

الذكاء الاصطناعي والأمن السيبراني: الوظائف والتحديات

*The impact of Artificial intelligence and cyber-Security: Opportunities and challenges*سارة بخوش^{*1}Sarrra BEKHOUCHE^{1*}¹ جامعة قسنطينة 3-صالح بوبنيدر، (الجزائر)، sarrra.bekhouch@univ-constantine3.dz

تاريخ النشر: 2025/06/05

تاريخ القبول: 2025/05/29

تاريخ الإرسال: 2024/11/05

Abstract:

This research paper aims to study the impact of artificial intelligence on cyber security, through a conceptual study that explains the uses of artificial intelligence applications in the field of cyber security, as the integration of artificial intelligence into various aspects of digital infrastructure has created opportunities and challenges.

The study reached many results, the most important of which is the positive effects of employing artificial intelligence in the field of cyber security, especially with regard to digital security.

Keywords: artificial intelligence; Cyber security; Cyber threa; Cyberspace.

ملخص:

تهدف هذه الورقة البحثية إلى دراسة تأثير الذكاء الاصطناعي على الأمن السيبراني، من خلال دراسة مفاهيمية توضح استخدامات تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني، حيث أدى دمج الذكاء الاصطناعي في مختلف جوانب البنية التحتية الرقمية إلى خلق فرص وتحديات.

وتوصلت الدراسة إلى العديد من النتائج أهمها التأثيرات الإيجابية التي يحدثها توظيف الذكاء الاصطناعي في مجال الأمن السيبراني خاصة ما يتعلق بالأمن الرقمي.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، التهديدات السيبرانية، الفضاء السيبراني.

* المؤلف المرسل.

1. مقدمة

أدى التطور الذي عرفه مجال تكنولوجيا المعلومات والاتصالات إلى التأثير على العديد من المجالات بما في ذلك مجال الأمن السيبراني وأمن المعلومات والاختراقات في مجال الحماية، وهذا ما يؤدي إلى زيادة تهديدات الأمن السيبراني التي تتميز بالتعقيد والتطور والتغير السريع بفعل الابتكارات السريعة في مجال الذكاء الاصطناعي، الذي يعد من أبرز التطورات التكنولوجية التي ظهرت في المجتمع المعاصر، ولهذه التقنية المتطورة العديد من الاستخدامات والتطبيقات المختلفة في مجالات العلوم الحديثة لكل القطاعات ما يفرض على الحكومات والمؤسسات اتباع استراتيجية دمج أنظمة الذكاء الاصطناعي مع القدرات البشرية من أجل تحقيق استفادة أكبر في مجال الأمن السيبراني.

ويُعد كلاً من الذكاء الاصطناعي والأمن السيبراني من صور التطور التكنولوجي الهائل، وقد اكتسبا هذان المجالان شهرة في التكنولوجيا الحديثة، نظراً لأدوارهما الحاسمة في تشكيل العالم الرقمي، وعليه تهدف هذه الدراسة إلى تسليط الضوء على مفهوم وتقنيات ومجالات الذكاء الاصطناعي، والتعرف على مفهوم الأمن السيبراني والاشكاليات المرتبطة بتطبيقات الذكاء الاصطناعي على الأمن السيبراني من خلال تحليل المفهوم، ودراسة الفرص التي يتيحها الذكاء الاصطناعي ومعرفة التحديات التي تواجه توظيفه، ومن هذا المنطلق تتمحور إشكالية الدراسة في الآتي: ماهي أهم تأثيرات تطبيق الذكاء الاصطناعي في مجال الأمن السيبراني؟

ويندرج ضمن هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية:

1. ما هو الذكاء الاصطناعي، وماهي أهم تقنياته؟
2. ما هو الأمن السيبراني، وفيما تتمثل أهم أبعاده؟
3. ماهي أهم وظائف الذكاء الاصطناعي في مجال الأمن السيبراني.

تتعلق الدراسة من فرضية مفادها أنه كلما ازداد التطور في البيئة الرقمية كلما ازداد توظيف الذكاء الاصطناعي في مجال الأمن السيبراني.

وتعتمد الدراسة على المنهج الوصفي التحليلي الذي يهدف إلى دراسة العلاقة بين الذكاء الاصطناعي والأمن السيبراني من خلال تحليل أدبيات الموضوع، واستقراء المفاهيم، مما يسمح بفهم معمق للفرص التي يوفرها الذكاء الاصطناعي في تعزيز الأمن السيبراني، وكذلك التحديات والمخاطر التي يفرضها.

وللإجابة على الإشكالية السابقة تم تقسيم الدراسة إلى المحاور التالية:

1. الذكاء الاصطناعي والأمن السيبراني: مقارنة مفاهيمية
2. استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني.
3. تحديات الأمن السيبراني في عصر الذكاء الاصطناعي.

2. الذكاء الاصطناعي والأمن السيبراني: مقارنة مفاهيمية

يعتبر كل من مفهوم الذكاء الاصطناعي والأمن السيبراني من المفاهيم الحديثة في مجال الدراسات السياسية، وقبل التطرق إلى الترابطات والتأثيرات الموجودة بين المفهومين، سنحاول في هذا المحور التطرق إلى مفهوم الذكاء الاصطناعي والأمن السيبراني، من خلال تفكيك هذه المفاهيم وتعريف مفرداتها.

1.2 مفهوم الذكاء الاصطناعي:

يعتبر مفهوم الذكاء الاصطناعي من أبرز المفاهيم التي عرفت نقاشات واسعة، وقد اختلف الباحثون في إيجاد تعريف دقيق لمفهوم الذكاء الاصطناعي، نظرا لاختلاف ميولاتهم الفكرية ومجالاتهم البحثية، ويعد الأميركي جون مكارثي عالم في الحاسوب (1927-2011) أول من طرح مصطلح الذكاء الاصطناعي عام 1956، تزامنا مع

انعقاد مؤتمر علمي في كلية دارتموث الأميركية حول إمكانية تصميم آلة ذكية قادرة على تقليد ومحاكاة عمل البشر.¹

وقد عرف الذكاء الاصطناعي بأنه: "فرع واسع النطاق من علوم الكمبيوتر يهدف إلى أداء المهام المرتبطة تقليدياً بالذكاء البشري".²

وعرف كذلك بأنه: "مجموعة التقنيات القادرة على التعلم واستخدام المنطق والتكيف وأداء المهام بطرق مستوحاة من العقل البشري".³

كما عرف بأنه: "ذلك التيار العلمي والتقني الذي يضم الطرق والنظريات والتقنيات التي تهدف إلى إنشاء آلات قادرة على محاكاة الذكاء، حيث يستخدم المنطق الرياضي والخوارزميات".⁴

ويشكل الذكاء الاصطناعي إحدى الركائز الأساسية للثورة الصناعية الرابعة، بفضل قدرته على تمكين الآلات من تقليد السلوك البشري وتحليل كميات هائلة من البيانات بكفاءة عالية، وتدرج ضمن الذكاء الاصطناعي عدة تقنيات متقدمة أهمها⁵:

1.1.2 التعلم الآلي (ML): هو مجموعة فرعية من الذكاء الاصطناعي الذي يمكن

الأنظمة من التعلم والتحسين من التجربة دون أن تتم برمجتها بشكل صريح، وفي مجال الأمن السيبراني، يتم استخدام التعلم الآلي لتحديد الأنماط والحالات الشاذة أي التمييز بين حركة مرور الشبكة العادية والأنشطة الضارة المحتملة.

2.1.2 معالجة اللغات الطبيعية (NLP): تتضمن البرمجة اللغوية العصبية قدرة

أجهزة الكمبيوتر على فهم اللغة البشرية وتفسيرها وتوليدها.

3.1.2 الشبكات العصبية: نماذج متقدمة للتعلم الآلي مستوحاة من بنية الدماغ

البشري ووظيفته، تركز على تحديد الأنماط المعقدة في البيانات بسبب بنيتها العميقة ذات

الطبقات وقدرتها على تعلم العلاقات غير الخطية، على عكس نماذج التعلم الآلي التقليدية التي غالباً ما تقتصر على التفسيرات الخطية أو البسيطة القائمة على قواعد القرار.

4.1.2 كشف الشذوذ: أسلوب يستخدم لتحديد الأنماط غير العادية التي لا تتوافق

مع السلوك المتوقع، وهو مفيد بشكل خاص في تحديد التهديدات السيبرانية الجديدة التي لم يسبق لها مثيل.

5.1.2 التحليلات التنبؤية: تستخدم التحليلات التنبؤية التقنيات الإحصائية ونماذج

التعلم الآلي لتحديد احتمالية النتائج المستقبلية بناءً على البيانات التاريخية.

فالذكاء الاصطناعي هو أكثر من مجرد تقنية؛ إنه ظاهرة معرفية واجتماعية مركبة فهمه يتطلب رؤية متعددة التخصصات تجمع بين الحوسبة، الفلسفة، والسياسة، وتعتبر تقنياته أدوات حيوية تساهم في تحسين الكفاءة والقدرة على اتخاذ القرارات في مجموعة متنوعة من المجالات.

2.2 تعريف الأمن السيبراني:

يُعدّ الأمن السيبراني من المفاهيم الحديثة التي فرضت نفسها نتيجة التحول العميق نحو الرقمنة في مختلف المجالات الحيوية، ومع تنامي استخدام الفضاء الرقمي، أصبحت البيانات والأنظمة المعلوماتية تواجه تهديدات متصاعدة ومتنوعة، ما استوجب تطوير آليات لحمايتها من التهديدات الإلكترونية، وهو ما مهدّ لظهور مفهوم "الأمن السيبراني" كإطار شامل لحماية النظم والمعلومات.

يعد مصطلح "سيبراني" من أكثر المصطلحات استخداماً في معجم الأمن الدولي، وكلمة cyber مشتقة من الكلمة اليونانية kybernetes حيث تشير مجازاً للمتحكم governor، في حين نسبها البعض إلى عالم الرياضيات الأمريكي (1894-1964) Norbert Wiener وذلك للتعبير عن التحكم الآلي.⁶

أما اصطلاحاً هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يطلق السيبراني على كل ما له علاقة بالشبكات الالكترونية الحاسوبية، وشبكة الانترنت، والفضاء السيبراني يعني الفضاء الالكتروني.

ويشير مصطلح الأمن السيبراني حسب موسوعة "انفستوبيديا" الى: "مجموعة التدابير المتخذة للحفاظ على خصوصية المعلومات الالكترونية وأمانها من التلف أو السرقة، يتم استخدامه أيضاً للتأكد من عدم إساءة استخدام الأجهزة والبيانات".⁷

في حين عرفه قاموس Oxford وقاموس word-reference على أنه: "حالة الأمان من الجريمة الالكترونية والإجراءات المتخذة لتنفيذ ذلك".⁸

وعرفه Amoroso Edward بأنه: "وسيلة من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة".⁹

أما وزارة الدفاع الأمريكية اعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات من مختلف الجرائم كالتجسس، والهجمات.¹⁰

ونظراً لتعدد زوايا المقاربة، تختلف التعريفات الأكاديمية للأمن السيبراني تبعاً للسياق الذي يُدرس فيه، بين من ينظر إليه كأداة أمن قومي، ومن يراه امتداداً لحماية حقوق الإنسان الرقمية، أو كأحد مكونات حوكمة الإنترنت، عموماً يمكن القول بأن الأمن السيبراني يهتم بأمن الفضاء الافتراضي والرقمي والتكنولوجي والاتصالي والتواصلي وكل ما يتعلق بالبيئة السيبرانية.

3.2 أبعاد الأمن السيبراني:

لا يقتصر الأمن السيبراني على كونه مسألة تقنية تتعلق بحماية الأنظمة والشبكات، بل هو مفهوم متعدد الأبعاد يتقاطع مع قضايا أمنية، واقتصادية، واجتماعية، وقانونية،

ومع اتساع نطاق التهديدات الرقمية، برزت الحاجة إلى مقارنة شاملة تتناول الأمن السيبراني من مختلف زواياه، لضمان حماية فعّالة للفضاء الرقمي، وتتنوع أبعاد الأمن السيبراني على عدة محاور رئيسية:

1.3.2 البعد العسكري: يهتم بالجوانب العسكرية والدفاعية، وذلك من خلال حماية

البنية التحتية السيبرانية للقوات المسلحة، ويتطلب تحقيق هذا البعد المهم للأمن السيبراني وجود قدرات واستراتيجيات للكشف المبكر عن التهديدات السيبرانية المحتملة، والاستعداد للرد عليها، عبر تطوير تقنيات وأدوات.¹¹

2.3.2 البعد السياسي: يقوم هذا البعد على أساس حماية نظام الدولة وكيانها من

الناحية السياسية، فيمكن لتسريب وثائق حساسة أن يتسبب في مشاكل كبيرة سواء داخليا أو خارجيا، وهذا ما يؤثر على أمن واستقرار الدول وزعزعة العلاقات الدولية.¹²

3.3.2 البعد الاقتصادي: نظرا لأهمية المعرفة في الاقتصاد والترابط الوثيق بينهما

يبرز جليا أهمية الأمن السيبراني في حماية المصالح الاقتصادية للدول، إذ أصبح الاقتصاد الرقمي واستخدام تكنولوجيات المعلومات والاتصال في مختلف المعاملات المالية والاقتصادية عاملا مهما لتحقيق التنمية الاقتصادية لذا لا بد من توفير الأمان لهذه المعلومات التي تعتبر ثروة وطنية.¹³

4.3.2 البعد الاجتماعي: يضمن البعد الاجتماعي في مجال الأمن السيبراني مسألة

التوازن بين الخصوصية والأمن، فيجب حماية الخصوصية للأفراد من جهة، ومن جهة أخرى، يجب الحفاظ على الأمن السيبراني ومكافحة التهديدات الإلكترونية، ويلعب الوعي والتثقيف السيبراني دوراً حاسماً في تعزيز الأمن السيبراني وتحسين الأفراد والمجتمع ضد الشبكات الإجرامية الناشطة في الفضاء السيبراني وضمان سلامة البيانات والمعلومات الحساسة على الإنترنت.¹⁴

5.3.2 البعد القانوني: يشير إلى القوانين والتشريعات التي تنظم وتحمي

المعلومات والبيانات الرقمية من التهديدات والاختراقات الإلكترونية، كما تحمي حقوق الأفراد والشركات فيما يتعلق بالخصوصية والملكية الفكرية والمعلومات الحساسة.

تُظهر هذه الأبعاد أن الأمن السيبراني لم يعد مجرد مسألة فنية، بل أصبح ركيزة للأمن القومي، مما يستدعي تطوير سياسات شاملة وتعاون دولي لمواجهة التهديدات السيبرانية المتصاعدة، فالأمن السيبراني يمثل منظومة متكاملة من السياسات، والإجراءات، والتقنيات التي تهدف إلى حماية المعلومات والشبكات والأنظمة من التهديدات الرقمية.

3. استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني

أصبح الذكاء الاصطناعي جزءاً أساسياً من استراتيجيات الأمن السيبراني الحديثة، حيث يُسهم بشكل كبير في تعزيز القدرة على حماية الأنظمة الرقمية من التهديدات والهجمات المتزايدة من خلال الاستفادة من تقنياته، فقد برز (AI) باعتباره عامل تغيير في مجال الأمن السيبراني، خاصة في خدمات تطوير البرمجيات التي تمكن من تمشيط كميات كبيرة من البيانات والكشف عن الحالات الشاذة،¹⁵ والتعريف بالمعدات المعيبة والأخطاء البشرية فيها، أو الانتهاكات الأمنية والتهديدات السيبرانية، وفيما يلي بعض الاستخدامات الرئيسية للذكاء الاصطناعي في هذا المجال:

1.3 تعزيز كشف التهديدات:

يعمل الذكاء الاصطناعي على تعزيز الاستخبارات المتعلقة بالتهديدات من خلال تحليل مجموعات البيانات الكبيرة في الوقت الفعلي وتقديم رؤى تنبؤية، حيث يمكنه التعرف على نمط سلوك الهجمات السيبرانية وكشف التهديدات المحتملة قبل حدوثها من خلال استفادته من تقنيات التعلم الآلي والتعلم العميق للتعرف على الأنماط واكتشاف

السلوك غير المعتاد، وتحسين خوارزميات الكشف الخاصة به للحوادث المستقبلية، تعتبر هذه القدرة ضرورية لتحديد التهديدات بشكل استباقي مما يوفر دفاعاً قوياً ضد التهديدات السيبرانية المتطورة،¹⁶ مما يعزز مرونة الأمن السيبراني بشكل عام.

2.3 تحليل البيانات:

تكمن أهمية الذكاء الاصطناعي في مجال الأمن السيبراني في قدرته على التعامل مع حجم كبير من المعلومات وتدقيقها بكفاءة وفعالية والكشف عن التهديدات والمخاطر المحتملة والعمل على التخفيف من حدتها، الأمر الذي يساعد على الحفاظ على أمن الشبكة وسلامتها، وتمكين استراتيجيات استجابة أكثر فعالية.¹⁷

3.3 تعزيز الاستجابة:

تعد السرعة أمراً بالغ الأهمية أثناء الهجوم السيبراني، ويعزز الذكاء الاصطناعي الاستجابة للحوادث من خلال أتمتة اكتشاف التهديدات وتحليلها والتخفيف من آثارها، وبالتالي يتم تقليل الوقت من الاكتشاف إلى الإجراء، ويتم تقليل تأثيرات الاختراق المحتملة إلى الحد الأدنى، حيث توفر الأنظمة المدعومة بالذكاء الاصطناعي سياقاً محسناً لتحديد أولويات التنبيهات الأمنية وتمكين الاستجابة السريعة للحوادث، وتحديد الأسباب الجذرية للتخفيف من نقاط الضعف ومنع المشكلات المستقبلية.

فالذكاء الاصطناعي يمكن من تطوير استجابة أسرع وأكثر فعالية للاختراقات والهجمات وذلك عن طريق الكشف واستدلال الهجمات واتخاذ التدابير الصحيحة، وتقلل هذه الاستجابة السريعة عبء العمل على فرق الأمان من خلال أتمتة بعض أنشطة البحث عن التهديدات واتخاذ إجراءات فورية وتلقائية،¹⁸ ومنع الأضرار التي لا يمكن إصلاحها الناجمة عن الهجمات السيبرانية، وضمان تنفيذ التدابير الأمنية بسرعة وفعالية من خلال أتمتة الكشف عن التهديدات والاستجابة.

4.3 تحسين الأمان الشبكي:

يساهم الذكاء الاصطناعي في تعزيز الأمان الشبكي من خلال استخدام العديد من الأدوات كاختبار CAPTCHA، مساحات بصمات الأصابع، والتعرف على الوجه، الأمر الذي يساهم في تحسين عملية تصنيف البيانات وتشفيرها، إذ تسمح هذه الأدوات بالتحقق من هويات المستخدم ومنع الهجمات السيبرانية المتوقعة وبالتالي ضمان عدم المساس ببياناته¹⁹، فالذكاء الاصطناعي يعمل في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات، وأتمتة آليات الاستجابة، مما يعزز من البنية التحتية للأمن.

عموماً يمثل الذكاء الاصطناعي أداة قوية وضرورية في مجال الأمن السيبراني، حيث يساهم في اكتشاف التهديدات بشكل أسرع وأكثر دقة، ويعمل على تحسين فعالية الدفاعات الإلكترونية من خلال الأتمتة والتعلم المستمر.

4. تحديات الأمن السيبراني في عصر الذكاء الاصطناعي

على الرغم من أن الذكاء الاصطناعي يوفر فرصاً مهمة لتعزيز فعالية الأمن السيبراني، إلا أن التوسع في استخدامه يفرز تحديات متزايدة ومعقدة، إذ بات يشكل أداة ذات استخدام مزدوج، تُوظف في الحماية والهجوم على حد سواء، الأمر الذي يصعب من عملية التنبؤ بالتهديدات ويزيد من سرعة تطورها وتتمثل أبرز هذه التحديات فيما يلي:

1.4 التحيز في صنع القرار:

تثار أسئلة حول المساءلة والمسؤولية في توظيف الذكاء الاصطناعي في مجال الأمن السيبراني، على اعتبار أن أنظمة الذكاء الاصطناعي أصبحت أكثر استقلالية وقدرة على اتخاذ القرارات المستقلة، فمن المسؤول عندما يتخذ نظام الأمن السيبراني المدفوع بالذكاء الاصطناعي قراراً تنتج عنه عواقب غير مقصودة، وبالتالي إن تحقيق التوازن

الصحيح بين الاستقلالية والإشراف البشري أمر بالغ الأهمية لتجنب النتائج السلبية غير المقصودة،²⁰ حيث يمكن أن يؤدي ضعف التفاعل البشري الآلي إلى عدم فعالية التواصل بين أنظمة الذكاء الاصطناعي والقادة البشريين، مما قد يؤدي إلى سوء الفهم واتخاذ قرارات غير فعالة وتطبيق قرارات آلية دون تدخل بشري، وتثير هذه المخاوف تساؤلات حول فقدان السيطرة البشرية على الآلات وإمكانية السلوكيات الضارة في المجتمعات.²¹

2.4 أضرار عرضية :

قد يؤدي الاعتماد على تقنيات الذكاء الاصطناعي إلى أخطاء فنية أو أضرار عرضية، وهذا مثير للقلق بشكل خاص عندما يتعلق الأمر باستخدام البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني، فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.

3.4 المضلات الأخلاقية :

يُعدُّ البُعد الأخلاقي من أبرز التحديات التي تفرض نفسها عند توظيف الذكاء الاصطناعي في مجالات أمن المعلومات، فمع تزايد الاعتماد على الخوارزميات الذكية في اتخاذ قرارات أمنية حساسة، تبرز تساؤلات جوهرية تتعلق بالمساءلة، الخصوصية، التحيز، فيمكن أن يؤدي تحيز الذكاء الاصطناعي وانعدام الشفافية إلى استهداف غير عادل كما يمكن أن يؤدي هذا إلى تعريف خاطئ على أنه تهديد داخلي، مما يتسبب في ضرر لا يمكن إصلاحه²²، على سبيل المثال، قد تُصنَّف أنشطة بعض المستخدمين بشكل خاطئ على أنها تهديدات بناءً على أنماط غير موضوعية موجودة في البيانات.

ويعد ضمان خلو خوارزميات الذكاء الاصطناعي من التحيزات والتزامها بالمبادئ الأخلاقية أمراً بالغ الأهمية للحفاظ على الثقة والنزاهة في ممارسات الأمن السيبراني،

فمثلاً تحتاج تقنيات الذكاء الاصطناعي إلى بيانات ضخمة لتعمل بكفاءة، الأمر الذي قد يفرض نوعاً من المراقبة الشاملة للمستخدمين، وهنا يظهر التوتر بين الحاجة إلى حماية النظام، وضرورة احترام خصوصية الأفراد ويجب أن تلتزم المؤسسات بضوابط قانونية وأخلاقية تحد من جمع البيانات دون مبرر مشروع، لذا يجب على متخصصي الأمن السيبراني ومطوري البرمجيات مواكبة اللوائح والمعايير المتعلقة بأخلاقيات الذكاء الاصطناعي، لأن تحقيق التوازن بين الفوائد المحتملة للذكاء الاصطناعي والاستخدام الأخلاقي يعد أمراً ضرورياً في بناء إطار للأمن السيبراني يحمي البيانات وقيم الأفراد والمنظمات.²³

4.4 إساءة استخدام الذكاء الاصطناعي:

أحد المخاوف المهمة أيضاً هو استخدام الذكاء الاصطناعي في تطوير البرمجيات الخبيثة والهجمات السيبرانية المتطورة،²⁴ لاستعانة منفذي الهجمات الإلكترونية بأنظمة ذكاء اصطناعي في تهديد البنية التحتية للمؤسسات²⁵، وفي هذا تشكل تقنية Deepfake تهديداً كبيراً للأفراد والمنظمات وحتى الأمن القومي، حيث يمكن من خلالها إنشاء محتوى مزيف بعمق لخداع الأفراد أو التلاعب بالرأي العام، وأصبح اكتشاف هذا التزييف العميق أمراً صعباً نظراً لتطور قدرة خوارزميات الذكاء الاصطناعي على إنشاء محتوى واقعي للغاية.

إضافة إلى أن البيانات التي تتناولها خوارزميات الذكاء الاصطناعي قد تكون متحيزة ضد أفراد أو مجموعات وفقاً لعوامل ديموغرافية أو ثقافية، ما يؤدي إلى تحليلات خاطئة من قبل هذه الخوارزميات.²⁶

5.4 تكلفة التنفيذ:

إن دمج تكنولوجيا الذكاء الاصطناعي في الأمن السيبراني يمكن أن يكون مكلفاً ويتطلب الكثير من الموارد أجهزة متخصصة، وبنية تحتية داعمة، وقدرة معالجة كبيرة

وقوة لتشغيل العمليات الحسابية المعقدة²⁷، إضافة الى مهارات متقدمة في مجالات الأمن والتحليلات والبرمجة والذكاء الاصطناعي، مما قد يشكل تحدياً في توفير الموارد البشرية المناسبة.²⁸

في ظل التحديات المتزايدة التي فرضها التوسع في استخدام الذكاء الاصطناعي، أصبح من الضروري تبني استراتيجيات متكاملة لتعزيز الأمن السيبراني وتمثل بعض هذه الاستراتيجيات في:²⁹

- **التعاون وتبادل المعلومات:** يجب على متخصصي الأمن السيبراني والباحثين في مجال الذكاء الاصطناعي وأصحاب المصلحة في الصناعة التعاون وتبادل المعرفة للبقاء في صدارة مواجهة التهديدات المتطورة.
- **الاستثمار في البحث والتطوير:** من المهم الاستثمار في البحث وتطوير حلول الذكاء الاصطناعي الآمنة، ويشمل ذلك تعزيز الخطط الحكومية مثل CERT-In، وتعزيز الشراكات بين القطاعين العام والخاص، وتعزيز التعاون بين أصحاب المصلحة.
- **تثقيف الجمهور:** يعد تثقيف الجمهور حول النظافة السيبرانية وعمليات الاحتيال عبر الإنترنت وممارسات خصوصية البيانات أمراً ضرورياً لبناء مجتمع رقمي مرن.

5. خاتمة

يتّضح من خلال التحليل أن الذكاء الاصطناعي يمثل مجاًلاً تقنياً متقدماً يقوم على تمكين الأنظمة والآلات من أداء مهام تحاكي الذكاء البشري، وقد أصبح هذا المجال يشكل تحولاً نوعياً في مقاربة قضايا الأمن السيبراني، إذ لم يعد يُنظر إليه فقط كأداة لتعزيز الحماية، بل بات عاملاً مركزياً في إعادة تشكيل طبيعة التهديدات والردود عليها، فقد مكّن

الذكاء الاصطناعي من تطوير آليات دفاعية أكثر فاعلية ضد الهجمات السيبرانية، قادرة على التعلّم والتكيف عبر تقنيات متطورة تُعدّ محوراً رئيسياً في استراتيجيات الأمن السيبراني المعاصرة.

وينظر إلى الذكاء الاصطناعي كذلك كأداة فعالة في تحقيق الأمن الرقمي، بفضل قدراته في التعلّم الآلي، وتحليل البيانات، ومعالجة اللغات الطبيعية، واكتشاف الشذوذ، والتحليل التنبؤي. إلا أن هذا التوظيف يثير تحديات متعددة، من أبرزها احتمالات سوء الاستخدام، وانتهاك الخصوصية، وضعف الشفافية، إلى جانب الإشكالات المرتبطة بالمساءلة والالتزام الأخلاقي. ومن ثم، فإن التوفيق بين الاستفادة من إمكاناته التقنية والحد من مخاطره يتطلب اعتماد مقاربة شاملة ومتكاملة تراعي الأبعاد التكنولوجية، والسياسية، والأخلاقية في آنٍ واحد.

عموماً، يُعدّ الأمن السيبراني في ظل تطور الذكاء الاصطناعي تحدياً معقداً ومتعدد الأبعاد، غير أن تبني نهج استباقي في مواجهة المخاطر، إلى جانب الاستفادة الفعالة من الإمكانيات التي تتيحها هذه التقنيات، يُمكن من بناء بيئة رقمية أكثر أماناً واستقراراً، وذلك من خلال ما يلي:

- توفير بنية تقنية متطورة تسهم في تنفيذ مشاريع الذكاء الاصطناعي.
- إعداد كوادر متخصصة في مجال الأمن السيبراني ورفع مستوى الوعي والتدريب المهني لتعزيز استراتيجيات الحماية من الاختراقات.
- تعزيز الشفافية في خوارزميات الذكاء الاصطناعي لضمان إمكانية تتبع القرارات الأمنية والتحقق منها.
- وضع أطر تشريعية وتنظيمية تحكم استخدام الذكاء الاصطناعي في الأمن السيبراني وتضمن التزامه بالمعايير الأخلاقية.

– تعزيز التعاون بين الدول لإيجاد استراتيجيات جديدة حول التهديدات السيبرانية المستجدة المدعومة بالذكاء الاصطناعي.

– ضرورة بلورة ميثاق دولي ملزم ينظم الاستخدام السلمي والأمن للذكاء الاصطناعي، يشمل أبعاد الأمن السيبراني وحقوق الإنسان الرقمية.

6 . الهوامش والمراجع

¹ موسوعة الجزيرة، الذكاء الاصطناعي...حينما تفكر الآلة، 16-05-2024، نقلا عن الموقع:

<https://shorturl.at/1alip>, 2024-10-12 .

² Coursera Staff , What Is Artificial Intelligence? Definition, Uses, and Types, 3 avr. 2024, in <https://shorturl.at/f3b0A>, 12-10-2024

³ دحماني محمد، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، المجلد 07، العدد:02، 2023، ص 600.

⁴ عجمي نعا، واقع الرقمنة والذكاء الاصطناعي في الضمان الاجتماعي: تجربة الجزائر نموذجا، مجلة البحوث في الحماية الاجتماعية، المجلد: 03، العدد:02، 2023، ص 05.

⁵ Brotherskeep, AI & Cybersecurity (Part 1): Introduction, 4 January 2024, in <https://shorturl.at/MoMzy>, 25-10-2024.

⁶ مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية بجامعة المنصورة، العدد: 111، يوليو 2020، ص 9.

⁷ فاطمة علي إبراهيم وآخرون، الأمن السيبراني والنظافة الرقمية، المجلة المصرية لعلوم المعلومات، المجلد: 09، العدد:02، أكتوبر 2022، ص 395.

⁸ المرجع نفسه، ص 397.

⁹ قلاع الضروس سمير، الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الالكترونية بالجزائر، مجلة الرواق للدراسات الاجتماعية والإنسانية، المجلد: 08، العدد: 02، 2022، ص 252.

¹⁰ مني عبد الله السمحان، مرجع سابق، ص 10.

¹¹ سعد بوه الشيخ محفوظ الحبيب، أبعاد الأمن السيبراني، 5-3-2024، نقلا عن الموقع:

<https://shorturl.at/IHp3h>, 2024-10-27 .

¹² مني عبد الله السمحان، مرجع سابق، ص 15.

¹³ سعد بوه الشيخ محفوظ الحبيب، مرجع سابق.

¹⁴ المرجع نفسه.

¹⁵ Boitumelo Mosia , Adapting Cybersecurity Changes in the AI-Driven World 06-12-2023, in <https://shorturl.at/51Omd>, 19-10-2024

¹⁶ Balbix, AI in Cybersecurity: Transforming Threat Detection and Prevention, in <https://shorturl.at/jXDwD>, 14-10-2024 .

¹⁷ (ب،ك) حالات استخدام الذكاء الاصطناعي في الأمن السيبراني، نقلا عن الموقع: 19-06-2024، نقلا عن الموقع: <https://shorturl.at/iOUpP>، 14-10-2024.

¹⁸ Paloaltonetwork, What are the Risks and Benefits of Artificial Intelligence (AI) in Cybersecurity?, In <https://shorturl.at/ZP6qx> , 14-10-2024.

¹⁹ (ب،ك)، مرجع سابق.

²⁰ Paloaltonetwork ,Op.Cit.

²¹ Future for Advanced Research and Studies, The role of artificial intelligence in modern warfare, 22 May 2024, in <https://shorturl.at/4SpJf> (18-10-2024)

²² EC-Council University, Cybersecurity Threats in the Age of Artificial Intelligence, in <https://shorturl.at/oHcnZ> (18-10-2024).

²³ Boitumelo Mosia , Op.cit.

²⁴ EC-Council University, Op.cit.

²⁵ المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، أمن قومي: دور الذكاء الاصطناعي في الأمن السيبراني، 03 فبراير 2024، نقلا عن الموقع: <https://shorturl.at/X6q4f> (2024-10-22).

²⁶ المرجع نفسه.

²⁷ EC-Council University, Op.cit.

²⁸ أمال عيسى المهدي، العصر الرقمي... الذكاء الاصطناعي والأمن السيبراني: الفرض والتحديات، 29-08-2024، نقلا عن الموقع: <https://shorturl.at/FpxlO> 18-10-2024.

²⁹ EC-Council University, Op.cit .