

أي دور للذكاء الاصطناعي في مواجهة الجريمة السيبرانية؟

What role does artificial intelligence play in combating cybercrime?
 Quel rôle joue l'intelligence artificielle dans la lutte contre la cybercriminalité ?

سعيد زيوش¹ * الطاهر بومدفع²

تاريخ الإرسال: 2025/03/12 تاريخ القبول: 2025/11/25 تاريخ النشر: 2025/12/31

ملخص:

لقد أحدثت تقنية الذكاء الاصطناعي ثورة في الطريقة التي نحمي بها أصولنا الرقمية وكل ما يمت بصلة للواقع الرقمي، وقد سمعنا جميعاً عن الذكاء الاصطناعي وكيف بدأ بالتغلغل في كل خصوصياتنا، في هذه المقالة البحثية سنناقش دوره في الحماية من الجريمة السيبرانية، وسنحاول أن نستكشف كيف يمكن استخدام الذكاء الاصطناعي كأداة قوية لمكافحة المجرمين على الإنترنت، وكيف يمكنه من تحسين التدابير الأمنية الحالية، وسننظر في بعض التحديات والفرص المحتملة التي تطرحها تقنية منع الجرائم الإلكترونية القائمة على الذكاء الاصطناعي، لقد اعتمادنا على المنهج الوصفي باعتباره المنهج الأنسب لموضوعنا وكانت أهم النتائج التي توصلنا إليها أنه لا مفر من استخدام الذكاء الاصطناعي في جميع مناحي الحياة اليومية مع التأكيد على تدابير الأمن السيبراني، كما أنه يجب إشراك جميع الفاعلين في المجتمع في بلورة فكرة رقمية مبنية على الذكاء الاصطناعي لحماية المجتمع ومختلف بنياته.

الكلمات المفتاحية: الذكاء الاصطناعي، الجريمة السيبرانية، التطبيقات، التحديات، الأهداف.

Abstract:

Artificial intelligence (AI) technology has revolutionized the way we protect our digital assets and everything related to the digital world. We've all heard about AI and how it has begun to infiltrate our privacy. In this research paper, we will discuss its role in protecting against cybercrime. We will explore how AI can be used as a powerful tool to combat online criminals and how it can improve current security measures. We will also examine some of the potential challenges and opportunities posed by AI-based cybercrime prevention technology. We adopted a descriptive approach as the most appropriate approach for our topic. Our most important findings are that the use of AI is inevitable in all aspects of daily life, with an emphasis on cybersecurity measures. It is also imperative to engage all stakeholders in developing an AI-based digital strategy to protect society and its various structures.

Keywords : Artificial Intelligence ; Cybercrime ; Applications ; Challenges ; Objectives.

Résumé :

L'intelligence artificielle (IA) a révolutionné notre façon de protéger nos actifs numériques et tout ce qui touche à la réalité numérique. Nous avons tous entendu parler de l'IA et de son intrusion dans notre vie privée. Dans ce document de recherche, nous aborderons son rôle dans la protection contre la cybercriminalité et explorerons comment l'IA peut être utilisée comme un puissant outil de lutte contre les cybercriminels. Nous avons adopté l'approche descriptive, la plus adaptée à notre sujet. Nos principales conclusions sont que l'utilisation de l'IA est inévitable dans tous les aspects de la vie quotidienne, notamment en matière de cybersécurité. Il est également nécessaire d'impliquer tous les acteurs de la société dans le développement d'un concept numérique basé sur l'IA pour protéger la société et ses différentes structures.

* سعيد زيوش

¹ Ziouche Said, University Center Of Barika, Algeria, said.ziouche@cu-barika.dz

² Boumedfa Tahar, University Of Medea, Algeria, boumedfa.tahar@univ-medea.dz

Mots clés : Intelligence Artificielle ;Cybercriminalité ; Applications ; Défis ; Objectifs.

مقدمة:

أدت الحوادث الأمنية الأخيرة، مثل هجمات التصيد الاحتيالي المستندة إلى الذكاء الاصطناعي التوليدي في عام 2023 واختراق بيانات مستخدم Facebook في عام 2018 ، إلى إعادة العلاقة بين الذكاء الاصطناعي والجريمة الإلكترونية إلى المحادثات السائدة على وجه الخصوص في ضوء النمو السريع الأخير لاستخدام الذكاء الاصطناعي عبر الصناعات، وحتى في حياتنا الشخصية أصبح من المهم أكثر من أي وقت مضى لعامة الأفراد أن يثقوا في قدرة المؤسسة على إدارة أنظمة الذكاء الاصطناعي الخاصة بها بشكل صحيح وتأمين بيانات المستهلك ضد النشاط الإجرامي المتقدم (الغامدي، 2024، صفحة 21)

وإذا كنا جزءا من مؤسسة تتطلع إلى إدخال الذكاء الاصطناعي في أنظمة الأمن التشغيلي والسيبراني الخاصة بنا، فسنحتاج أولا إلى فهم ما يمكن أن يفعله الذكاء الاصطناعي لأعمالنا، ليس ذلك فحسب بل سنحتاج إلى معرفة الطرق التي يخترق بها مجرمو الإنترنت أنظمة الذكاء الاصطناعي للشركة أو المؤسسة لأغراض ضارة وحتى إنشاء أنظمة الذكاء الاصطناعي الخاصة بهم لتعطيل المؤسسات، يمكن أن تساعدنا حلول الأمن السيبراني القائمة على الذكاء الاصطناعي أيضا في مواجهة التهديدات التي تشكلها الجهات الفاعلة السيئة باستخدام الذكاء الاصطناعي (الغامدي، 2024، صفحة 33)

من هنا نطرح السؤالين التاليين:

- ماهي التهديدات السيبرانية المحتملة التي قد يشكلها الذكاء الاصطناعي على بيانات المؤسسة؟
- كيف يمكن للمؤسسة حماية نفسها من هذه التهديدات الرقمية الجديدة مع الاستمرار في الاستثمار في حلول الذكاء الاصطناعي.

1- الذكاء الاصطناعي وتأثيره على الأمن السيبراني:

عندما يتعلق الأمر بالأمن السيبراني، فإن الذكاء الاصطناعي لديه القدرة على أن يكون حاميا رائعا - ولكن ما هو الذكاء الاصطناعي بالضبط وكيف يفعل ذلك؟

يعرف الذكاء الاصطناعي بأنه "قدرة جهاز كمبيوتر أو روبوت يتحكم فيه الكمبيوتر على القيام بمهام يقوم بها البشر عادة لأنها تتطلب ذكاء بشريا وتمييزا" (العبيدي، 2021، صفحة 25) .

باختصار إنها قدرة الآلات على التفكير والتصرف مثل البشر، يستخدم البيانات والنماذج الخوارزمية المتقدمة لتحديد الاتجاهات واكتشاف الحالات الشاذة واتخاذ القرارات بنفسه، يمكنه زيادة العمليات والتنبؤ أو توقع النتائج والتعلم من التجربة والتكيف مع البيانات الجديدة، تُعد السيارات ذاتية القيادة (في بعض الدول المتقدمة)، والتسوق الشخصي، والمكانس

الكهربائية الروبوتية، والمساعدين المنزليين الذين يتم تنشيطهم صوتياً، وروبوتات الدردشة جزءاً من عالم الذكاء الاصطناعي الاستثنائي. (العبيدي، 2021، صفحة 26)

فمن المتوقع أن يصل سوق الذكاء الاصطناعي العالمي إلى 1,811.8 مليار دولار بحلول عام 2030، مما يدل على أنها صناعة سريعة النمو ولديها القدرة على تغيير طريقة عيشنا وعملنا، في الواقع، تتميز 77٪ من الأجهزة التي نستخدمها اليوم بشكل من أشكال تقنية الذكاء الاصطناعي، (الغامدي، 2024، صفحة 25) ولكن ماذا يعني هذا بالنسبة للأمن السيبراني؟

عندما يتعلق الأمر بالأمن السيبراني يُمكن أن يكون لجهاز الذكاء الاصطناعي تأثير كبير على مكافحة الجرائم الإلكترونية، أولاً يُمكن استخدامه لتحليل كميات كبيرة من البيانات بسرعة لتحديد الأنشطة المشبوهة وتنبيه المسؤولين عند اكتشاف تهديد ما بالإضافة إلى ذلك، يُمكن تدريب الذكاء الاصطناعي على التعرف على التهديدات المحتملة قبل حدوثها من خلال مراقبة سلوك المستخدم وتحليل أي تغييرات بمرور الوقت، أخيراً يُمكن أيضاً استخدام الأنظمة التي تعتمد على الذكاء الاصطناعي لنشر التدابير المضادة تلقائياً ضد الهجمات الإلكترونية في الوقت الفعلي.

يظهر تطبيق الذكاء الاصطناعي في الأمن السيبراني وعدداً كبيراً من المتوقع أن ينمو الذكاء الاصطناعي في سوق الأمن السيبراني بمعدل نمو سنوي مركب قدره 23.6٪ من عام 2020 إلى عام 2027 ليصل إلى 46.3 مليار دولار بحلول عام 2027، ومن المتوقع أن تكون هذه الزيادة مدعومة بمشهد التهديدات سريع التطور، والحاجة إلى تأمين نقاط نهاية أكثر من أي وقت مضى، والنقص الواسع النطاق في المهارات، والحاجة إلى الحد من خروقات البيانات والاستجابة بشكل أكثر فعالية للحوادث. (الغامدي، 2024، صفحة 27)

من الواضح أن الذكاء الاصطناعي يمكن أن يساعد الشركات والمؤسسات على حماية أصولها الرقمية بشكل أكثر فعالية من أي وقت مضى، ولكن هل يمكن أن يكون الذكاء الاصطناعي هو الأداة المثالية لمكافحة الجرائم الإلكترونية؟ وهل فوائد الذكاء الاصطناعي تفوق المخاطر؟

3- تطبيقات الذكاء الاصطناعي في الأمن السيبراني:

يتمتع الذكاء الاصطناعي بالقدرة على إحداث ثورة في الأمن السيبراني والسبب أنه يمكن استخدام الذكاء الاصطناعي لاكتشاف التهديدات السيبرانية المحتملة التي قد يفوتها المحللون البشريون، كما يمكن لخوارزميات الذكاء الاصطناعي أيضاً اكتشاف تغييرات التعليمات البرمجية ونقاط الضعف في النظام في الوقت الفعلي. (العلي، 2019، صفحة 36)

بالإضافة إلى ذلك يُمكن أن يتيح الذكاء الاصطناعي تقييمات مخاطر أكثر شمولاً عن طريق مسح حركة مرور الشبكة في جميع الأوقات بدلاً من مجرد دورية، ويمكن للأدوات التي تعتمد عليه من إنشاء خطة استجابة فردية للتعامل مع الاختراق.

ليس ذلك فحسب بل إن هذه الآلات قادرة على التعلم من التجربة، مما يعني أنها تتحسن مع كل فحص واستجابة تؤديها من خلال إجراء عمليات الفحص الآلي بشكل مستمر، كما يمكن للأنظمة التي تعمل بالطاقة الذكاء الاصطناعي اكتشاف الأنشطة غير العادية والإبلاغ عنها بسرعة - عادة قبل حدوث أي ضرر فعلي. فيما يلي بعض حالات الاستخدام الأكثر شيوعاً لمنظمة الذكاء الاصطناعي في الأمن السيبراني:

- اكتشاف التهديدات وتحليلها
- كشف التسلل ومنعه
- الكشف عن البرامج الضارة
- إدارة الثغرات الأمنية
- تحسين مركز عمليات الأمان (SOC)
- إدارة الهوية والوصول
- كشف الاحتيال
- أمن البيانات
- الحماية بكلمة مرور والمصادقة
- أمن الشبكة
- الكشف عن التصيد الاحتيالي والوقاية منه (بلال، 2022، صفحة 41)

4- تحديات الذكاء الاصطناعي في الأمن السيبراني:

يمثل الذكاء الاصطناعي العديد من التحديات عندما يتعلق الأمر بالأمن السيبراني، يمكن أن يكون معقداً وقد يتطلب من المؤسسات الاستثمار في الموارد والتدريب والموظفين، هناك أيضاً مشكلات تتعلق بخصوصية البيانات تنشأ عن استخدام التحليلات المستندة إلى الذكاء الاصطناعي لاكتشاف التهديدات الأمنية، بالإضافة إلى مخاوف بشأن كيفية تخزين البيانات التي تم جمعها واستخدامها. (الفقي، 2012، صفحة 39)

4-1 الموارد وتكاليف التدريب:

يتطلب دمج الذكاء الاصطناعي في الأمن السيبراني استثمارات كبيرة في الموارد والأدوات والموظفين، تحتاج الشركات إلى الحصول على الأجهزة والبرامج اللازمة لحلّول الذكاء الاصطناعي وتكوينها، ويحتاجون أيضاً إلى تدريب موظفيهم على التكنولوجيات الجديدة، التي تأتي مع تكاليف إضافية قد يصعب على بعض المنظمات تحملها، كما يتطلب تنفيذ أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي محترفين ذوي مهارات عالية يمكنهم تصميم الأنظمة وتطويرها وصيانتها، وتكافح العديد من المؤسسات للعثور على موظفين يتمتعون بالخبرة والتجربة اللازمة لبناء برامج الأمن السيبراني القائمة على الذكاء الاصطناعي وصيانتها (الخياط، 2022، صفحة 44).

4-2 جودة البيانات:

تعتمد أنظمة الذكاء الاصطناعي على كميات كبيرة من البيانات عالية الجودة لتحديد الأنماط وإجراء تنبؤات دقيقة، يمكن أن تؤدي البيانات ذات الجودة الرديئة إلى نتائج غير دقيقة وإيجابيات خاطئة وتواجه العديد من المؤسسات صعوبة في جمع وإدارة كميات كبيرة من البيانات اللازمة لبرامج الأمن السيبراني الفعالة القائمة عليه (الخياط، 2022، صفحة 45).

4-3 خصوصية البيانات:

يعني استخدام الذكاء الاصطناعي في حلول الأمن السيبراني جمع وتحليل كمية هائلة من البيانات، مما يثير مخاوف بشأن خصوصية البيانات، كما تحتاج الشركات إلى التأكد من امتثالها للقوانين ذات الصلة مثل اللائحة العامة لحماية البيانات عندما يتعلق الأمر بتخزين بيانات العملاء وحمايتها، ويحتاجون أيضا إلى التأكد من عدم استخدام البيانات التي تم جمعها لأي أغراض غير مصرح بها أو مشاركتها مع أطراف ثالثة دون إذن (عبد الرحيم، 2021، صفحة 56).

4-4 تحليل دقيق:

لا تكون حلول الذكاء الاصطناعي فعالة إلا إذا تمكنت من تحديد التهديدات المحتملة بدقة والاستجابة بشكل مناسب، هذا يعني أنه يجب تدريبهم باستمرار على مجموعات البيانات الكبيرة من أجل التحسن في التعرف على أنماط النشاط الضار، والتي يمكن أن تستغرق وقتا طويلا، بالإضافة إلى ذلك تحتاج الشركات إلى التأكد من أن أنظمة الذكاء الاصطناعي الخاصة بها يتم اختبارها بانتظام للتأكد من دقتها من أجل التخفيف من أي إيجابيات خاطئة أو سلبيات خاطئة يمكن أن تنتج عن تحليل غير دقيق. (الباهي، 2022، صفحة 50)

4-5 الأخلاق والتحيزات:

هناك خطر من أن الأنظمة القائمة على الذكاء الاصطناعي يمكن أن تديم أو حتى تضخيم التحيزات والتمييز القائمة، يجب على المؤسسات اتخاذ خطوات لضمان أن أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي عادلة وشفافة وأخلاقية. (الباهي، 2022، صفحة 51)

5- دور الذكاء الاصطناعي في الهجمات الإلكترونية:

إذا كان هناك شيء واحد يجب مجرمو الإنترنت القيام به، فهو التغلب على أنظمة الأمان، ربما يكون العيب الأكبر في الذكاء الاصطناعي هو أنه ليس دائما المدافعون عن الإنترنت هم الذين يستخدمون الذكاء الاصطناعي لتطوير استراتيجيات جديدة كما أن المهاجمون يفعلون ذلك أيضا.

كان ChatGPT، وهو أحدث روبوت محادثة الذكاء الاصطناعي تم إطلاقه مؤخرا، في الأخبار بسبب مستواه المتقدم في فهم اللغة، ولكن أيضا للعديد من الأسباب الخاطئة، يمكن لروبوت الدردشة الذكاء الاصطناعي بالفعل إنشاء رسائل بريد إلكتروني مقنعة للغاية للتصيد الاحتيالي وعمليات احتيال الهندسة الاجتماعية، علاوة على ذلك يمكن لقدرات الترميز الخاصة به إنشاء تعليمات برمجية للبرامج الضارة أثناء التنقل، حيث أن أكثر من 53٪ في تقرير حديث للمشاركين قلقون من أن ChatGPT قد يساعد المتسللين في إنشاء رسائل بريد إلكتروني تصيد أكثر مصداقية وإقناعا، ويقول

49٪ إنه سيتمكن المتسللين الأقل كفاءة من تحسين مهاراتهم التقنية ونشر معلومات مزيفة. (الغامدي، 2024، صفحة 52)، في الحقيقة لقد اخذنا ChatGPT على سبيل المثال لا الحصر لأنه قد ظهرت ولا زالت تظهر العديد من مواقع الذكاء الاصطناعي المتخصصة والدقيقة إلى حد بعيد.

بينما يساعد الذكاء الاصطناعي في تقليل عبء العمل على المحللين البشريين، وتنفيذ العمليات الأمنية، فإنه يمكن المتسللين أيضا من أتمتة حملاتهم الضارة وتعزيزها.

5-1 دور الذكاء الاصطناعي في الحلول الأمنية:

يمكن أن يكون الذكاء الاصطناعي قويا بشكل لا يصدق عندما يتعلق الأمر باكتشاف التهديدات السيبرانية واتخاذ تدابير أمنية للحفاظ على الأصول الرقمية آمنة، ولكن لا تزال هناك بعض أفضل الممارسات التي يجب أن نضعها في اعتبارنا عند الاستفادة من الذكاء الاصطناعي للحلول الأمنية.

يتطور عالم الذكاء الاصطناعي باستمرار، لذلك من المهم البقاء على اطلاع دائم بأحدث التطورات والاتجاهات في الصناعة، سيساعدنا هذا على فهم أفضل لكيفية نشر الذكاء الاصطناعي لاحتياجاتنا الأمنية المحددة (خاصة بالنسبة لمسؤولي المؤسسات العمومية أو الخاصة)، مواكبة الأخبار وقراءة منشورات الصناعة وحضور المؤتمرات والندوات عبر الإنترنت المتعلقة الذكاء الاصطناعي والأمن السيبراني (كابلان، الرياض، صفحة 63).

5-2 مراقبة إدخال البيانات بانتظام:

لكي تعمل خوارزمية الذكاء الاصطناعي بشكل صحيح، فإنها تحتاج إلى تدفق مستمر من البيانات الموثوقة من أجل اكتشاف التهديدات أو الحالات الشاذة التي يمكن أن تكون مؤشرا على هجوم محتمل، ويجب التأكد من أننا نراقب بانتظام إدخال البيانات في الخوارزميات الخاصة بنا، حيث يمكن أن تؤدي التناقضات إلى استنتاجات خاطئة أو اتخاذ قرارات غير صحيحة. (بروك، 2018، صفحة 78).

5-3 التصميم مع وضع قابلية التوسع في الاعتبار:

عند تصميم حل أمان الذكاء الاصطناعي، يجب التأكد من أنه قابل للتطوير بحيث يمكننا تعديله بسهولة حسب الحاجة إذا نمت المؤسسة أو تغيرت بأي شكل من الأشكال، سيضمن ذلك أن حل الأمان الخاص به يمكن أن يتوسع أو يخفض بسهولة اعتمادا على الموقف، مع التأكد من أن أصوله الرقمية آمنة ومأمونة دائما. (بروك، 2018، صفحة 79).

6- التطبيقات الحالية للذكاء الاصطناعي في العمليات:

على الرغم من كونه مثيرا للجدل في بعض الدوائر، فلا شك في أن الذكاء الاصطناعي أصبح بسرعة الحركة التكنولوجية التالية في العمليات التجارية الحديثة، يحتوي الذكاء الاصطناعي على عدد كبير ومتنوع من الاستخدامات التي يمكن تنفيذها في كل جانب من جوانب العمليات التجارية اليومية. (بروك، 2018، صفحة 81).

6-1 زيادة الوظيفة وليس الاستبدال:

أثار الاستخدام المتزايد الذكاء الاصطناعي في مكان العمل مناقشات حول ما إذا كانت التقنيات الرقمية موجودة لتحل محل العمالة البشرية إلى الأبد، تسارعت هذه المناقشة فقط مع توفر الذكاء الاصطناعي التوليدي على نطاق واسع، مما يمنح أصحاب العمل القدرة على استخدام الذكاء الاصطناعي لإنشاء صور ونصوص ومقاطع فيديو قد تبدو أصلية أو من صنع الإنسان.

ومع ذلك على الرغم من خطو الذكاء الاصطناعي خطوات لا تصدق، لا يزال لديه العديد من القيود التي تجعل من المستحيل حالياً الاعتماد عليه بشكل كامل بدلاً من الجهود البشرية، على سبيل المثال يفتقر الذكاء الاصطناعي إلى فهم المشاعر البشرية أو السياق الثقافي، وغير قادر على توجيه أفعاله بالتعاطف، وهو جانب مهم جداً من صنع القرار البشري.

علاوة على ذلك عندما يتعلق الأمر الذكاء الاصطناعي التوليدي، على الرغم من أن إنتاجه مثير للإعجاب للغاية، إلا أن هناك أخطاء ملحوظة في المرحلة الحالية من التطور، على سبيل المثال غالباً ما يحتوي نص الذكاء الاصطناعي التوليدي على معلومات خاطئة يتم تقديمها بثقة على أنها حقيقة، هذه الظاهرة التي تسمى هلوسة الذكاء الاصطناعي، وهي معروفة جيداً وتعني أن البشر بحاجة إلى التحقق بعناية من صحة النص الذي تم إنشاؤه بواسطة الذكاء الاصطناعي، بالإضافة إلى ذلك تحتوي الصور التي تم إنشاؤها بواسطة الذكاء الاصطناعي أحياناً على أخطاء غريبة، مثل صراعها الشهير في إنشاء عقارب واقعية وطباعة نص على صورها، إذا احتاجت الشركة إلى تمثيل نفسها للعالم بشعار جديد أو مقالة دقيقة من الناحية الواقعية، فإن الاعتماد على الذكاء الاصطناعي وحده لا معنى له. (Wardini, 2024)

بالإضافة إلى ذلك في أفضل حالاته يتمتع الذكاء الاصطناعي بالقدرة على جعل مهام العمل اليومية أكثر قابلية للإدارة، بدلاً من استبدال البشر تماماً يتفوق الذكاء الاصطناعي والبشر في أنواع مختلفة من الذكاء، وتأتي أفضل النتائج من الاحتفاظ بكليهما في مكان العمل، كما يمكن للذكاء الاصطناعي التعامل مع المهام المتكررة دون الشعور بالملل أو التعب أو عدم التحفيز، كما يمكن له أيضاً إجراء مهام التحليل بشكل أسرع بكثير مما يمكن للإنسان القيام به، وباستخدام الذكاء الاصطناعي التوليدي، يمكنه إنشاء تقارير وحتى الإجابة على أسئلة البشر بلغة المحادثة، ومع ذلك يحتاج البشر إلى العمل مع الذكاء الاصطناعي لتحديد كيفية التصرف بناءً على المعلومات الواردة. (Globenewswire, 2021)

إذن يمكن أن يجعل الذكاء الاصطناعي أماكن العمل أكثر كفاءة من خلال تعويض النقص المؤقت في العمالة وإكمال المهام التي تستغرق وقتاً طويلاً من خلال أتمتة العمليات، يمكن أن يسمح تنفيذ المهام الجسدية والعقلية المتكررة، مثل التلاعب بالمخزون المادي وتفسير البيانات للموظفين بالتركيز على المهام الأكثر أهمية لأدوارهم المحددة. (Wardini, 2024)

6-2 ذكاء الأعمال:

يُعد ذكاء الأعمال (BI) مفتاحاً لقدرة أي مؤسسة مهنية على تتبع بياناتها وتحليلها بدقة، وتحسين سير العمل، وإنشاء أهداف قصيرة وطويلة الأجل لعملياتها، بهذه الطريقة يكمل الذكاء الاصطناعي وذكاء الأعمال بعضهما البعض،

يمكن استخدام الذكاء الاصطناعي لجمع وتنظيم كميات كبيرة من البيانات بسهولة، كما يمكن للمحللين والمديرين بعد ذلك استخدام هذه البيانات لاتخاذ قرارات ملموسة للعمليات والمشاريع قصيرة الأجل أو طويلة الأجل والتخطيط المالي والمزيد من ذلك. (الرحمان، 2021، صفحة 33).

6-3 إجراءات التوظيف والتوصيف:

كما تُدرك العديد من المؤسسات والشركات الكبرى خاصة لدى الدول المتطورة بالفعل، أصبح الذكاء الاصطناعي أداة شائعة بشكل متزايد في الفحص المسبق واختيار المرشحين للوظائف الشاغرة، يمكن لأنظمة تتبع المتقدمين (ATS) استخدام الذكاء الاصطناعي لمراجعة الحجم الهائل للطلبات بشكل أسرع بكثير مما يمكن للإنسان، واختيار تلك التي تتطابق بشكل وثيق مع المعايير التي يبحث عنها صاحب العمل.

بالإضافة إلى توظيف المرشحين أنفسهم، تقدم بعض خدمات توظيف الذكاء الاصطناعي أيضا جدولة تلقائية وإعادة توجيه المرشحين الأقوياء إلى مناصب أخرى مناسبة في الشركة.

تجدر الإشارة إلى أن أصحاب العمل بحاجة إلى توخي الحذر في كيفية استخدامهم الذكاء الاصطناعي لعملية التوظيف، على وجه الخصوص يمكن أن يعكس الذكاء الاصطناعي أي تحيزات موجودة في عملية التوظيف وتضخمها، والمسؤول على هذا الاختصاص في الشركة أو المؤسسة يحتاج إلى فهم كيفية عمل الخوارزميات الكامنة وراء أنظمة تتبع المتقدمين لتجنب التمييز في التوظيف وفقدان المواهب. (الغامدي، 2024، صفحة 101)

7- تدابير الأمن السيبراني:

في حين أن هذه المداخلة بمثابة تحذير بشأن تهديدات الجرائم الإلكترونية التي يتعرض لها الذكاء الاصطناعي، يمكن أن يكون الذكاء الاصطناعي أيضا تأثيرات مفيدة للأمن السيبراني، أحد أكثر استخدامات الذكاء الاصطناعي تعقيدا هو إدارة تهديدات الأمن السيبراني، حيث يمكن تعليم الذكاء الاصطناعي اكتشاف البرامج الضارة والفيروسات، على سبيل المثال بمرور الوقت يمكن أن يصبح الذكاء الاصطناعي أسرع من البشر في اكتشاف التهديدات الإلكترونية لأنظمتك من خلال الكشف الآلي عن التهديدات، في المتوسط تم العثور على تطبيقات الذكاء الاصطناعي لتقليل متوسط تكلفة سيناريو خرق بيانات المؤسسة بمقدار كبير من المال. (الغامدي، 2024، صفحة 110)

نعتقد أن إحدى الطرق التي يمكن أن يعزز بها الذكاء الاصطناعي الأمن السيبراني هي من خلال قدرات التعلم الآلي، والذي يكون بشكل أساسي من خلال التعرف على الأنماط والتنبؤ بها، يمكن ل الذكاء الاصطناعي التعرف على سلوك مجرمي الإنترنت وتوقع الهجمات الإلكترونية أو منعها أو الاستجابة لها بشكل أفضل.

7-1 الذكاء الاصطناعي والجرائم الإلكترونية:

الذكاء الاصطناعي هو أداة متعددة الأوجه يمكن استخدامها لكل من جمع البيانات وتنظيمها، فضلا عن حماية هذه البيانات من القوى الخارجية، نظرا للاعتماد الواسع النطاق لنظام الذكاء الاصطناعي في العمليات التجارية في السنوات

الأخيرة، طور الذكاء الاصطناعي والحماية من الجرائم الإلكترونية علاقة مترابطة في نماذج الأمن السيبراني المعاصرة. (الباهي، 2022، صفحة 84)

يمكن أن يزيد الذكاء الاصطناعي بشكل كبير من كفاءة أي نظام أمان بيانات من خلال اكتشاف التهديدات المحتملة قبل أن تؤدي ثمارها وسحق الهجمات الإلكترونية القادمة بسرعة بسرعات تتجاوز البشر، ومع ذلك من خلال الاستمرار في التركيز على فوائد تكامل الذكاء الاصطناعي في أنظمة التشغيل المختلفة، فإن العديد من أصحاب الأعمال غير مدركين للتهديدات التي قد تشكلها أنظمة الذكاء الاصطناعي الخارجية أيضا على أعمالهم، بالإضافة إلى نقاط الضعف في أنظمة الذكاء الاصطناعي الخاصة بهم.

أدت الهجمات الإلكترونية التي حظيت بتغطية إعلامية كبيرة في ولاية لويزيانا بالولايات المتحدة الأمريكية وفي جميع أنحاء العالم إلى تجديد المخاوف بشأن زيادة دمج تقنيات الذكاء الاصطناعي في الحياة اليومية خاصة في العمليات التجارية، علاوة على ذلك الآن بعد أن تم إكمال عمليات التصيد الآلي والبرامج الضارة وبرامج الفدية بواسطة الذكاء الاصطناعي، أصبحت الهجمات بمساعدة الذكاء الاصطناعي أكثر شيوعا، يؤدي تقدم أنظمة الذكاء الاصطناعي إلى تطور تعقيد الهجمات الإلكترونية ذات المستوى الأدنى. (الباهي، 2022، صفحة 86).

7-2 الذكاء الاصطناعي وحماية العمل:

كما هو الحال مع أي تقنية تتعامل مع البيانات الحساسة، هناك مخاطر لتنفيذ الذكاء الاصطناعي دون فهم أفضل طريقة للحفاظ على أمنه وفائدته، لحسن الحظ مع بدء المزيد من الشركات في دمج تقنية الذكاء الاصطناعي، هناك تدابير أمنية إلكترونية أقوى ومتاحة على نطاق واسع يمكن لفريقك استخدامها لحماية البيانات الحساسة وأنظمة الذكاء الاصطناعي من الهجوم السيبراني.

نظرا لأن الذكاء الاصطناعي نفسه يوفر أيضا مصدرا متزايدا وموثوقا به لتكتيكات الأمن السيبراني، فإن معرفة كيفية تنفيذ هذه التقنية في الأمن السيبراني الخاص بالمؤسسة سيكون مفتاحا لحمايتها. (الخياط، 2022، صفحة 69).

7-3 تطوير استراتيجيات المرونة السيبرانية:

تصف المرونة السيبرانية قدرة نظام البيانات على مواصلة عملياته أثناء أو بعد الهجوم السيبراني، كما أنه يأخذ في الاعتبار قدرة النظام على استعادة البيانات المسروقة أو العمليات الميكانيكية بعد حدوث تلف في البيانات أو النظام. تعد المرونة السيبرانية جانبا حيويا للأمن السيبراني، لأنها تشارك بشكل مباشر في صيانة حلول الاسترداد في حالة هجوم النظام، كما تُعد النسخ الاحتياطية للبيانات المستندة إلى الذكاء الاصطناعي وبروتوكولات استرداد النظام جزءا لا يتجزأ من تطوير المرونة الإلكترونية للمؤسسة. (الخياط، 2022، صفحة 77).

إذن يمكن أن يزود الذكاء الاصطناعي أقسام تكنولوجيا المعلومات بالإجراءات المحتملة التي يجب اتخاذها في استعادة البيانات، وإعادة تنظيم البيانات حتى يتم استرداد النظام الرئيسي بالكامل، وحتى تحسين عملية النسخ الاحتياطي لجعلها أكثر كفاءة.

7-4 تنفيذ حلول الأمن الهجومي والدفاعي:

يُعد الذكاء الاصطناعي جزءاً أساسياً من الأمن السيبراني الحديث، خاصة عندما يتعلق الأمر بتحديد التهديدات بسرعة، وأفضل طريقة لحماية العمل هي استخدام كل من الأمن السيبراني الاستباقي والتفاعلي، والاستفادة من الذكاء الاصطناعي للمساعدة في حماية العمل من التهديدات، على سبيل المثال يتم الآن استخدام تقنيات الذكاء الاصطناعي لتحسين قدرة أنظمة الأمن السيبراني على الانخراط في صيد التهديدات ومراقبتها، كلاهما من الإجراءات الأمنية الاستباقية الرئيسية التي يمكن أن تمنع الهجمات الإلكترونية قبل حدوثها. (السلام، 2023، صفحة 85).

عندما يتعلق الأمر باستخدام الذكاء الاصطناعي لاكتشاف التهديدات، فإن اثنين من أهم الأساليب اليوم هما نماذج معالجة اللغة الطبيعية (NLP) والتعلم الآلي (ML)، باستخدام البرمجة اللغوية العصبية والتعلم الآلي، يمكن للذكاء الاصطناعي مراجعة كميات كبيرة من البيانات بسرعة، والتعرف على الأنماط والتنبؤ بشكل استباقي بالتهديدات السيبرانية أو تحديدها بشكل تفاعلي. (Marr, 2019)

يمكن تدريب معالجة اللغة الطبيعية، التي تسمح ل الذكاء الاصطناعي بمعالجة اللغة البشرية وفهمها، على تحديد هجمات التصيد الاحتيالي في رسائل البريد الإلكتروني، على سبيل المثال من خلال تدريب نماذج البرمجة اللغوية العصبية على كمية كبيرة من البيانات، بما في ذلك رسائل البريد الإلكتروني المخادعة بالإضافة إلى رسائل البريد الإلكتروني الحميدة، يمكنها تعلم كيفية مراجعة معلومات المرسل بشكل فعال، وسطور الموضوع، والنص الأساسي، والروابط الصادرة، والمرفقات للنوايا الضارة، تُفهم هذه النماذج نوع اللغة المرتبطة بالتصيد الاحتيالي، بما في ذلك الكلمات التي بها أخطاء إملائية والمعلومات المتناقضة والشعور بالإلحاح. (Mukherjee, 2024)

من ناحية أخرى، يستخدم التعلم الآلي الخوارزميات لمعالجة البيانات، سواء التعلم منها أو اتخاذ القرارات بناء عليها يتم استخدام هذه النماذج بشكل متزايد لاكتشاف الحالات الشاذة لأغراض الأمن السيبراني. يمكنهم التعرف على الأنماط الخارجة عن القاعدة والتي قد تشكل خطراً أمنياً من خلال تقديم هذه النماذج ببيانات حول نشاط الشبكة الموثوقة، مثل سلوك المستخدم وأنماط حركة المرور وأداء النظام، يمكنها معرفة ما هو طبيعي وما هو شاذ (غير عادي) ومحاولات تسجيل الدخول غير العادية، والزيادات غير المتوقعة في حركة المرور، والتغيرات غير الطبيعية في الأنظمة، على سبيل المثال يمكن أن تمثل تهديداً إلكترونياً. (Marr, 2019)

7-5 توظيف خبراء الذكاء الاصطناعي والجرائم الإلكترونية:

بالإضافة إلى توظيف موظفي تكنولوجيا المعلومات القياسيين، يجب على أي مؤسسة تتطلع إلى دمج الذكاء الاصطناعي في أنظمتها أن تفكر أيضاً في توظيف خبراء داخليين أو خارجيين في أمن الذكاء الاصطناعي وصيانتها، يمكن هؤلاء المهنيين ذوي المهارات العالية تنفيذ بروتوكولات الأمان المنتظمة في هذه الأنظمة، بالإضافة إلى ضمان فعالية خوارزميات نظام الذكاء الاصطناعي. (بروك، 2018، صفحة 104).

8- قيود وتحديات الذكاء الاصطناعي على الأمن السيبراني:

في المشهد المعزز للذكاء الاصطناعي اليوم ليس هناك شك في أنه يوفر إمكانيات كبيرة لتحسين الأمن السيبراني، في الواقع فإن المؤسسات التي لا تستفيد من الذكاء الاصطناعي لأنها السيبراني معرضة لخطر التخلف عن الركب والوقوع ضحية لنقاط الضعف من الجرائم الإلكترونية التي تعمل بطاقة الذكاء الاصطناعي، ولكن هناك قيود وتحديات في الاعتماد على الذكاء الاصطناعي للأمن السيبراني يجب وضعها في الاعتبار، يجب على المؤسسات الحرص على عدم وضع كل ثقتها في الأنظمة الآلية - لا تزال الرقابة البشرية مكونا حاسما في الأمن السيبراني. (العبيدي، 2021، صفحة 82).

8-1 الاعتماد المفرط على الأنظمة الآلية:

إن الاعتماد المفرط على الأنظمة الآلية ينطوي على مخاطر كبيرة على المؤسسات، من خلال افتراض أن الذكاء الاصطناعي قادر تماما ودقيقا تماما، ويدير أمن المؤسسة السيبراني بشكل فعال من البداية إلى النهاية، فقد يصبح المسؤول راضيا عن نفسه ويفوت النقاط العمياء في الذكاء الاصطناعي، نتيجة لذلك قد تكون هناك ثغرات أمنية في أنظمة مؤسسته لا يستطيع الذكاء الاصطناعي تحديدها ومعالجتها لاحقا، قد يكون تدريب الذكاء الاصطناعي قصيرا عندما يتعلق الأمر باستراتيجيات الجرائم الإلكترونية الجديدة أو الهجمات الإلكترونية الأكثر تعقيدا. (العلي، 2019، صفحة 69)

نتيجة لذلك يجب على المؤسسات الاستثمار في نهج ذو شقين يتضمن كلا من الذكاء الاصطناعي ومتخصصي الأمن السيبراني البشري، يمكن للعاملين البشريين دعم جهودهم الخاصة باستخدام أدوات الذكاء الاصطناعي، بالإضافة إلى تحديث تدريب الذكاء الاصطناعي بانتظام حتى يتمكن من التحسين المستمر وأخذ المعلومات الناشئة في الاعتبار. (العلي، 2019، صفحة 70)

8-2 تجاوز تقنيات الذكاء الاصطناعي أو استغلالها:

غالبا ما تتعلم تقنيات الذكاء الاصطناعي، وخاصة تلك التي تتضمن التعلم الآلي، من البيانات يمثل ذلك خطرا، حيث يمكن لمجرمي الإنترنت محاولة استخدام هذه البيانات أو خوارزميات الذكاء الاصطناعي ضدها، على سبيل المثال قد يتمكن المهاجمون الإلكترونيون الذين يدرسون تقنيات مكافحة الفيروسات التي تعمل بالطاقة الذكاء الاصطناعي من تعديل برامجهم الضارة بطريقة لم تعد الذكاء الاصطناعي معروفة، مما يسمح لها بتجاوز النظام. (بلال، 2022، صفحة 120).

قدر الإمكان، يجب مراعاة هذه المخاطر من البداية باستخدام الذكاء الاصطناعي المستخدم للأمن السيبراني، يمكن أن يتخذ هذا شكل تدريب الخصومة كجزء من مرحلة تدريب الذكاء الاصطناعي، من خلال تغذية البيانات التي تم التلاعب بها إلى الذكاء الاصطناعي أثناء تدريبه، يمكنه تعلم كيفية التعرف على مثل هذه الهجمات والاستجابة لها بشكل أفضل، عنصر مهم آخر هو التدخل البشري، يجب أن يكون خبراء الأمن السيبراني في المؤسسة مسؤولين عن مراقبة أنظمة الأمن السيبراني الذكاء الاصطناعي على أساس منتظم، بالإضافة إلى تحديثها بمرور الوقت للتعرف على أحدث التكتيكات في الجرائم الإلكترونية. (بلال، 2022، صفحة 122).

8-3 الرقابة البشرية لا تزال حاسمة:

بغض النظر عن مدى تقدم الذكاء الاصطناعي، فإنه سيتطلب دائما إشرافا بشريا، التهديدات السيبرانية معقدة، والخبراء البشريون مجهزون بشكل أفضل لرؤية وفهم بعض الفروق الدقيقة في الجرائم الإلكترونية في سياق أكبر، تحدث حالات شاذة إحصائية، مما قد يتسبب في قيام الذكاء الاصطناعي بتحديد نشاط حميد عن طريق الخطأ على أنه تهديد، يمكن لخبير الأمن السيبراني البشري أن ينظر بسرعة إلى السياق المحيط بهذا النشاط ويدرك أنه لا يشكل تهديدا. (الباهي، 2022، صفحة 99)

عندما تختار مؤسسة ما تنفيذ تقنيات الذكاء الاصطناعي في أمنها السيبراني، فمن الأهمية بمكان تعليم موظفي الأمن السيبراني حول هذه التقنيات، كما يجب أن يكون فريق الأمن السيبراني قادرا على الاستفادة بشكل فعال من هذه التقنيات مع مراعاة قيودها منذ البداية، ويجب وضع عمليات على الفور لمتخصصي الأمن السيبراني لمراقبة هذه التقنيات بشكل مستمر، وتدقيقها لتقييم فعاليتها على أساس دوري، والتدخل لتقديم التقييم والعمل بشأن الحالات المعقدة.

9- أهداف الأمن السيبراني:

بدون تحديد أهداف الأمن السيبراني لمؤسستك وتحديد أولوياتها بشكل صحيح، سيكون من الصعب استخدام الذكاء الاصطناعي لصالحه الكامل ويتضمن ذلك ما يلي:

- فهم أكبر التهديدات: يمكن أن تساعد معرفة التهديدات المحددة التي تشكل أكبر خطر على المؤسسة، الآن وفي المستقبل في العثور على حلول الذكاء الاصطناعي المناسبة للتخفيف من تلك التهديدات الحرجة. (Globenewswire, 2021)

- إعطاء الأولوية للأمن السيبراني الاستباقي مقابل الأمن السيبراني التفاعلي: في حين أن أفضل نهج للأمن السيبراني يتضمن مزيجا من التدابير الاستباقية والتفاعلية، فمن المهم معرفة أيهما له الأولوية في المؤسسة، ستكون التهديدات التي تواجهها، بالإضافة إلى تحمل المسؤول للمخاطر الفريدة بالنسبة له وتؤثر على كيفية تقسيم انتباهه وموارده بين الأمن السيبراني الاستباقي والتفاعلي. يمكن أن يكون الذكاء الاصطناعي أداة فعالة لكليهما، حيث يدعم تتبع التهديدات واكتشاف الحالات الشاذة والتكتيكات الاستباقية الأخرى، بالإضافة إلى الاستجابة للحوادث والأنشطة التفاعلية الأخرى (الباهي، 2022، صفحة 105).

- الالتزام بالأخلاقيات: تأتي تقنيات الذكاء الاصطناعي مع اعتبارات أخلاقية مهمة من أجل استخدامه أخلاقيا منذ البداية، تحتاج المنظمة إلى فهم الأسئلة الأخلاقية التي تنشأ مع استخدام الذكاء الاصطناعي، مثل التحيزات ومخاوف الخصوصية، قبل تنفيذ تقنياته، يجب أن تكون هناك عمليات لضمان نشرها بشكل أخلاقي ومع إشراف بشري مناسب (الباهي، 2022، صفحة 106) من خلال معالجة هذه القيود والتحديات، يمكن للمؤسسات الاستفادة بنجاح من الذكاء الاصطناعي لأغراض الأمن السيبراني، مما يضمن دفاعا قويا ضد تهديدات اليوم والأيام القادمة.

خاتمة:

مع استمرار تطور الذكاء الاصطناعي وأصبح أكثر اندماجا في الأمن السيبراني، يجب على المؤسسات توخي اليقظة في الاستفادة من إمكانياته للحماية من الهجمات الإلكترونية، كما يمكن أن يكون الذكاء الاصطناعي أداة قوية للكشف عن الأنماط الضارة والاستجابة بسرعة للتهديدات، ولكن له أيضا مخاطر وتحديات فريدة يجب معالجتها. الجزائر كغيرها من الدول التي تحاول أن تضع الخطوات الأولى لاستعمال الذكاء الاصطناعي بدء من خلق مؤسسات بحثية إلى تشجيع الابتكار والاختراع في هذا المجال، وترمي سياسة الدولة الجزائرية إلى المضي قدما نحو تعميم الرقمنة في جميع مجالات الحياة، وهذا يترتب عليه مزيد من الفطنة واليقظة الرقمية.

إذن إذا كنا نفكر في تنفيذ حلول قائمة على الذكاء الاصطناعي لمواجهة تحديات الأمن السيبراني التي قد نواجهها، فيجب التأكد من القيام بذلك بشكل صحيح، حيث مع تحديد الأهداف والغايات بوضوح، ومع مراعاة قيود هذه الحلول على الرغم من أن الذكاء الاصطناعي يمكنه تسريع القدرات الأمنية وتحسينها، إلا أن هذا غير ممكن بدون الخبرة المناسبة، لهذا السبب من المهم جداً العمل مع شريك موثوق به يمكنه المساعدة في تحديد أفضل الطرق للاستفادة من الذكاء الاصطناعي والتنفيذ لتعزيز وضع الأمن السيبراني الخاص بالمؤسسة عامة وبالفرد خاصة.

قائمة المراجع العربية:

- أسامة عبد الرحمان. (2021). *الذكاء الاصطناعي ومخاطره*. الرياض: دار الشروق.
- حسان الباهي. (2022). *الذكاء الاصطناعي وتحديات مجتمع المعرفة*. القاهرة: دار الهدى.
- ديري كابلان. (الرياض). *الذكاء الاصطناعي ما يحتاج الجميع لمعرفته*. 2020: شركة بوكمانيا للترجمة والنشر.
- صباح الخياط. (2022). *الذكاء الاصطناعي مفاهيمه تقنياته أساليب برمجته*. الأردن: دار حنين للنشر والتوزيع سلسلة كتب الكمبيوتر العربية.
- عبد الاله ابراهيم الفقي. (2012). *الذكاء الاصطناعي والنظم الخبيرة*. الأردن: دار الثقافة والنشر والتوزيع.
- عبد الله موسى، احمد حبيب بلال. (2022). *الذكاء الاصطناعي*. القاهرة: المجموعة العربية للتدريب والنشر.
- على زياد العلي. (2019). *الصراع والأمن الجيوسياسي*. الأردن: دار أمجد للنشر والتوزيع.
- عمر عباس خضير العبيدي. (2021). *مكافحة الجرائم السيبرانية: بلية لتعزيز الأمن الاقليمي*. لبنان: مركز الدراسات العربية للنشر والتوزيع.
- قاري ريم عبد الرحيم، الصافي ريم علوي، و علام نوف خالد. (2021). *مفاتيح الأمن لاسيبراني في التعليم*. القاهرة: الأفاق للنشر والتوزيع.
- محمد بن فوزي الغامدي. (2024). *الذكاء الاصطناعي في التعليم*. الرياض: مكتبة الملك فهد الوطنية.
- محمد حسن عبد السلام. (2023). *الذكاء الاصطناعي وتطبيقاته التعليمية*. الرياض: دار جرير.
- هنري بروك. (2018). *الذكاء الاصطناعي*. لبنان: دار المجاني سلسلة المغامرون.

قائمة المراجع الأجنبية:

- Globenewswire. (2021, 09 16). *Artificial Intelligence (AI) in Cybersecurity Market*. Retrieved from Globenewswire: Globenewswire, Artificial Intelligence (AI) in Cybersecurity Market, September 16, 2021, " <https://www.globenewswire.com/> , Date of access: 03-01-2025
- Marr, B. (2019, 05 29). *Artificial Intelligence In The Workplace: How AI Is Transforming Your Employee Experience*. Retrieved from forbes: <https://www.forbes.com>
- Mukherjee, A. (2024, 03 13). *The Role of AI in Protecting Digital Assets from Cybercrime*. Retrieved from threatintelligence: [https://www.threatintelligence.com/blog/ai#:~:text=Artificial%20intelligence%20\(AI\)%20can%20be,times%20rather%20than%20just%20periodically](https://www.threatintelligence.com/blog/ai#:~:text=Artificial%20intelligence%20(AI)%20can%20be,times%20rather%20than%20just%20periodically)
- Wardini, J. (2024, 01 03). *36 Eye-Opening AI Statistics You Should Know*. Retrieved from techjury: <https://techjury.net/blog/ai-statistics/>