الاعتراض الأمثل للصواريخ ذات السرعات الفائقة

2) **التنبؤ بمسار المسيرات**: قامت إسرائيل بتتبع المسيرات الإيرانية البطيئة والمنخفضة، وتدميرها. خاصة أنها تمتلك شبكة رادارية ضخمة. يتولى الذكاء الاصطناعي تحليل بياناتها للتنبؤ بدقة بمسارات هذه المسيرات، وأهدافها المحتملة، مما يمكن أنظمة الدفاع من تحييدها.

تداعيات الصراع الإيراني الإسرائيلي:

1) **سباق التسلح في الذكاء الاصطناعي**: إذ تمتلك إيران وإسرائيل برنامجاً نشطاً للذكاء الاصطناعي لأغراض عسكرية. من شأنه خلق ديناميكية سباق تسلح جديد وخطير، حيث يحاول كل طرف منهما خداع خوارزميات الطرف الآخر أو تعطيلها.

2) **خطر التصعيد الكارثي**: أي خطأ في الخوارزمية، مثل تحديد خاطئ لهدف على أنه هجوم إيراني (ضربة صاروخية نووية مثلاً)، أو هجوم إلكتروني خرج عن نطاق السيطرة، يمكن أن يؤدي إلى رد فعل متسلسل وينتهي بحرب إقليمية شاملة، ذات عواقب لا يمكن تصورها.

3) **الغموض والمساءلة في الفضاء السيبيري**: يجعل الطبيعة غير الملموسة للهجمات الإلكترونية، والمعززة بالذكاء الاصطناعي، من المستحيل تقريباً إثبات هوية الفاعل بشكل قاطع، مما يزيد من صعوبة تطبيق قواعد الردع والمساءلة الدولية.