مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

التحديات المستقبلية للامن السيبراني في عصر الذكاء الاصطناعي

م.م. هند محمد محمود (*)

المقدمة

يشــهد العالــم اليوم تحــولاً رقمياً واســع النطاق، حيــث أصبحــت التكنولوجيــا جزءاً أساســياً من الحيــاة اليومية، ســواء على مســتوى الأفراد أو المؤسســات أو الحكومــات. ومــع هــذا التوســع المتســارع في استخدام التكنولوجيا، تتزايد أهمية الأمن الســيبراني باعتباره خط الدفاع الأول ضد التهديــدات الرقميــة. ومع ذلك، فإن هــذا المجال يواجه مجموعة من التحديات المســتقبلية المعقدة التي تتطلب اســتعداداً عالياً وتخطيطاً استراتيجياً شــاملاً. وأحــد أبرز هــذه التحديات هــو التطور المســتمر في أســاليب الهجمات السيبرانية. حيث لم تعد الهجمات مقتصرة على الأساليب التقليدية، بل باتت أكثر تطورًا وتعقيدًا، مما يجعل اكتشافها والتصــدي لها أمرًا بالغ الصعوبــة. فالمهاجمون يســتغلون الثغــرات الأمنيــة بــذكاء، وينفــذون هجمات متقدمة تســتهدف الأنظمة الحيوية بدقة، مثل الهجمات المســتمرة المتقدمة (APT)، التي تهدف إلى التســلل والبقاء داخل الشبكات لأطول فترة ممكنة دون اكتشاف.

كمــا أن الاعتمــاد المتزايد على الفضــاء الرقمي يشكل تحديًا آخر، فمع توسع الخدمات الإلكترونية فــي مختلــف القطاعات مثــل التعليــم، الصحة، البنــوك، والحكومات، أصبح هنــاك كمٌّ هائل من البيانــات الحساســة معرّض للاختــراق، ما يزيد من أهميــة تعزيز حمايــة هذه المعلومــات. كلما توســعت البنية التحتية الرقمية، زادت احتمالات الهجوم، وأصبح من الضروري تطوير أســاليب جديــدة للحماية تواكب هذا النمو.من جهة أخرى، يُعــد العامل البشــري أحــد أضعــف الحلقات في الأمن السيبراني. فالكثير من الاختراقات لا تكون ناتجــة عــن ضعف في النظام نفســه، بل بســبب أخطاء بشرية، كفتح روابط مجهولة، أو مشاركة كلمات مرور ضعيفة، أو التعامل مع رسائل بريد إلكتروني مشبوهة. وبالتالي فإن التوعية المستمرة للمستخدمين وتدريبهم على أســاليب الحماية يُعد من الأمور الأساسية لمواجهة هذا التحدي.

مشــكلة البحث:يشــهد العالم تطورًا متسارعًا في تقنيات الذكاء الاصطناعي، مما أثر بشــكل كبير علــى مفاهيم وأســاليب الأمن الســيبراني. ورغم

(*) جامعة النهرين / مكتب مساعد رئيس الجامعة للشؤون الإدارية
Hind.mohamed@nahrainuniv.edu.iq

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

أن هـذه التقنيات تقدم أدوات قوية لتعزيز الحماية الرقميــة، إلا أنهــا فــي الوقت ذاته تفتــح المجال أمــام تهديدات جديدة أكثر تعقيدًا. تكمن المشــكلة فــي كيفيــة التوفيــق بين الاســتفادة مــن قدرات الــذكاء الاصطناعي وحماية الأنظمة الرقمية من المخاطر التي قد تنتج عن إساءة استخدامه.

فرضية البحث:يمكن تقليل التهديدات السـيبرانية المســتقبلية الناتجــة عن الــذكاء الاصطناعي من خلال تطوير اســتراتيجيات أمنيــة مبتكرة تجمع بيــن التقنيــة والرقابــة، وتُبنــى على فهم شــامل للتحديات المتوقعة في هذا المجال.

أهميــة البحث:تبــرز أهمية هذا البحــث في كونه يتناول قضية معاصرة تمس جميع القطاعات التي تعتمد على التكنولوجيا الرقمية، ســواء الحكومية أو الخاصة. كما يســاهم في تســليط الضوء على المخاطــر المســتقبلية التي قد لا تكــون واضحة بعد، ويساعد في وضع الأســس العلمية والأمنية لمواجهتها بفاعلية. ويشكل هذا الموضوع مرجعًا مهمًا لصنــاع القرار والباحثيــن والمختصين في مجال الأمن السيبراني.

أهداف البحث:

١.تحديد أبرز التحديات المســتقبلية التي يفرضها الذكاء الاصطناعي على الأمن السيبراني.

٢.تحليل طرق اســتغلال الذكاء الاصطناعي في تنفيذ الهجمات السيبرانية.

٣.تقييم فعالية اســتخدام الــذكاء الاصطناعي في الحماية من التهديدات الرقمية.

٤.اقتراح توصيات لتعزيز السياســات الأمنية في ظل تطور الذكاء الاصطناعي.

منهجيــة البحث:يعتمد هــذا البحث علــى المنهج الوصفي التحليلي، حيث يتم اســتعراض الأدبيات والدراســات الســابقة المتعلقة بالأمن الســيبراني والــذكاء الاصطناعــي، ثم تحليــل العلاقة بينهما مــن حيث التهديدات والحلــول المقترحة. كما يتم تقديم نمــاذج واقعية لحالات اســتُخدم فيها الذكاء الاصطناعي بشــكل إيجابي أو ســلبي في المجال الســيبراني، بهدف الوصول إلى استنتاجات دقيقة وتوصيات عملية.

المبحث الاول

مفهوم الذكاء الاصطناعي وتطبيقاته في المجال السيبراني

الــذكاء الاصطناعي هــو العلم الذي يســعى إلى تطويــر نظم حاســوبية تعمل بكفاءة عالية تشــبه كفاءة الإنسان الخبير، أي أنه قدرة الآلة على تقليد ومحــاكاة العمليــات الحركية والذهنية للإنســان، وطريقــة عمــل عقله فــي التفكيــر والاســتنتاج والرد والاســتفادة مــن التجارب الســابقة وردود الفعــل الذكية؛ فهو مضاهاة عقل الإنســان والقيام بدوره[1]. (الأمين، ٢٠٢٤: ١٢)

ويعرف أيضاً بأنه عملية محاكاة الذكاء البشــري عبر أنظمة الحاســوب عن طريق دراســة سلوك البشــر، وإجــراء تجــارب علــى تصرفاتهــم، ووضعهــم في مواقف معينــة، ومراقبة رد فعلهم ونمط تفكيرهم وتعاملهم مع هذه المواقف، ومن ثم محاولة محاكاة طريقة التفكير البشرية عبر أنظمة

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

الحاسوب، فلكي تتسم الآلة بالذكاء الاصطناعي لا بد أن تكون قادرة على التعلم وجمع البيانات وتحليلها، واتخاذ القرارات بناء على عملية تحليل بصورة تحاكي طريقة تفكير البشر.

و أنه سعي الآلة أو الحاسوب للاقتراب أكثر من قدرات العقل البشري وإمكانياته، والتفوق عليه في بعض الأحيان، وهو نظام علمي يشتمل على طرق التصنيع والهندسة لما يسمى بالاجهزة والبرامج الذكية بهدف إنتاج آلات مستقلة قادرة على المهام المعقدة باستخدام انعكاسات مماثلة لتلك التي لدى البشر، ويتم تصميم برامج وتطبيقات الذكاء الاصطناعي بدراسة كيفية تفكير العقل البشري؟ وكيف يتعلم الإنسان ويقرر ويعمل أثناء محاولة حل مشكلة.

يتم تدريب الأنظمة الذكية على كميات ضخمة من البيانات، لتتمكن من التعلم واستخلاص الأنماط وتحسين أدائها مع مرور الوقت، دون الحاجة إلى برمجة صريحة لكل مهمة. وتتمثل قوة الذكاء الاصطناعي في قدرته على التعامل مع البيانات المعقدة، وتحليلها بسرعة تفوق قدرات الإنسان، مما يجعله أداة فعّالة في العديد من المجالات، ومنها الأمن السيبراني.

ومع تزايد التهديدات الرقمية، أصبح الذكاء الاصطناعي من أهم الأدوات المستخدمة لحماية الأنظمة والشبكات. وفيما يلي أبرز تطبيقاته في الأمن السيبراني[٢]:

١. كشف التهديدات السيبرانية وتحليلها:يمكن للذكاء الاصطناعي التعرف على الأنماط غير المعتادة أو الشاذة في الشبكة، والتي قد تدل على وجود اختراق أو محاولة هجوم. على سبيل المثال، عند ملاحظة نشاط غير معتاد لمستخدم معين أو تحميل بيانات بكميات ضخمة، قد تقوم الأنظمة الذكية بتنبيه مسؤولي الأمن فوراً، أو اتخاذ إجراء تلقائي لحماية النظام.

٢. التصدي للهجمات الإلكترونية في الزمن الحقيقي:توفر تقنيات الذكاء الاصطناعي القدرة على الاستجابة الفورية للهجمات، وذلك من خلال اتخاذ إجراءات تلقائية مثل حظر عنوان IP مشبوه، أو تعطيل حسابات يُشتبه في اختراقها، مما يقلل من الأثر المحتمل للهجوم.

٣. تعزيز أنظمة التحقق من الهوية:يُستخدم الذكاء الاصطناعي في أنظمة المصادقة البيومترية، مثل التعرف على الوجه أو بصمة الإصبع أو الصوت. كما يمكنه تحليل سلوك المستخدم (مثل طريقة الكتابة أو التصفح) للتأكد من أن المستخدم الحالي هو نفسه الذي سُجلت بياناته سابقًا، مما يوفر طبقة أمان إضافية.

٤. التنبؤ بالهجمات المستقبلية:من خلال تحليل البيانات التاريخية لأنواع الهجمات السابقة، يمكن للذكاء الاصطناعي توقع الهجمات المحتملة في المستقبل واقتراح تدابير وقائية. هذا يساعد المؤسسات في الاستعداد للهجمات قبل وقوعها.

٥. تصفية وتحليل رسائل البريد الإلكتروني:يُستخدم الذكاء الاصطناعي لاكتشاف رسائل البريد الاحتيالية (Phishing) والبرمجيات الخبيثة المرفقة بالبريد الإلكتروني. يستطيع النظام تحليل محتوى الرسالة والتعرف على الكلمات أو الروابط المشبوهة بدقة أكبر من

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

الطرق التقليدية.

٦. إدارة التهديدات بشكل ذكي (Threat Intelligence):يُستخدم الذكاء الاصطناعي لتحليل كميات ضخمة من المعلومات حول التهديدات من مصادر مختلفة، وتجميعها في تقارير مفيدة تساعد الخبراء في اتخاذ قرارات أمنية مبنية على بيانات دقيقة وحديثة.

إن استخدام الذكاء الاصطناعي في الأمن السيبراني يُعد نقلة نوعية في قدرة الأنظمة على حماية البيانات والبنية التحتية الرقمية. ولكن، في الوقت ذاته، يُشكل تحدياً كبيراً إذا ما تم استغلاله بشكل سلبي من قبل المهاجمين. لذا فإن تطوير هذه التقنيات، مع وضع ضوابط لاستخدامها، يُعد من الضروريات في المستقبل الرقمي.

المطلب الاول: الذكاء الاصطناعي وتعزيز الأمن السيبراني

في ظل تزايد الهجمات السيبرانية من حيث العدد والتعقيد، لم تعد الأساليب التقليدية في الدفاع كافية لحماية الأنظمة والمعلومات. ولهذا السبب، أصبح الذكاء الاصطناعي أداة محورية في تعزيز قدرات الأمن السيبراني، وذلك بفضل قدرته على تحليل كميات ضخمة من البيانات، واكتشاف الأنماط، والتصرف بشكل ذكي وتلقائي لمواجهة التهديدات[٣].

أولاً: كشف التهديدات السيبرانية

الذكاء الاصطناعي قادر على اكتشاف التهديدات السيبرانية بشكل أسرع وأكثر دقة من البشر أو البرمجيات التقليدية. إذ تعتمد أنظمة الذكاء الاصطناعي، خاصة تلك المبنية على «تعلم الآلة»، على تحليل السلوك الطبيعي للمستخدمين والأجهزة داخل الشبكة، ومن ثم رصد أي سلوك غير اعتيادي قد يدل على وجود اختراق أو تهديد.على سبيل المثال، إذا قام موظف بتحميل كميات غير معتادة من الملفات خارج أوقات العمل، أو ظهرت محاولات دخول متكررة من مواقع جغرافية غير معتادة، يمكن للنظام الذكي أن يعتبر ذلك تهديدًا محتملاً، ويصدر إنذارًا أو يوقف العملية مؤقتًا لحين التحقق منها[٤].

ثانيًا: تحليل البيانات الأمنية

يتعامل الأمن السيبراني مع كميات هائلة من البيانات، مثل سجلات الدخول، حركات المرور عبر الشبكة، محاولات الدخول الفاشلة، رسائل البريد الإلكتروني، وغيرها. تحليل هذه البيانات يدويًا يُعد أمرًا صعبًا ويستهلك وقتًا كبيرًا. هنا يأتي دور الذكاء الاصطناعي، الذي يستطيع قراءة وتحليل هذه البيانات بسرعة فائقة، واستخراج أنماط التهديدات الجديدة، وحتى التنبؤ بالهجمات المستقبلية.

بفضل الذكاء الاصطناعي، لم يعد دور النظام الأمني مجرد الاستجابة للهجمات بعد وقوعها، بل أصبح بإمكانه التنبؤ بها والتصرف بشكل استباقي، وهو ما يُعرف بـ «الدفاع السيبراني الاستباقي».

ثالثًا: أتمتة عمليات الاستجابة

من المزايا الإضافية لاستخدام الذكاء الاصطناعي في الأمن السيبراني، أنه يمكنه تنفيذ ردود أفعال

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

فورية دون الحاجة لتدخل بشري. فعندما يكتشف تهديدًا معينًا، يمكنه مثلاً حظر عنوان IP مشبوه، أو عـزل جهاز معيـن داخل الشـبكة، أو إغلاق اتصال مؤقت حتـى يتم التحقق منه، مما يحد من انتشار الهجوم ويقلل من الأضرار المحتملة[٥].

الـذكاء الاصطناعـي أصبح عنصرًا أساسـيًا في أنظمة الأمن السـيبراني الحديثة، خاصة في مهام مثل كشـف التهديـدات وتحليل البيانـات. بفضل قدرته على التعلم والتصـرف الذكي، يوفر طبقة حماية أكثر فاعليـة ومرونة من أي وقت مضى، ويسـاعد المؤسسـات فـي الاسـتعداد للهجمـات ومواجهتها بشكل أسرع وأدق.

ومع التوسـع الكبيـر فـي اسـتخدام التكنولوجيا وزيـادة حجـم التهديـدات السـيبرانية، لـم تعـد أدوات الحماية التقليديـة كافية للتصدي للهجمات الإلكترونية الحديثة، وخاصة تلك التي تعتمد على البرمجيات الخبيثة التي تتغير وتتطور باستمرار. وهنـا برز دور الـذكاء الاصطناعي، وبالأخص تقنية «تعلم الآلة»، كأحد الحلول الفعالة في مجال الأمن السـيبراني، وتحديدًا في كشـف ومواجهة البرمجيـات الخبيثة.فـي السـابق، كانـت أنظمة الحماية تعتمد بشـكل أساسـي على قاعدة بيانات تحتـوي علـى «توقيعـات» محددة للفيروسـات والبرمجيات الضـارة، أي أنها تبحث عن تطابق بين الملفـات الموجودة في الجهـاز والبرمجيات المعروفـة لديها. لكن مع تطـور التهديدات، بات من السـهل على المهاجمين تعديل شكل البرمجية الخبيثـة أو طريقة عملها لتبـدو مختلفة تمامًا عن النسـخة الأصلية، وهكـذا تنجح في التسـلل إلى النظام دون أن يتم اكتشافها[٦].

فـي المقابل، يوفـر تعلم الآلة طريقـة أكثر ذكاءً فـي التعامل مع هذا التهديد. حيث لا يعتمد النظام فقط على شـكل الملف أو توقيعه، بل يقوم بتحليل سـلوك البرنامج. بمعنى آخـر، إذا قام ملف معين بمحاولة فتح اتصال بشـبكة مشـبوهة، أو حاول التلاعـب بملفات النظـام، أو بـدأ بتحميل ملفات دون إذن المسـتخدم، فإن النظام المدعوم بالذكاء الاصطناعـي يتعـرف علـى هـذا السـلوك غير الطبيعي، حتى لو لم يكن الملف نفسه معروفًا من قبل.

علـى سـبيل المثـال، هنـاك برامج حديثـة مثل CylancePROTECT وMicrosoft Defender for Endpoint تعتمـد على الذكاء الاصطناعـي في تحليل سـلوك البرامـج قبل أن يُسـمح لها بالعمل. هذه البرامج تـم تدريبها على ملايين العينات من البرمجيات الضارة والسليمة، مما يجعلها قادرة على التمييز بين النشاط الطبيعي والضـار بكفاءة عاليـة، دون الحاجـة لتحديثات مستمرة أو تدخل بشري مباشر.

مـا يميز هذه الأنظمة هو أنهـا تتعلم من كل حالة تتعامل معها. فكل محاولة هجوم أو تصرف غير طبيعي يتم تحليله وتخزينه، مما يساعد النظام في تحسـين أدائه في المسـتقبل. ومع الوقت، يصبح أكثـر دقة في التنبؤ بالتهديدات، بل وقد يتمكن من التعرف على برمجيات خبيثة جديدة حتى قبل أن تُسـتخدم فعليًا فـي هجمات موسـعة.بالتالي، فإن اعتماد الأمن السيبراني على الذكاء الاصطناعي وتعلـم الآلة لم يعد رفاهيـة، بل ضرورة، خاصة مـع ازديـاد تعقيد التهديـدات الرقمية، وسـرعة انتشـارها، والحاجـة لحلول دفاعية قـادرة على

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

العمل بشكل فوري وذكي دون تأخير[٧].

المطلب الثاني: مزايا استخدام الذكاء الاصطناعي في تعزيز الدفاع السيبراني.

أصبح الذكاء الاصطناعي جزءًا لا يتجزأ من البنية الدفاعية للأنظمة السيبرانية، لما يتمتع به من قدرات متقدمة في التحليل، التعلم، والاستجابة الفورية. وقد أظهر فعالية كبيرة في التصدي للهجمات الإلكترونية المعقدة، التي يصعب على الأنظمة التقليدية اكتشافها أو التعامل معها. ومن أبرز المزايا التي يقدمها الذكاء الاصطناعي في هذا السياق ما يلي[٨]:

١.يتميز الذكاء الاصطناعي بالسرعة في تحليل كميات هائلة من البيانات خلال وقت قصير جدًا، وهو ما يعجز عنه الإنسان أو حتى الأدوات التقليدية. فأنظمة الذكاء الاصطناعي قادرة على مراقبة حركة المرور داخل الشبكة وتحليل الأنشطة الرقمية في الزمن الحقيقي، مما يمكنها من اكتشاف التهديدات بسرعة قبل أن تتسبب في أضرار فعلية.

٢.يوفر الذكاء الاصطناعي قدرة على التعلم المستمر والتطور الذاتي. فعبر تقنيات تعلم الآلة، تصبح أنظمة الحماية قادرة على تحسين أدائها مع مرور الوقت، كلما تعرضت لمواقف جديدة أو تهديدات غير مسبوقة. وهذا يعني أن الذكاء الاصطناعي لا يعتمد على قواعد ثابتة، بل يتكيف مع المستجدات ويطور آليات الحماية تلقائيًا.

٣.يمتلك الذكاء الاصطناعي قدرة مميزة على رصد السلوكيات الشاذة داخل الشبكات. فعوضًا عن البحث فقط عن البرمجيات الضارة المعروفة، يمكنه التعرف على سلوك غير طبيعي لمستخدم أو جهاز معين، وهو ما قد يشير إلى محاولة اختراق أو نشاط غير مشروع. هذا النوع من الحماية السلوكية يعتبر من أهم التطورات الحديثة في الأمن السيبراني.

٤.يسهم الذكاء الاصطناعي في أتمتة عمليات الاستجابة للحوادث الأمنية، وهو ما يُعرف باسم «الاستجابة التلقائية» (Automated Response). حيث يمكن للأنظمة الذكية أن تتخذ قرارات فورية مثل عزل جهاز مخترق، أو حظر عنوان IP مشبوه، دون انتظار تدخل بشري، مما يقلل من زمن الاستجابة ويحد من الأضرار.

٥.يُساعد الذكاء الاصطناعي في تخفيف الضغط عن فرق الأمن السيبراني البشرية. ففي ظل النقص العالمي في المتخصصين بهذا المجال، يصبح الذكاء الاصطناعي عنصرًا مساعدًا مهمًا من خلال تنفيذ المهام المتكررة أو المعقدة، مما يتيح للخبراء التركيز على تحليل التهديدات الكبرى ووضع استراتيجيات الحماية.

٦.تُمكن تقنيات الذكاء الاصطناعي المؤسسات من التنبؤ بالهجمات المستقبلية عبر تحليل الأنماط السابقة ومحاكاة سيناريوهات محتملة للهجمات، مما يتيح بناء استراتيجيات دفاعية أكثر فعالية واستباقية.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

المبحث الثاني

التحديات والمخاطر السيبرانية المستقبلية الناتجة عن الذكاء الاصطناعي

على الرغم من أن الذكاء الاصطناعي أصبح عنصرًا أساسيًا في دعم وتعزيز الأمن السيبراني، إلا أنه في المقابل أوجد نوعًا جديدًا من التهديدات والتحديات، مما يجعل العلاقة بين الذكاء الاصطناعي والأمن السيبراني معقدة ومزدوجة. فالذكاء الاصطناعي يُستخدم اليوم ليس فقط كأداة للحماية، بل أيضًا كسلاح بيد المهاجمين، وهذا ما يثير قلق الباحثين وصناع القرار حول العالم[٩].

أحد أخطر التحديات هو أن الذكاء الاصطناعي يمكن استغلاله لتنفيذ هجمات سيبرانية أكثر تطورًا وخداعًا. فعلى سبيل المثال، يمكن استخدام تقنيات «التعلم العميق» لإنشاء رسائل تصيد احتيالي تبدو أكثر واقعية وذات طابع شخصي، مما يزيد من احتمالية وقوع المستخدمين ضحية لها. كما يمكن استخدام الذكاء الاصطناعي في تصميم برمجيات خبيثة قادرة على التخفي والتكيّف، مما يصعّب من عملية اكتشافها والتصدي لها بالطرق التقليدية. تحدٍ آخر يتمثل في صعوبة التنبؤ بسلوك الأنظمة الذكية، خاصة تلك التي تعتمد على التعلم الذاتي. فبعض نماذج الذكاء الاصطناعي قد تصل إلى قرارات أو سلوكيات غير متوقعة في ظل ظروف معينة، مما يفتح الباب لاحتمال ارتكاب أخطاء أو انحرافات تؤدي إلى تهديد أمني. هذا يخلق حاجة ملحّة إلى ما يُعرف بـ»الذكاء الاصطناعي القابل للتفسير»، أي الأنظمة التي يمكن فهم منطق عملها وتوقع نتائجها. من جهة أخرى، تزداد تحديات الخصوصية وسرية البيانات مع توسّع استخدام الذكاء الاصطناعي، إذ تحتاج هذه التقنيات إلى كميات هائلة من البيانات لتعمل بكفاءة، مما يدفع بعض الجهات إلى جمع بيانات المستخدمين وتحليلها بشكل قد ينتهك خصوصيتهم. في حال اختراق هذه البيانات، فإن المخاطر لا تقتصر على السرقة أو التشويه فقط، بل قد تُستخدم في تدريب أنظمة هجومية ذكية. كذلك، تبرز الفجوة التشريعية والتنظيمية كخطر مستقبلي، حيث إن سرعة تطور الذكاء الاصطناعي تتجاوز بكثير وتيرة تطور القوانين. لا توجد حتى الآن معايير موحدة تحكم استخدام الذكاء الاصطناعي في الفضاء السيبراني، مما يسمح باستخدامه بطرق ضارة دون مساءلة قانونية واضحة، وخصوصًا في الهجمات العابرة للحدود[١٠].

وتجدر الإشارة أيضًا إلى أن الهجمات السيبرانية المدعومة بالذكاء الاصطناعي قد تكون أكثر صمتًا وتأثيرًا. فبفضل قدرتها على تحليل الأهداف واختيار أساليب الهجوم الأمثل، يمكن لهذه الأنظمة تنفيذ اختراقات دقيقة تستهدف شبكات حساسة، مثل البنية التحتية للطاقة أو المؤسسات الحكومية، دون أن يتم اكتشافها بسهولة. ورغم الفوائد الكبيرة التي يوفرها الذكاء الاصطناعي في مجال الأمن السيبراني، إلا أنه يفتح المجال أمام تهديدات مستقبلية أكثر تعقيدًا وصعوبة في المواجهة. هذه التحديات تتطلب من المؤسسات والحكومات تطوير أدوات قانونية وتقنية متقدمة، بالإضافة إلى بناء وعي عالمي حول كيفية استخدام الذكاء الاصطناعي بشكل مسؤول وآمن.

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

كمـا أن التعـاون الدولي في هذا المجال سـيكون عاملًا حاسمًا في الحد من مخاطره المحتملة.

المطلب الاول: اســتغلال الذكاء الاصطناعي في الهجمات السيبرانية

في الوقت الذي يُعتبر فيه الذكاء الاصطناعي أداة رئيسية لتحسين الأمن السيبراني وحماية الأنظمة الرقمية، إلا أنه في الجهة المقابلة يُستغل أيضًا من قبل المهاجمين في تنفيذ هجمات سيبرانية متطورة وذكية. يعد هذا الاسـتغلال للـذكاء الاصطناعي فـي الهجمـات السـيبرانية أحـد أكبـر التحديات التـي تواجه عالم الأمـن السـيبراني في العصر الحديث، حيث أن الذكاء الاصطناعي يعزز قدرة المهاجمين على شـن هجمات أكثر تعقيدًا، وأكثر دقة، وأسرع من أي وقت مضى[١١].

١. الهجمات الذكية باسـتخدام تقنيات التعلم الآلي (Machine Learning):

يستفيد المهاجمون من تقنيات التعلم الآلي لتطوير برمجيات خبيثـة قادرة على التعلـم والتكيف مع الأنظمـة التـي تحـاول الدفاع عنها. على سـبيل المثال، يمكن للبرمجيات الخبيثة التي تعتمد على تعلـم الآلـة أن تلتقـط أنماطًا في كيفية اكتشـاف الأنظمـة الأمنيـة لهـا وتعـدل سـلوكها لتجنـب اكتشـافها في المستقبل. هذا النوع من البرمجيات الخبيثة يمكنه التكيف بشكل ديناميكي مع الأنظمة المدافعـة عنها ويعمـل بطريقة أكثـر فعالية من البرمجيات التقليدية.

٢. هجمات التصيد الاحتيالي الذكية (Phishing Attacks):

تُعتبر هجمات التصيـد الاحتيالي واحدة من أكثر الأسـاليب التي يتم اسـتغلال الذكاء الاصطناعي فيها. عبر اسـتخدام تقنيات التعلم العميق (Deep Learning)، يسـتطيع المهاجمـون إنشـاء رسـائل تصيد احتيالي مخصصة ومقنعة للغاية، تحتـوي على تفاصيـل دقيقة تجعلهـا أكثر إقناعًا للضحية. على سبيل المثال، يمكن استخدام الذكاء الاصطناعي لتحليل البريد الإلكتروني للمستهدف (مثل رسـائل سابقة) لتوليد رسـائل تصيد تتنكر كرسـائل من جهات موثوقـة، مثل البنك أو مكان العمل، وبالتالي زيادة فرص نجاح الهجوم.

٣. إنشـاء البرمجيات الخبيثة التي يمكنها التكيف (Adaptive Malware):

مع استخدام الذكاء الاصطناعي، يمكن للمهاجمين تطوير برمجيات خبيثة قادرة على تغيير شـكلها وحيلتها لتجنب اكتشاف برامج الحماية. ما يسمى بـ البرمجيات الخبيثة المتغيرة (Polymorphic Malware) يمكنهـا التلاعب بشـيفرتها بشـكل مسـتمر، ممـا يجعلها صعبة الكشـف بواسـطة تقنيات الأمن التقليدية مثل تحليل التوقيعات .

٤. هجمـات الحرمـان مـن الخدمـة الموزعـة (DDoS) المدعومة بالذكاء الاصطناعي:

تسـتخدم بعـض الهجمـات المدعومـة بالـذكاء الاصطناعـي تقنيـات تعلـم الآلـة لتحليـل نقاط الضعف في شبكة أو موقع مستهدف، ومن ثم تنفيذ هجمات الحرمان من الخدمة الموزعة (DDoS) بشكل أكثر ذكاءً ودقة. الذكاء الاصطناعي يمكنه تحديد أهداف الهجوم الأكثر ضعفًا وتحديد أفضل طريقة لإغراق الخوادم بحركة مرور ضارة مما

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

يؤدي إلى توقف الخدمة[١٢].

٥. الهجمات على الأنظمة المدعومة بالذكاء الاصطناعي:

مع تزايد استخدام الذكاء الاصطناعي في حماية الأنظمة، يظهر نوع جديد من الهجمات التي تستهدف اختراق الأنظمة الذكية نفسها. يمكن للمهاجمين محاولة التلاعب في طريقة تعلم النظام الذكي، مثل إدخال بيانات مغلوطة لتوجيه النتائج في صالحهم، أو حتى التسبب في تعلم النظام سلوكيات خاطئة. يُطلق على هذا النوع من الهجمات «الهجوم على البيانات التدريبية»، وهو من التهديدات المتزايدة في الأنظمة المدعومة بالذكاء الاصطناعي.

٦. الهجمات على السيارات الذاتية القيادة والأنظمة الذكية:

بسبب الاستخدام المتزايد للذكاء الاصطناعي في السيارات الذاتية القيادة والطائرات دون طيار (UAVs)، قد تصبح هذه الأنظمة هدفًا للهجمات السيبرانية. يمكن استغلال الثغرات الأمنية في الأنظمة الذكية لهذه المركبات لتحويل مسارها أو تعطيل عملها بشكل يتسبب في حوادث خطيرة.

٧. التلاعب بالبيانات الصوتية والمرئية (Deepfakes):

تقنية الـ «Deepfake» تعتمد على الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صوتية مزورة بشكل دقيق، مما قد يُستخدم في تشويه الحقائق أو توجيه حملات تشويه ضد شخصيات عامة أو مؤسسات. هذه التقنية يمكن أن تستخدم في الهجمات السيبرانية لتضليل الجمهور أو المهاجمين من خلال التلاعب بالهوية.

إن استغلال الذكاء الاصطناعي في الهجمات السيبرانية يمثل تهديدًا كبيرًا، ويجب على المؤسسات والشركات أن تكون على وعي تام بالتطورات السريعة في هذا المجال. المهاجمون يستغلون الذكاء الاصطناعي لزيادة تعقيد الهجمات وتجاوز الأنظمة التقليدية، مما يجعل مواجهة هذه التهديدات يتطلب تطوير أدوات وتقنيات متقدمة للحماية. كما يفرض هذا الوضع ضرورة التعاون بين الحكومات، المؤسسات، ومجتمع البحث العلمي لمواكبة التطورات السريعة في مجال الذكاء الاصطناعي وتطوير استراتيجيات جديدة لمكافحة هذه الهجمات المعقدة[١٣].

المطلب الاول: تحديات الخصوصية وسوء استخدام البيانات.

تعتبر الخصوصية وحماية البيانات من أبرز القضايا التي تظهر في سياق تطبيقات الذكاء الاصطناعي في الأمن السيبراني. في حين أن الذكاء الاصطناعي يوفر فوائد كبيرة في تعزيز الأمان وحماية الأنظمة من الهجمات، فإنه يُعنى أيضًا بالكميات الكبيرة من البيانات الحساسة والشخصية التي يتم جمعها وتحليلها. ومع هذه الفوائد، تزداد المخاوف المتعلقة بتسريب البيانات، سوء استخدامها، و انتهاك حقوق الخصوصية.

تحتاج الأنظمة المدعومة بالذكاء الاصطناعي إلى كميات ضخمة من البيانات لتدريب نماذج التعلم الآلي وتحسين أدائها. هذه البيانات قد تشمل

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

معلومات شخصية وحساسة مثل سجلات التصفح، البيانات الطبية، رسائل البريد الإلكتروني، والموقع الجغرافي. إذن، تكمن المشكلة الأولى في أن معظم هذه الأنظمة تحتاج إلى جمع بيانات واسعة من المستخدمين أو من أنظمة مختلفة. التحدي هنا يكمن في أن جمع هذه البيانات قد يتم دون إذن صريح أو قد يتجاوز حدود الاستخدام الأخلاقي المسموح بها، مما يؤدي إلى انتهاك الخصوصية الشخصية للمستخدمين. فعلى سبيل المثال، قد تقوم بعض الشركات بجمع البيانات وتحليلها بطريقة غير شفافة أو دون اطلاع المستخدم على كيفية استخدام هذه البيانات.

مع الاعتماد الكبير على البيانات في أنظمة الذكاء الاصطناعي، يظهر تحدٍ آخر وهو إمكانية التلاعب بالبيانات لتوجيه نتائج الذكاء الاصطناعي بما يخدم مصالح معينة. إذا تم تسميم البيانات ، يمكن أن يتم تدريب النظام على بيانات مغلوطة تؤدي إلى قرارات خاطئة أو لا أخلاقية.على سبيل المثال، في حال تم اختراق قاعدة بيانات تدريبية لذكاء اصطناعي، قد تُدخل بيانات ضارة تؤدي إلى تفعيل هجوم سيبراني أو تحيزات عنصرية في نتائج النظام. ما قد يُسهل تهديدات مثل اختراق البيانات أو حتى التلاعب في الانتخابات العامة أو تلاعب في الخدمات المالية.(١٤)

غالبًا ما تفتقر بعض الأنظمة التي تعتمد على الذكاء الاصطناعي إلى آليات قوية للرقابة على كيفية استخدام البيانات، مما يعزز فرص الاستغلال غير المشروع. حيث يتم استخدام البيانات من قبل أطراف ثالثة أو كيانات تجارية بشكل غير قانوني أو غير أخلاقي بهدف تحقيق مكاسب مالية أو تسويق مستهدف، دون أن يتمكن المستخدم من التحكم في تلك الاستخدامات.في العديد من الحالات، لا يتم توفير معلومات دقيقة للمستخدمين حول كيفية جمع و استخدام بياناتهم، ولا تُتاح لهم الخيارات للتحكم في هذا. ففي حال غياب قوانين فعالة مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، قد تبقى هذه الممارسات غير خاضعة للمساءلة القانونية(١٥).

والنماذج المدعومة بالذكاء الاصطناعي، خصوصًا في مجالات مثل التعرف على الوجوه، تحليل الصوت، أو حتى معالجة النصوص، تعتمد على تخزين معلومات دقيقة حول الأشخاص، مما يثير القلق بشأن التوثيق للبيانات الشخصية. هذه الأنظمة يمكن أن تُستخدم للتعرف على الأفراد في الحياة اليومية، مما يؤدي إلى مخاطر كبيرة على الخصوصية. على سبيل المثال، يمكن لبعض الأنظمة التي تستخدم الذكاء الاصطناعي في التعرف على الوجوه في الأماكن العامة أن تشكل تهديدًا للحرية الشخصية، حيث يتم تعقب الأفراد دون موافقتهم أو علمهم، وهو ما يعارض بشكل مباشر مبادئ الخصوصية.

وتسعى العديد من الشركات إلى جمع أكبر قدر ممكن من البيانات الشخصية حول المستخدمين لتحسين استهدافها الدعائي وتسويق منتجاتها بشكل أكثر فاعلية. لكن هذه الممارسات التجارية تثير أسئلة حول حماية البيانات الشخصية وحقوق المستخدمين في التحكم بكيفية استخدام بياناتهم. ففي بعض الحالات، قد يتم بيع هذه البيانات

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

أو استخدامها دون علم الأفراد.من أمثلة ذلك أنظمة الذكاء الاصطناعي التي تقوم بتحليل سلوك المستخدمين على الإنترنت و تخصيص الإعلانات بناءً على البيانات الشخصية، الأمر الذي قد يتجاوز حدود الخصوصية المتوقعة.

بينما يوفر الذكاء الاصطناعي إمكانيات هائلة لتعزيز الأمن السيبراني، إلا أن هناك مخاطر جدية على الخصوصية وسوء استخدام البيانات التي يجب أن يتم التعامل معها بحذر. إن غياب قوانين فعّالة أو الشفافية في كيفية استخدام البيانات يجعل الأفراد عرضة للاستغلال غير المشروع. من الضروري أن يتم وضع إطار قانوني وأخلاقي يحمي خصوصية الأفراد ويضمن استخدام البيانات بشكل آمن وعادل في تطبيقات الذكاء الاصطناعي.

المطلب الثاني: الفجوات التشريعية وألاخلاقية في التعامل مع الذكاء الاصطناعي.

بينما يُعد الذكاء الاصطناعي (AI) من الأدوات القوية في مجال الأمن السيبراني، فإن استخدامه يثير العديد من القضايا التشريعية والأخلاقية التي لم يتم التعامل معها بشكل كافٍ حتى الآن. هذه الفجوات تشكل تحديات كبيرة، سواء من الناحية القانونية أو من ناحية القيم الإنسانية، ويجب معالجتها لضمان أن يُستخدم الذكاء الاصطناعي بشكل آمن وعادل(١٦).

١. الفجوات التشريعية في استخدام الذكاء الاصطناعي

تُعد الفجوات التشريعية واحدة من أبرز التحديات التي يواجهها الذكاء الاصطناعي في المجال السيبراني. فالتشريعات الحالية لا تواكب التطورات السريعة في تقنيات الذكاء الاصطناعي، مما يسمح بوجود ثغرات في حماية البيانات وأمن المعلومات.

أ) غياب التشريعات الموحدة والقيود القانونية: إحدى أكبر المشكلات هي غياب التشريعات الموحدة التي تنظم استخدام الذكاء الاصطناعي في الأمن السيبراني عبر الحدود. في الوقت الذي تسعى فيه بعض الدول إلى وضع قوانين محلية لتنظيم استخدام الذكاء الاصطناعي، إلا أن هذه القوانين غالبًا ما تكون غير مكتملة أو غير متوافقة مع بعضها البعض. ذلك يجعل من الصعب وضع إطار قانوني عالمي يضمن استخدام الذكاء الاصطناعي بشكل آمن ومنظم عبر جميع الدول.

ب) نقص قوانين مكافحة التلاعب بالبيانات: الذكاء الاصطناعي يعتمد بشكل كبير على البيانات، وهناك تحدٍ قانوني يتعلق بكيفية حماية البيانات الشخصية وحمايتها من التلاعب أو الاستغلال من قبل الأنظمة المدعومة بالذكاء الاصطناعي. فعلى الرغم من وجود قوانين مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، إلا أن هذه القوانين غالبًا ما تكون غير كافية لمواكبة التطورات السريعة في الذكاء الاصطناعي، مما يفتح الباب أمام انتهاكات الخصوصية و التلاعب بالبيانات.

ج) التشريعات المتعلقة بالمسؤولية القانونية: من المشكلات التشريعية التي تبرز أيضًا هي

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

تحديد المسؤولية القانونية في حال وقوع هجوم سيبراني باستخدام الذكاء الاصطناعي. في حال فشل نظام سيبراني مدعوم بالذكاء الاصطناعي في اكتشاف هجوم أو التعاطي معه، من يتحمل المسؤولية؟ هل هي الشركة التي صممت النظام؟ أم الحكومة؟ أم المستخدمون؟ وهذا الغموض في تحديد المسؤولية القانونية يزيد من صعوبة تنفيذ الإجراءات القانونية ضد الجهات المذنبَة في حال وقوع اختراقات.

٢. الفجوات الأخلاقية في استخدام الذكاء الاصطناعي

إلى جانب القضايا التشريعية، هناك قضايا أخلاقية كبيرة تتعلق باستخدام الذكاء الاصطناعي في المجال السيبراني. هذه القضايا تتعلق بمدى التوازن بين الأمان الشخصي وحقوق الأفراد وفعالية الأنظمة الأمنية.

أ) التمييز والتحيز في الأنظمة الذكية: تقنيات الذكاء الاصطناعي يمكن أن تكون عرضة للتحيزات المدمرة في حال تدريبها على بيانات غير ممثلة أو منحازة. على سبيل المثال، في حال تم تدريب نظام أمني باستخدام بيانات قد تتضمن تمييزًا على أساس العرق أو الجنس أو العمر، فإن النظام قد يطور تحيزًا ضد فئات معينة من الأشخاص. هذا يمكن أن يؤدي إلى نتائج غير عادلة في الكشف عن تهديدات أو حتى اتخاذ قرارات تتعلق بالأمن.

ب) استخدام الذكاء الاصطناعي في المراقبة الشاملة: استخدام الذكاء الاصطناعي في مجال الأمن السيبراني يمكن أن يؤدي إلى زيادة المراقبة والتجسس على الأفراد بشكل مفرط، مما يثير القلق بشأن الخصوصية. في العديد من البلدان، قد يُستخدم الذكاء الاصطناعي لمراقبة حركة الإنترنت وتحليل بيانات المستخدمين بشكل يفوق الحدود المقبولة أخلاقيًا. هذه الأنظمة يمكن أن تكون انتهاكًا للحقوق الإنسانية، مثل الحق في الخصوصية.

ج) الاستجابة التلقائية للتهديدات: بعض الأنظمة المدعومة بالذكاء الاصطناعي قد تتخذ قرارات تلقائية في حال اكتشاف تهديدات سيبرانية، مثل عزل الأجهزة أو حظر الحسابات. لكن قد تثير هذه الإجراءات مخاوف أخلاقية تتعلق بمصداقية النظام في اتخاذ قرارات دقيقة وعادلة. فمثلًا، إذا تم حظر حساب أو جهاز بناءً على تقييم خاطئ للنظام.

د) الهجمات الهجينة والأخلاقية: الذكاء الاصطناعي قد يُستخدم أيضًا في الهجمات الهجينة التي تهدف إلى تحقيق أغراض غير أخلاقية مثل التضليل الإعلامي أو تشويه السمعة. فعلى سبيل المثال، يمكن استخدام تقنيات التزييف العميق لإنشاء مقاطع فيديو مزيفة لأشخاص أو مؤسسات بغرض التشهير أو الإضرار بسمعتها. ويثير هذا النوع من الهجمات أسئلة أخلاقية حول الحدود بين حرية التعبير و التحايل على الحقيقة.

٣. الحاجة إلى إطار تشريعي وأخلاقي متكامل

الذكاء الاصطناعي في الأمن السيبراني يتطلب إطارًا قانونيًا وأخلاقيًا متكاملًا يعالج كل هذه الفجوات بشكل فعّال. يتطلب الأمر تشريعات دولية موحدة لضمان توافق الأنظمة وحمايتها

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

من الاستغلال السيء، بالإضافة إلى ممارسات أخلاقية صارمة لتقليل تأثير التحيز وحماية خصوصية الأفراد.

و أن الفجوات التشريعية والأخلاقية في التعامل مع الذكاء الاصطناعي في المجال السيبراني تمثل تحديات كبيرة. بينما يقدم الذكاء الاصطناعي حلولًا فعالة للتصدي للهجمات السيبرانية، فإن غياب القوانين الواضحة والإرشادات الأخلاقية قد يؤدي إلى استخدام غير مسؤول أو ضار لهذه التقنية. لذلك، من الضروري على صعيد الحكومات والمؤسسات أن تتعاون لوضع معايير تشريعية وأخلاقية تكفل الاستخدام الآمن والموثوق للذكاء الاصطناعي في هذا المجال[١٧].

المطلب الثالث: دور التقنيات الحديثة في دعم الأمن السيبراني

تُستخدم التقنيات المتطورة في دعم وتعزيز الحماية الرقمية من خلال عدد من التطبيقات، منها ما يلي[١٨] :

أ. إدارة كميات ضخمة من البيانات: تشهد الخوادم أنشطة كثيرة يوميًا، ما يؤدي إلى انتقال كميات هائلة من البيانات بين المستخدمين والبنية التحتية. هذا التزايد في حجم البيانات يفرض تحديات كبيرة على المختصين في الأمن الرقمي عند محاولة فحص كل حركة وتحليل المخاطر. وتساعد الحلول التقنية المتقدمة في متابعة حركة المرور وتحليل النشاط بدقة، مما يسهم في التعرف التلقائي على المخاطر المحتملة.

ب. التنبؤ بالتهديدات المستقبلية: نظرًا لتعدد مصادر البيانات وتشعبها، فإن التنبؤ بالمخاطر قبل حدوثها يمثل تحديًا. إلا أن أدوات التحليل الحديثة قادرة على معالجة كميات هائلة من المعلومات في وقت وجيز، مما يساعد على الكشف المبكر عن الأنشطة المشبوهة، وتقليل الجهد والموارد المطلوبة، بالإضافة إلى تعزيز قدرة المؤسسات على الاستجابة الوقائية.

ج. تسريع عملية اكتشاف المخاطر: أصبح الكشف السريع عن المخاطر أمرًا بالغ الأهمية، حيث أبلغت ٤٢٪ من المؤسسات عن زيادة في التهديدات التي تتطلب استجابة فورية. وتُظهر الحلول التقنية قدرتها على تحليل البيانات الضخمة بسرعة وكفاءة، مما يحسن من مستوى الحماية. وأشارت تقارير إلى أن أكثر من نصف المؤسسات تعاني من ضغوط في التعامل مع التحليلات الأمنية، بينما صرّح ٢٣٪ منها بعدم القدرة على التحقق الفعّال من التهديدات.

د. خفض التكاليف التشغيلية: تعاني العديد من المؤسسات من خسائر مالية كبيرة بسبب الاختراقات. وتشير الدراسات إلى أن استخدام الأدوات التكنولوجية الحديثة يوفر في التكاليف بنسبة تصل إلى ٨٠٪، حيث تنخفض التكلفة السنوية من ٦,٧١ مليون دولار إلى ٢,٩ مليون دولار للمؤسسات التي تعتمد على هذه الحلول. ويواجه استخدام الحلول التقنية المتطورة في المجال الأمني عددًا من العقبات، من أبرزها ما يلي[١٩] :

أ. صعوبات الدمج مع الأنظمة الحالية: غالبًا ما يواجه صناع القرار معوقات تتعلق بتكامل الحلول

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

الحديثــة مع البنى التحتيــة القائمة، خصوصًا في ظل محاولات الجهات الخبيثة التكيف السريع مع كل جديد.

ب. متطلبــات البنية التحتية: تفرض هذه الأدوات احتياجات كبيرة من حيث الاســتثمار في قدرات المعالجــة والتخزين، فضلًا عن ضرورة إنشــاء مراكز بيانات قوية.

ج. نقــص الكفــاءات المؤهلــة: تُعد قلــة الخبراء القادريــن على التعامل مع هذه التقنيات أحد أبرز التحديات، بالإضافة إلى الحاجة إلى بيانات كافية وتوظيف الأدوات الملائمة بطريقة فعالة.

د. محدوديــة أدوات التنقيــب عــن البيانات: تمثل صعوبة الحصول على أدوات فعالة لاستكشــاف وتحليــل البيانــات أحــد التحديــات التــي تواجه المؤسسات الراغبة في تطبيق الحلول المتقدمة.

هـ. اســتخدام مــزدوج من قبــل المهاجم يمكن أن تُســتخدم هذه الأدوات من قبــل الجهات المهاجمة أيضًا، ما يجعلها ســلاحًا ذا حدين، يزيد من تعقيد المعركة الرقمية ويزيد من تطور الهجمات.

و. فجوة بين المؤسســات والمهاجمين: في الوقت الــذي تفرض فيه المؤسســات قواعد وسياســات صارمــة للحد من اســتخدام هذه الحلول، يســتفيد المهاجمــون من حرية أكبر فــي التلاعب بالتقنية واستغلالها.

الخاتمة

فــي الختــام، يمثل الأمــن الســيبراني في عصر الذكاء الاصطناعي تحديــاً متزايد التعقيد يتطلب جهوداً متواصلة واستراتيجيات متطورة لمواكبة التطورات السريعة في هذا المجال. وعلى الرغم من الفوائد الكبيرة التي يقدمها الذكاء الاصطناعي في تحســين الدفاعات السيبرانية، إلا أن المخاطر المرتبطة بســوء اســتخدامه والتحديات القانونية والأخلاقيــة تفــرض علــى المختصيــن وصنّاع القــرار تبني حلول متوازنــة تضمن الحماية دون الإخلال بالخصوصية والحقوق الرقمية. المستقبل يتطلــب تعاونــاً دولياً وتشــريعات مرنة وتطوير تقنيــات أكثــر شــفافية وعدالة لضمان اســتخدام الذكاء الاصطناعي كأداة للأمن لا كتهديد له ، لذا توصلنا الى عدد من الاستنتاجات والتوصيات :

أولا: الاستنتاجات

١.يمثــل الــذكاء الاصطناعــي ثــورة حقيقية في تعزيز الأمن السيبراني من خلال استخدام تقنيات مثــل التعلم الآلــي وتحليل البيانــات الكبيرة. فهو يساعد في الكشف المبكر عن التهديدات، اكتشاف البرمجيــات الخبيثــة، وتحليل الأنماط الســلوكية الشاذة داخل الشبكات.

٢.رغــم الفوائد التي يوفرها الذكاء الاصطناعي، فإنه يعرض الأنظمة الســيبرانية لمخاطر جديدة. فالمهاجمــون يمكنهــم اســتخدام نفــس التقنيــات المدعومــة بالــذكاء الاصطناعــي لاســتهداف الأنظمــة، مثــل اســتخدام البرمجيــات الخبيثــة

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

المتكيفة، وتحسين هجمات التصيد الاحتيالي، وتوليد مقاطع deepfake، مما يخلق بيئة أكثر تعقيدًا بالنسبة للأمن السيبراني.

٣.ما زالت هناك فجوات كبيرة في التشريعات المتعلقة باستخدام الذكاء الاصطناعي في المجال السيبراني. التشريعات الحالية غير كافية لمواكبة التطورات السريعة في هذه التقنية، مما يؤدي إلى غياب آليات تنظيم فعالة لمنع إساءة استخدام الذكاء الاصطناعي. إضافة إلى ذلك، هناك قضايا أخلاقية، مثل التحيز في الأنظمة الذكية، وتهديد الخصوصية، والاستخدام المفرط للمراقبة.

٤.ستستمر التحديات في الظهور مع تقدم الذكاء الاصطناعي في الأمن السيبراني. ستتطلب هذه التحديات استراتيجيات دفاعية ذكية للغاية يمكنها التكيف مع أنواع الهجمات السيبرانية الجديدة. كما أن تطوير الذكاء الاصطناعي بشكل أسرع من تطور التشريعات سيستمر في خلق فجوات قانونية وأخلاقية.

ثانيا: التوصيات

١.تطوير تشريعات وأطر قانونية موحدة: يجب أن تسعى الحكومات والمنظمات الدولية إلى وضع قوانين وتشريعات موحدة تنظم استخدام الذكاء الاصطناعي في الأمن السيبراني، بما يتماشى مع المعايير الدولية. هذه التشريعات يجب أن تغطي جميع جوانب الذكاء الاصطناعي بما في ذلك حماية الخصوصية، والمراقبة، ومسؤولية الأنظمة الذكية في حال حدوث اختراقات أو أخطاء.

٢.استثمار في البحث والتطوير لتحسين الأمن السيبراني: ينبغي تعزيز استثمارات البحث والتطوير في تقنيات الذكاء الاصطناعي بحيث تصبح أكثر قدرة على التنبؤ بالتهديدات المستقبلية والاستجابة لها بشكل استباقي. كما يجب تطوير أدوات متقدمة للتعامل مع البرمجيات الخبيثة المتكيفة التي تستخدم الذكاء الاصطناعي.

٣.التعاون بين القطاعين العام والخاص: التعاون بين الحكومات والشركات يعد أمرًا بالغ الأهمية من أجل مشاركة المعلومات المتعلقة بالتهديدات والتهديدات المتطورة. يجب أن يتم هذا التعاون أيضًا في إطار تشريعي يضمن استخدام الذكاء الاصطناعي بشكل مسؤول وآمن.

٤.وضع معايير أخلاقية واضحة: يجب أن تكون هناك معايير أخلاقية واضحة للاستخدام المسؤول للذكاء الاصطناعي في الأمن السيبراني. هذه المعايير يجب أن تعالج قضايا مثل التحيز في الأنظمة الذكية، حماية الخصوصية، و الاستجابة العادلة للتهديدات. كما يجب على المنظمات أن تتبنى سياسة الشفافية في كيفية استخدام الذكاء الاصطناعي في عملياتها الأمنية.

٥.تدريب العاملين على استخدام الذكاء الاصطناعي بشكل آمن: من المهم توفير التدريب والتثقيف للمختصين في مجال الأمن السيبراني حول كيفية استخدام تقنيات الذكاء الاصطناعي بشكل آمن وفعّال. هذا يشمل تطوير القدرة على التنبؤ بالتهديدات وتقييم المخاطر المحتملة المتعلقة باستخدام الأنظمة الذكية.

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

٦.تحسين الشفافية في الأنظمة الذكية: يجب تحسين الشفافية في الأنظمة المدعومة بالذكاء الاصطناعي من خلال وضع آليات لتفسير قرارات الأنظمة. عندما تكون الأنظمة الذكية قادرة على اتخاذ قرارات بشكل مستقل، يجب أن تكون هذه القرارات قابلة للفهم والمراجعة من قبل البشر، خاصة في الأنظمة التي قد تؤثر على الأشخاص أو المجتمع.

المصادر والمراجع

أولا:المصادر العربية

١.الأمين، دبار محمد، و جمال الدين، بابو. (٢٠٢٤). تداعيات الذكاء الاصطناعي على الأمن القومي. Journal of Private Law، ٢(١)، ١٠٠-١٢٢.

٢.حداوي، أميرة هاتف، و مسلم، ضرغام علي، و محمد، صفاء تايه. (٢٠٢٣). القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات-دراسة تحليلة لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف. مجلة العلوم الإنسانية والطبيعية، ٥(١).

٣.دحماني، محمد. (٢٠٢٣). الذكاء الاصناعي كآلية لتعزيز الامن السيبراني. مجلة الفكر القانوني والسياسي، ٧(٢)، ٥٩٧-٦٠٨.

٤.درار، خديجة محمد. أخلاقيات الذكاء الاصطناعي والروبوت: دراسة تحليلة. المجلة الدولية لعلوم المكتبات والمعلومات، ٦(٣)، ٢٣٧-٢٧١.

٥.العتيبي، عبدالرحمن بجاد شارع. (٢٠٢٠). دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ (رسالة ماجستير). جامعة نايف العربية للعوم الأمنية.

٦.مختار، محمد. (٢٠٢٣). الأمن السيبراني مفاهيم المستقبل، مجلة اتجاهات الأحداث، (٢)، ٦-٧.

٧.المصري، فرح محمد. (٢٠٢٤). دور الذكاء الاصطناعي في تحسين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، ٣(٢).

ثانيا: المصادر الأجنبية

1.Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE.

2. Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

tering approach for industrial IoT networks. IEEE Internet of Things Journal, 10(9), 7884-7892.

8. Umezawa, Y., Umezawa, K., & Sato, H. (1995). Selectivity coefficients for ion-selective electrodes: Recommended methods for reporting KA, Bpot values (Technical Report). Pure and applied chemistry, 67(3), 507-518.

الهوامش

(١)الأمين، دبار محمد، و جمال الدين، بابو. (٢٠٢٤). تداعيات الذكاء الاصطناعي على الأمن القومي. Journal of Private Law، ٢(١)، ١٠٠-١٢٢، ص١٢.

(٢) حداوي، أميرة هاتف، و مسلم، ضرغام علي، و محمد، صفاء تايه. (٢٠٢٣). القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات-دراسة تحليلة لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف. مجلة العلوم الإنسانية والطبيعية، ٥(١)، ص١٨١.

(٣) دحماني، محمد. (٢٠٢٣). الذكاء الاصناعي كأليـة لتعزيـز الامـن السـيبراني. مجلـة الفكر القانوني والسياسي،ص٦٤.

(٤) درار، خديجة محمد. أخلاقيات الذكاء الاصطناعي والروبوت: دراسة تحليلة. المجلة

3. Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

4. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3.

5.Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

6.Bhardwaj, A., Alshehri, M. D., Kaushik, K., Alyamani, H. J., & Kumar, M. (2022). (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. Journal of Electronic Imaging, 31(6), 061802-061802.

7. Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clus-

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

الدوليــة لعلوم المكتبات والمعلومات، ٦(٣)، ص ١٢.

(٥) العتيبي، عبدالرحمن بجاد شارع. (٢٠٢٠). دور الأمــن الســيبراني في تحقيــق رؤية ٢٠٣٠ (رســالة ماجســتير). جامعة نايف العربية للعوم الأمنية، ص١٨٧.

(٦) مختار، محمد. (٢٠٢٣). الأمن الســيبراني مفاهيم المســتقبل، مجلة اتجاهات الأحداث، (٢)، ص٢٢١.

(٧) مختار، محمد، المصدر السابق، ص٣٩٨.

(٨) المصري، فرح محمد. (٢٠٢٤). دور الذكاء الاصطناعي في تحســين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، ٣(٢)/ ص١٢٧.

(9) Dambe, S., Gochhait, S., & Ray, S. (2023, November). The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88-93). IEEE,p33.

(10) Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837. Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S (2021). ,p44.

(11) Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016),p18.

(12) Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28), e3-e3, p276.

(13) Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474,p132.

(14) Bhardwaj, A., Alshehri, M. D., Kaushik, K., Alyamani, H. J., & Kumar, M. (2022). (Retracted) Secure framework against cyber attacks on cyber-physical robotic systems. Journal of Electronic Imaging, 31(6), 061802-061802,p121.

مجلّة نصف سنوية محكّمة تصدر عن قسم الدراسات السياسية والاستراتيجية في بيت الحكمة - بغداد
رقم إيداع مجلة دراسات سياسية وأستراتيجية في دار الكتب والوثائق ٦٧٨ لسنة ٢٠٠٩
رقم الإيداع الدولي ISSN 2223-9464
Info@baytalhikma.iq

(15) Chithaluru, P., Al-Turjman, F., Kumar, M., & Stephan, T. (2023). Computational-intelligence-inspired adaptive opportunistic clustering approach for industrial IoT networks. IEEE Internet of Things Journal, 10(9), 7884-7892,p390.

(16) Umezawa, Y., Umezawa, K., & Sato, H. (1995). Selectivity coefficients for ion-selective electrodes: Recommended methods for reporting KA, Bpot values (Technical Report). Pure and applied chemistry, 67(3), 507-518.,p40.

(١٧) المصري، فرح محمد. (٢٠٢٤). دور الذكاء الاصطناعي في تحسين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، ٣(٢)، ص٢٨٥.

(١٨) حداوي، أميرة هاتف، و مسلم، ضرغام علي، و محمد، صفاء تايه. (٢٠٢٣). القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات-دراسة تحليلة لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف. مجلة العلوم الإنسانية والطبيعية، ٥(١)، ص٣٣.

(١٩) الأمين، دبار محمد، و جمال الدين، بابو. (٢٠٢٤). تداعيات الذكاء الاصطناعي على الأمن القومي. Journal of Private Law، ٢(١)، ١٠٠-١٢٢، ص٢٣.

الملخص

التحديات المستقبلية للأمن السيبراني في عصر الذكاء الاصطناعي تتنوع وتعكس تعقيدات وتهديدات جديدة في هذا المجال. مع تزايد الاعتماد على الذكاء الاصطناعي لتحسين الدفاعات السيبرانية، يواجه هذا المجال تحديات كبيرة تتعلق بالتكنولوجيا نفسها. من جهة، يمكن للذكاء الاصطناعي أن يساهم بشكل فعال في تعزيز الأمن من خلال تحسين القدرة على اكتشاف التهديدات وتحليل البيانات الكبيرة بشكل أسرع وأكثر دقة. ومع ذلك، تكمن التحديات في إمكانية استغلال هذه التقنيات من قبل المهاجمين الذين قد يستخدمون الذكاء الاصطناعي لتطوير هجمات متطورة وذكية تتجاوز الأنظمة الأمنية التقليدية. ومن أبرز المخاوف المستقبلية هي المخاطر المرتبطة بسوء استخدام الذكاء الاصطناعي، حيث يمكن أن يتم استغلاله في الهجمات الهجينة أو الهجمات الذكية التي تكون صعبة على الأنظمة الحالية في اكتشافها. كما أن التحديات القانونية تزداد بسبب تزايد استخدام الذكاء الاصطناعي في مجالات حساسة مثل المراقبة والتحليل، مما يثير قضايا تتعلق بـ الخصوصية و حماية البيانات. بالإضافة إلى ذلك، تتسم الأنظمة المدعومة بالذكاء الاصطناعي بأنها قد تكون عرضة للتحايل والتلاعب في حال تم تدريبها على بيانات غير موثوقة أو متحيزة.

الكلمات المفتاحية: الامن السيبراني، الذكاء الاصطناعي، الهجمات السيبرانية، التقنيات.

Semi-annual Quarterly journal issued byPolitical and Strategic Studies In Bayt Al-Hikma Baghdad
No.of deposit at Political and Strategic Studies(678)2009
ISSN.2223-9464
Info@baytalhikma.iq

Abstract

Future cybersecurity challenges in the age of artificial intelligence are diverse and reflect new complexities and threats. With the increasing reliance on AI to improve cyber defenses, the field faces significant challenges related to the technology itself. On the one hand, AI can effectively contribute to enhancing security by improving the ability to detect threats and analyze big data faster and more accurately. However, challenges lie in the potential exploitation of these technologies by attackers who may use AI to develop sophisticated and intelligent attacks that bypass traditional security systems. One of the most prominent future concerns is the risk associated with the misuse of AI, as it could be exploited in hybrid or intelligent attacks that are difficult for current systems to detect. Legal challenges are also increasing due to the increasing use of AI in sensitive areas such as surveillance and analytics, raising issues related to privacy and data protection. In addition, AI-powered systems may be vulnerable to fraud and manipulation if trained on unreliable or biased data.

Keywords: Cybersecurity, Artificial Intelligence, Cyber Attacks, Technologies