ARRAY
الشركة الوطنية الرائدة في مجال الذكاء الاصطناعي والبيانات
الذكاء الاصطناعي
أنظمة البيانات
التحول الرقمي والتطوير
للتواصل: hello@array.world
إحدى شركات محفظة ممتلكات البحرين

باحثة بحرينية تقترح إطارًا لحوكمة الذكاء الاصطناعي المسؤول والمنصف في الرعاية الصحية

أهمية الموازنة بين الاستفادة من التطور التقني وضمان حقوق المرضى وسلامتهم



تناول بحث للباحثة مريم الصالح التحديات الأخلاقية والتنظيمية المرتبطة بتوظيف تقنيات الذكاء الاصطناعي في قطاع الرعاية الصحية، مسلطًا الضوء على أهمية ضمان عدالة هذه الأنظمة وسلامتها لجميع المرضى، وعدم الاكتفاء بمؤشرات الدقة العامة عند تقييم أدائها.

وأوضح البحث أن أنظمة الذكاء الاصطناعي، رغم إمكاناتها في دعم القرارات السريرية وتحسين دقة التشخيص والتنبؤ بالمخاطر الصحية، قد تُظهر تفاوتًا في مستوى أدائها بين فئات المرضى، نتيجة اختلاف اللغة أو العمر أو الجنس أو الحالة الصحية، فضلًا عن طبيعة البيانات المستخدمة في تدريبها، الأمر الذي قد يؤدي إلى زيادة احتمالات الخطأ لدى بعض الفئات دون غيرها.

وأشار البحث إلى وجود فجوة بين المبادئ العامة للذكاء الاصطناعي المسؤول، بما تشمله من العدالة والشفافية والخصوصية والسلامة والمساءلة البشرية، وبين آليات تطبيقها عمليًا داخل المؤسسات الصحية، إذ لا توفر هذه المبادئ في كثير من الأحيان أدوات إجرائية واضحة لقياس مدى الالتزام بها وتدقيق الأنظمة قبل اعتمادها وخلال استخدامها.

وفي هذا السياق، اقترحت الباحثة إطارًا يحمل اسم RE-AL-Gov، وهو إطار لحوكمة دورة حياة الذكاء الاصطناعي المسؤول والمنصف، يهدف إلى تحويل المبادئ الأخلاقية إلى متطلبات تقنية وتنظيمية قابلة للقياس والتقييم والتدقيق، بما يعزز موثوقية أنظمة الذكاء الاصطناعي ويرفع مستوى المساءلة بشأن استخدامها في الرعاية الصحية.

ويؤكد البحث أهمية تبني نهج متكامل لحوكمة الذكاء الاصطناعي في القطاع الصحي، يوازن بين الاستفادة من التطور التقني وضمان حقوق المرضى وسلامتهم، بما يسهم في تعزيز الثقة بالتطبيقات الذكية ودعم توظيفها بصورة مسؤولة ومنصفة.

سلاسل التبريد الذكية تحت الحصار: كيف تحولت برادات أوروبا إلى ساحة حرب سيبرانية مدفوعة بالذكاء الاصطناعي؟



بقلم:
د. جاسم حاجي

تشهد القارة الأوروبية تحولاً جذرياً في مفهوم الأمن القومي الغذائي واللوجستي، حيث لم تعد التهديدات تقتصر على الحدود الجغرافية، بل امتدت لتستهدف عمق البنية التحتية الحيوية. في هذا السياق، برزت الهجمات السيبرانية على البرادات وأنظمة التبريد الصناعية في أوروبا كأحد أخطر التهديدات التقنية الناشئة. مع الاعتماد المتزايد على إنترنت الأشياء (IoT) والذكاء الاصطناعي لإدارة سلاسل الإمداد، تحولت هذه الأنظمة من مجرد آلات ميكانيكية إلى أهداف سيبرانية معقدة، حيث يتقاطع الأمن المادي مع الأمن الرقمي في معركة شرسة تقودها الخوارزميات الذكية من كلا الجانبين.

الهندسة التقنية للهجمات: اختراق الأنظمة التشغيلية (OT)

تعتمد البرادات الصناعية ومستودعات التبريد الضخمة في أوروبا على أنظمة التحكم الإشرافي وتحصيل البيانات (SCADA) والمنظمات المنطقية القابلة للبرمجة (PLCs). تعمل هذه المكونات على تنظيم درجات الحرارة والرطوبة وضغط الغازات الحيوية مثل الأمونيا أو ثاني أكسيد الكربون.

تتمثل الثغرة التقنية الأساسية في «تقارب تكنولوجيا المعلومات والتكنولوجيا التشغيلية" (IT/OT Convergence). يسعى المهاجمون إلى اختراق شبكات الشركات (IT) عبر بريد التصيد الاحتيالي أو ثغرات البرمجيات غير المحدثة، ثم الانتقال أفقياً (Lateral Movement) إلى شبكة التشغيل (OT). بمجرد الوصول، يتم التلاعب بالقراءات الرقمية للمستشعرات؛ فيبدو النظام للمشغلين البشريين مستقراً، بينما يتم في الواقع إيقاف التبريد أو رفع درجات الحرارة بشكل تدريجي، مما يؤدي إلى تلف الأغذية أو الأدوية الحيوية (مثل اللقاحات) دون إطلاق إنذارات فورية.

دور الذاء الاصطناعي في المعسكرين: الهجوم والدفاع

دخل الذكاء الاصطناعي كعامل حسم ومضاعف للقوة في هذه المواجهة، وصار يمثل سلاحاً ذا حدين:

1. الذكاء الاصطناعي كأداة هجومية (AI-Driven Attacks):

يستخدم القراصنة نماذج تعلم الآلة لتنفيذ هجمات «التصيد الاحتيالي الموجه» فائق الدقة لاستهداف مهندسي الصيانة. والأخطر من ذلك هو استخدام الذكاء الاصطناعي لتطوير برمجيات خبيثة متكيفة (Adaptive Malware). تستطيع هذه البرمجيات مراقبة سلوك نظام التبريد لأسابيع، وفهم دورة عمل البرادات، ثم توليد شفرات هجومية مخصصة لتجاوز جدران الحماية التقليدية، ومحاكاة البيانات الطبيعية للمستشعرات لإخفاء التخريب (Faking Sensor Data).

1. الذكاء الاصطناعي كدرع دفاعي (AI-Powered Defense):

في المقابل، لم تعد الحلول الدفاعية التقليدية القائمة على التوقيعات (Signatures) كافية. تتجه الشركات الأوروبية اليوم إلى نشر أنظمة «الدفاع السيبراني المناعي» المبنية على الذكاء الاصطناعي. تقوم هذه الأنظمة بتحليل سلوك شبكة البرادات في الوقت الفعلي، ووضع خط أساسي (Baseline) للمؤشرات الفيزيائية (كالطاقة، والضغط، والحرارة). إذا حدث أي انحراف دقيق جداً لا تدركه العين البشرية أو الأنظمة القديمة، يتداخل الذكاء الاصطناعي فوراً لعزل الجزء المصاب من الشبكة (Micro-segmentation) وتعديل بروتوكولات الأمان تلقائياً لوقف انتشار الهجوم.

التداعيات الاقتصادية

إن استهداف البرادات في أوروبا ليس مجرد تخريب عشوائي، بل هو أداة في حرب هجينة (Hybrid Warfare) تهدف إلى زعزعة الاستقرار الاقتصادي والاجتماعي. تؤدي هذه الهجمات إلى شلل في سلاسل توريد الأغذية، وخسائر مالية ضخمة للشركات، وضغوط تضخمية في الأسواق الأوروبية، فضلاً عن خطر تسمم المستهلكين في حال وصول أغذية فاسدة إلى الرفوف بسبب تلاعب سيبراني غير مكتشف.

إن مستقبل أمن سلاسل التبريد في أوروبا بات مرتبطاً ارتباطاً وثيقاً بمدى تطور خوارزميات الذكاء الاصطناعي الدفاعية. لم تعد المعركة تدور حول جودة العوازل الجدارية للبرادات، بل حول متانة الجدران النارية البرمجية وقدرة الذكاء الاصطناعي على التنبؤ بالتهديدات قبل وقوعها، لحماية شريان الحياة الغذائي للقارة العجوز.

ARRAY
#1 عالمياً
SPECTRUM AI™
OCR & AGENTIC RAG MODEL
المركز الأول عالميًا لمدة 30 أسبوعًا متتاليًا
ضمن فئة النماذج مفتوحة الأوزان
للتواصل: hello@array.world
ARRAY INNOVATION
الرائد الوطني للبيانات والذكاء الاصطناعي