الذكاء الاصطناعي كألية لتعزيز الامن السيبراني

Artificial intelligence as a mechanism to enhance cyber Security

محمد دحماني*، جامعة عمار ثليجي – الأغواط –
mo.dahmani@lagh-univ.dz

تاريخ إرسال المقال:2023/08/28 تاريخ قبول المقال: 2023/10/13 تاريخ نشر المقال: 2023/11/30

الملخص:

تعد ظاهرة التهديدات السيبرانية، والتي تتميز بشكل مختلف عن طبيعة التهديدات التقليدية، من الظواهر الخطيرة التي تهدد أمن الأفراد والدول، ومع الثورة التكنولوجية ظهر ما يسمى بالذكاء الاصطناعي كتقنية جديدة والتي غزت جميع المجالات، بما في ذلك مجال الأمن السيبراني، لقد جاءت هذه الدراسة ونتائجها لتوضيح دور تكنولوجيا الذكاء الاصطناعي في تحسين الأمن السيبراني، وذلك بالاعتماد على المنهج الوصفي، وقد توصلت الى ضرورة الأسرع في اعتماد التشريعات المتعلقة بالاستخدامات المختلفة لتكنولوجيا الذكاء الاصطناعي، من اجل الحماية والحفاظ على الخصوصية ، وإنشاء هيئات متخصصة في هذا الشأن.

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

Abstract:

The phenomenon of cyber threats, which is distinguished differently from the nature of traditional threats, is considered one of the dangerous phenomena that threaten the security of individuals and countries, and with the technological revolution, the so-called artificial intelligence appeared as a new technology that invaded all fields, including the field of cyber security. This study and its results came to clarify the role of artificial intelligence technology in improving cybersecurity, by relying on the descriptive approach, and i have concluded the need to quickly adopt legislation related to the various uses of artificial intelligence technology, in order to protect and preserve privacy, and to establish specialized bodies in this regard.

Key words: Artificial intelligence, cyber security, security, cyberspace

المقدمة:

تمثل تقنية الذكاء الاصطناعي اهم إنجاز للثورة الصناعية الرابعة، لما لها من استخدامات واسعة النطاق في مجالات الحياة المختلفة، فقد تم استخدامها في مجال الاقتصاد والصناعة والخدمات والمجال العسكري والمجال السياسي وفي تحسين الأمن السيبراني وتعزيزه، هذا الأخير ليس بمعزل عن الشؤون العامة

* المؤلف المرسل

للفرد والمجتمع، حيث تم استخدام هذه التقنية (الذكاء الاصطناعي) في عملية تحسين الأمن السيبراني في الدولة.

من خلال ما سبق يمكننا طرح إشكالية مفادها:

أولا: الإشكالية

ما مدى نجاعة استخدام تقنية الذكاء الاصطناعي في تحسين الأمن السيبراني؟

وهذا السؤال المحوري يتطلب منا طرح أسئلة فرعية جاءت كما يلي:

1. ما مفهوم تقنية الذكاء الاصطناعي، وما مجالات استخدامه؟
2. فيما يتمثل الامن السيبراني وما هي ابعاده؟
3. ما تطبيقات الذكاء الاصطناعي في الامن السيبراني؟

ثانيا: اهداف الدراسة

1. التعرف على الذكاء الاصطناعي واستخداماته
2. التعرف على الامن السيبراني وابعاده
3. معرفة تأثير الذكاء الاصطناعي على الامن السيبراني

ثالثا: أهمية الدراسة

تتبع أهمية هذا البحث من انه:

1. يشرح مفهوم الذكاء الاصطناعي واستخداماته
2. يتناول البحث الذكاء الاصطناعي، وعلاقته بالأمن السيبراني ولكن هناك حاجة لمزيد من البحث في هذا المجال، خاصة في ظل المنافسة الدولية في مجال الامن الر قمي وتزايد ظاهرة التهديدات السيبرانية.
3. المزيد من المعارف في مجال تكنولوجيا المعلومات.
4. من المؤمل أن تساعد هذه الدراسة ونتائجها المهتمين بالشأن المعلوماتي والأمني على تحديد المخاطر وفهمها.
5. تساعد في تصميم دراسات مستقبلية حول موضوع هذه الدراسة خصوصا ما تعلق بسياق الذكاء الاصطناعي في المجال الامني

رابعا: فرضية الدراسة

تنطلق فرضية الدراسة من رؤية مفادها أن الذكاء الاصطناعي يتداخل مع الامن السيبراني، حيث أن القاسم المشترك بينهم يكمن في أن جميع العمليات تقع في فضاء مشترك واحد وهو الفضاء السيبراني.

خامسا: منهج الدراسة

موضوع هذه الدراسة اقتضي منا إتباع المنهج الوصفي حيث تم دراسة تقنية الذكاء الاصطناعي واستخداماتها وكيف تمكنت بعض الدول من توظيف هذه التقنية في الشأن الأمني السيبراني

سادسا: خطة البحث

المبحث الاول: مفهوم الذكاء الاصطناعي والامن السيبراني

المطلب الأول مفهوم الذكاء الاصطناعي

المطلب الثاني: مفهوم الامن السيبراني

المبحث الثالث: تطبيقات الذكاء الاصطناعي في الامن السيبراني

المطلب الأول: الوظائف الرئيسية للذكاء الاصطناعي في الامن السيبراني

المطلب الثاني: تحديات الذكاء الاصطناعي في الامن السيبراني

الخاتمة: تضمنت جملة من النتائج المتوصل اليها وهذا بعد اختبار الفرضية المطروحة

1: مفهوم الذكاء الاصطناعي والامن السيبراني

الأمن السيبراني يشير إلى حماية الأنظمة الإلكترونية والشبكات من التهديدات السيبرانية مثل الاختراقات والاعتداءات الإلكترونية والبرمجيات الخبيثة، ويعتبر الأمن السيبراني أمرًا حيويًا في عصرنا الحالي حيث يتزايد استخدام التكنولوجيا والانترنت في حياتنا اليومية، ومن ناحية أخرى، الذكاء الاصطناعي (AI)هو مجال يهتم بتطوير الأنظمة والبرامج ، ويقوم بمحاكاة الذكاء البشري في تحليل البيانات واتخاذ القرارات، ويتم استخدام الذكاء الاصطناعي في مجموعة متنوعة من المجالات مثل التجارة الإلكترونية، والطب، والتعليم، وغيرها، من خلال هذا المبحث سنقف على مفهوم المصطلحين والاحاطة بهما ، حيث نتطرق في المطلب الأول الى مفهوم الذكاء الاصطناعي اما المطلب الثاني يكون مخصص لمفهوم الامن السيبراني.

1.1: مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي هو مجال يهتم بتطوير أنظمة الكمبيوتر القادرة على أداء المهام التي تتطلب تفكيرًا وتحليلًا بشريًا ذكيًا، وهو تطور هائل في مجال التكنولوجيا يسمح للأنظمة الذكية بالتعلم والتكيف والتفاعل مع البيئة المحيطة، من خلال هذا المطلب سنتطرق الى بعض تعريفات الذكاء الاصطناعي واهم المجالات التي يستخدم فيها

1.1.1: تعريف الذكاء الاصطناعي

تكشف مراجعة الأدبيات حول موضوع الذكاء الاصطناعي أن العديد من التعريفات لمفاهيم تكنولوجيا الذكاء الاصطناعي قد تم نشرها ليس فقط من قبل المنظمات والخبراء في هذا المجال، ولكن أيضًا من قبل الأشخاص المهتمين بمجال التكنولوجيا، وفيما يلي بعض تعريفات الذكاء الاصطناعي[1].

يصف سيمون الذكاء الاصطناعي بأنه مرتبط بعلم النفس والعلوم المعرفية وغيرها من العلوم التي تمكن أجهزة الكمبيوتر من أداء المهام بكفاءة، وتقليد القدرات البشرية، وجعل أجهزة الكمبيوتر تفكر بذكاء.

ويعرّف ريتش وكينج الذكاء الاصطناعي بأنه دراسة كيفية أداء أجهزة الكمبيوتر للمهام بشكل أفضل من البشر.

ويعرف مجلس صناعة المعلومات (ITI) الذكاء الاصطناعي بأنه "مجموعة من التقنيات القادرة على التعلم واستخدام المنطق والتكيف وأداء المهام بطرق مستوحاة من العقل البشري."

الذكاء الاصطناعي يشمل العلم والمعرفة التي يتم دمجها منطقيًا في أنظمة الكمبيوتر ويتم تجميعها وفقًا لخوارزميات محددة تعالج المشكلات التي تتطلب ذكاءً غير عادي [2].

ويشير الذكاء الاصطناعي إلى قدرة الآلات (مثل أجهزة الكمبيوتر) على اكتساب الذكاء والتفكير المنطقي (الصوت) على غرار قدرة الإنسان على التفكير أو تفسير كميات كبيرة من البيانات (مثل البيانات المكتوبة أو المنطوقة)[3]

هذه التعريفات ليست حصرية، هناك عدد لا يحصى من تعريفات الذكاء الاصطناعي، كل منها محدد من زوايا مختلفة اعتمادًا على مجال خبرة الفرد واهتماماته، وتجدر الإشارة أيضًا إلى أن العلماء لا يتفقون على تعريف واحد.

وعلى الرغم من اختلاف العديد من الباحثين حول إمكانات الذكاء الاصطناعي للوصول إلى مستوى العقل البشري بسبب الاختلافات الجوهرية، أصبح الذكاء الاصطناعي حقيقة واقعة وأصبح جزءًا من حياتنا العملية، ويتم استخدامه بشكل يومي

2.1.1: مجالات استخدام الذكاء الاصطناعي

للذكاء الاصطناعي العديد من الاستخدامات يمكن ان نلخصها فيما يلي:

1. تُستخدم تقنية الذكاء الاصطناعي في مجالات خدمية مختلفة مثل العسكرية والصناعية والتقنية والمالية والطبية والتعليمية، وتشمل التطبيقات المهمة لهذه التقنية السيارات ذاتية القيادة والطائرات بدون طيار، وتعمل الروبوتات بشكل مستقل وتشغل الآلات المستخدمة في مجموعة متنوعة من المهام، مثل العمل في المفاعلات النووية ومحطات الطاقة وإصلاح الكابلات ومدها تحت الأرض واكتشاف المناجم وغيرها من المهام التي تحل محل الاستخدام البشري.
2. تُستخدم عمليات المحاكاة الذكية الحاسوبية لدراسة كيف يتعرف الدماغ البشري على الوجوه والأصوات المألوفة، ويعالج الصور، ويستخرج البيانات المفيدة منها، وكيف تحسن الذاكرة، والأمر نفسه ينطبق على تطوير الألعاب الإلكترونية مثل الشطرنج وألعاب الفيديو.
3. يمكن أيضًا ممارسة المهارات الحركية والتحكم اللفظي وغير الخطي من خلال الأجهزة الذكية التي يمكنها أداء المهام العقلية مثل أبحاث التصميم الصناعي والتحكم في العمليات واتخاذ القرار.

4. تُستخدم لتعليم اللغة، والفهم التلقائي للغة المكتوبة والمنطوقة، وترجمة اللغة في الوقت الفعلي بإجابات مبرمجة مسبقًا، ويتم جمع العديد من عمليات البحث في Google على أجهزة كمبيوتر متصلة بالإنترنت.[4]

مما سبق يمكننا القول أن تقنية الذكاء الاصطناعي لها العديد من التطبيقات في مختلف المجالات، فنجد انها تستخدم في القطاعات العسكرية والمالية والخدمية والصناعية، كما يمكن استخدامها في مجال التعليم من خلال المنصات التعليمية والتطبيقات الرقمية المبرمجة، كما يقدم الذكاء الاصطناعي العديد من المزايا ،ففي مجال الطب ، يمكن أن يساعد الذكاء الاصطناعي الأطباء في تشخيص الأمراض وتوجيه العلاج بشكل أكثر دقة، و في مجال التصنيع ، يمكن للذكاء الاصطناعي تحسين عمليات الإنتاج وزيادة الكفاءة، حيث يمكن للروبوتات المجهزة بتقنيات الذكاء الاصطناعي أداء المهام الروتينية بدقة عالية وسرعة عالية ومع ذلك ، يواجه الذكاء الاصطناعي أيضًا بعض التحديات والقيود، في بعض المجالات التي تتطلب التفكير الإبداعي والحدس البشري.

2.1: مفهوم الأمن السيبراني

من خلال هذا المطلب سنقوم بالإحاطة بمفهوم الأمن السيبراني والمفاهيم المرتبطة به ، وهذا من أجل تقريب المفاهيم والمصطلحات ، وعليه سوف نتطرق في العنصر الأول إلى مفهوم الفضاء السيبراني باعتباره هو حيز العمليات السيبرانية ، ثم نتحدث عن التهديدات السيبرانية وهذا في العنصر الثاني، وفي الاخير يكون الحديث عن الأمن السيبراني واهم أبعاده.

1.2.1: الفضاء السيبراني

لقد دخل الفضاء السيبراني كمجال جديد للعلاقات الدولية يمكنه إنشاء قاعدة قوة جماعية للجهات الفاعلة الحكومية وغير الحكومية عبر الحدود، وإنه امتداد للنشاط البشري، جنبًا إلى جنب مع ما يفعله الناس في القطاعات والأماكن الدولية الأخرى، الأرض، البحر، الجو، الفضاء، إلخ.

مصطلح "الحكم" يأتي من عمل نوربرت وينر، الذي عرّف مصطلح "حوكمة" وسائل الإعلام.

تم الإبلاغ عن أن التفاعل بين الإنسان والآلة يؤدي إلى بناء بيئات اتصال بديلة تشكل النسيج الأساسي لمفاهيم الفضاء السيبراني.[5]

يُعرّف المعجم العسكري لوزارة الدفاع الأمريكية الفضاء السيبراني على النحو التالي: "المنطقة العالمية داخل بيئة المعلومات التي تتكون من شبكات مترابطة من البنية التحتية للبيانات وتكنولوجيا المعلومات مثل الإنترنت وشبكات الاتصالات والحوسبة والمعالجة والتحكم، وتخدم شبكات المعلومات حوسبة عالم الفضاء السيبراني ، والمعلومات الشبكة هي حجم رقمي المعلومات التي لا تعتمد كليًا على البيئة التي تم إنشاؤها فيها، ولكن مفرداتها تغطي مجموعة واسعة من المعالجات بالإضافة إلى سرعات نقل البيانات والوصول إلى الشبكة وما إلى ذلك، وبيئة الفضاء الإلكتروني تتعامل مع البيانات أثناء تدفقها.[6]

يمكن القول ان الفضاء السيبراني هو عالم افتراضي يتكون من أنظمة الكمبيوتر والشبكات والبرامج والبيانات والمعلومات. يشمل الفضاء السيبراني جميع الأنشطة والعمليات التي تتناول العالم الرقمي، بما في ذلك الاتصالات عبر الإنترنت، والتجارة الإلكترونية، والشبكات الاجتماعية، والخدمات المصرفية عبر الإنترنت، والحكومة الإلكترونية، وغيرها.

ومع تزايد استخدام التكنولوجيا والإنترنت في حياتنا اليومية، أصبح الفضاء الإلكتروني هدفًا للهجمات السيبرانية والتهديدات الأمنية ويتعرض الفضاء السيبراني للعديد من التحديات مثل القرصنة والبرامج الضارة والتصيد والتجسس السيبراني وغيرها من الهجمات السيبرانية.

2.2.1: التهديدات السيبرانية

التهديدات بالمعنى الاستراتيجي هي تضارب المصالح والأهداف الوطنية، ولا تتعلق بإيجاد حلول سلمية توفر الحد الأدنى من الأمن السياسي والاقتصادي والاجتماعي والعسكري للدول، ويتم تعريفها على أنها الوصول إلى مرحلة، الضغط الخارجي الغير المتوازن قد يجبر المتحاربين على اللجوء إلى استخدام القوة العسكرية، وتعريض الأمن القومي للخطر [7]

التهديد: وفقًا لباري بوزان، هو "عندما تكون أراضي الدولة مهددة بالضرر، أو العدوان، أو الاستخدام الأيديولوجي، أو قدرة دولة ما على قلب دولة أخرى"، ويمكن أن تأتي التهديدات للجهات الحكومية من خلال استخدام عناصر "الحيازة" من مصادر خارجية وداخلية. [8] "

السيبرانية: تأتي من كلمة cyber، والتي تعني أي شيء يتعلق بأجهزة الكمبيوتر وتكنولوجيا المعلومات والواقع الافتراضي، مشتق من الكلمة اليونانية Kybernetes، والتي تعني القاعدة أو الأمر، وعلم التحكم الآلي، وعلم التحكم الآلي، وعلم التحكم في الأنظمة والتحكم الآلي، سواء الآلات أو الكائنات الحية.[9]

التهديدات السيبرانية تعني استغلال أجهزة الكمبيوتر وتكنولوجيا المعلومات لتخريب البنية التحتية الاستخباراتية للعدو وتدميرها، وكذلك تعطيل شبكات الدفاع الجوي وفقًا لخطط مدروسة بعناية واستخدام البريد الإلكتروني ومكاتب المراقبة التابعة لرئيس الدولة، كما يعني حرق أنظمة المعلومات وغيرها من الاعمال

وبالتالي، فإن التهديد السيبراني أو الهجوم السيبراني يمثل تهديدًا للأمن الاجتماعي والأمن الاقتصادي والأمن القومي، وتم تحديد هذا الهدف لأن التهديدات السيبرانية ليس لها عواقب أخلاقية أو جسدية.[10]

يمكن تعريف التهديد عبر الإنترنت بأنه سلوك تهديدي، يمكن أن يعرض الضحايا للخوف بطرق مختلفة باستخدام الفضاء الإلكتروني مثل وسائط الاتصال وأجهزة الاتصال والإنترنت وتدفق المعلومات والبيانات، ويمكن أن يؤثر ذلك على الأفراد والجماعات وحتى البلدان.

يمكن القول ان التهديد السيبراني هو أي نشاط غير قانوني أو ضار يتم تنفيذه عبر الإنترنت أو شبكات الكمبيوتر وتتضمن هذه التهديدات مجموعة متنوعة من الأنشطة الضارة مثل الاقتحامات السيبرانية والبرامج الضارة والاحتيال السيبراني وسرقة الهوية والتجسس السيبراني والهجمات المنسقة على البنية التحتية

للشبكة، كما يمكن أن يكون للتهديدات السيبرانية تأثيرات خطيرة على الأفراد والشركات والحكومات، كما نجد انها تتطور باستمرار، حيث يستخدم المهاجمون تقنيات متقدمة ومتطورة للوصول إلى الأنظمة والشبكات. وبالتالي، تتطلب الحماية من التهديدات السيبرانية اتخاذ تدابير أمنية قوية مثل تحديث البرامج والأنظمة بانتظام، واستخدام كلمات مرور قوية، وتشفير البيانات، وتنفيذ أنظمة كشف التسلل، وتثقيف المستخدمين حول أفضل الممارسات الأمنية.

3.2.1: الأمن السيبراني

يُعرّف الأمن السيبراني بأنه: "أمن الشبكات وأنظمة المعلومات والبيانات والمعلومات والأجهزة المتصلة بالإنترنت؛ وبالتالي، يتعلق بالإجراءات الوقائية والمعايير التي يجب اتخاذها والالتزام بها من أجل مواجهة التهديدات ومنع الانتهاكات أو الوصول الى غير المصرح به. "على الأقل الحد من تأثيرها .

يعرف Richard A. Kemmerer الأمن السيبراني بأنه "إجراءات لتقليل مخاطر الهجمات على البرامج أو أجهزة الكمبيوتر أو عناصر التحكم، بما في ذلك الوسائل والأدوات المستخدمة."

الأمن السيبراني، بناءً على أهدافه، هو نشاط يضمن حماية الموارد البشرية والمالية المتعلقة بتكنولوجيا المعلومات والاتصالات وإمكانية تقليل الخسائر والأضرار التي تؤدي إلى تحقيق المخاطر والتهديدات، وربما يمكن استعادة التوسع في أسرع وقت ممكن، ويعتمد المدى الذي لا تتوقف عنده عجلات الإنتاج ولا يتحول الضرر إلى خسارة على ما إذا كانت الأنشطة أو الوظائف أو القدرات أو المعلومات الواردة في أنظمة المعلومات والاتصالات محمية من العناصر الضارة، أو الاستخدام أو إساءة الفهم أو إساءة الاستخدام[11]

1- أبعاد الأمن السيبراني:

يشمل الأمن السيبراني أنظمة الأمن العسكرية والاقتصادية والاجتماعية والسياسية والإنسانية التي تهدف إلى الحفاظ على الأمن من جميع التهديدات السيبرانية، كما يتم تضمين الأمن المتكامل الذي يعمل على الحفاظ على جوانب نظام الأمن السيبراني، ومن اهم ابعاد الامن السيبراني نجد:[12]

- **البعد العسكري:** ويهدف إلى الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يتيح تبادل وتدفق المعلومات والأوامر، وإنها فكرة لإنشاء ونشر شبكة للإنترنت والأهداف البعيدة، ولكنها أيضًا نقطة ضعف، خاصةً إذا كانت غير آمنة، ويمكن أن يؤدي تدمير قواعد البيانات العسكرية أو المساومة عليها إلى تعطيل الاتصالات بين وحدات القيادة والوحدات العسكرية، فضلاً عن إمكانية التحكم وفقدان السيطرة على بعض الأسلحة مثل الطائرات بدون طيار والصواريخ الموجهة والأقمار الصناعية
- **البعد الاقتصادي:** نظرًا لاستخدام أجهزة الكمبيوتر لتشغيل الصناعات وتنميتها ودفع الاقتصاد، ستصبح الإنترنت أساس التجارة والتمويل والمعاملات المالية، وكلها مرتبطة ببعضها البعض من خلال شبكات الكمبيوتر لتحقيق الأمن السيبراني خصوصا ما تعلق بالقطاع المالي

- **البعد الاجتماعي:** يوجد أكثر من 4 مليارات مستخدم للإنترنت في جميع أنحاء العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع الشبكات الاجتماعية، حيث مواقع التواصل الاجتماعي لديها أعلى تركيز للتفاعل البشري، تاركة الباب مفتوحًا على مصراعيه لمشاركة الأفكار والتجارب الجيدة، لكنها في المقابل تفضح أخلاق الناس، وإن صعوبة الرقابة على محتوى الإنترنت لا تعرض المجتمع للخطر فحسب، بل تعرض أيضًا المعلومات الشخصية لأنشطة خارجية تطفلية، والتي يمكن أن تهدد السلم الاجتماعي للبلد، نتيجة فقدان الأمن السيبراني الاجتماعي.
- **البعد السياسي:** بعيدًا عن تسريبات الوثائق السرية والامتيازات التي غالبًا ما تؤدي إلى أزمات دبلوماسية بين الدول، فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة إلى الأمن السيبراني وأهميته في البعد السياسي.
- **البعد القانونية:** يتطلب التطور التكنولوجي السريع الامتثال للقوانين القانونية من خلال تطوير الأطر والقوانين للأنشطة القانونية وغير القانونية في الفضاء السيبراني وأن الجرائم الإلكترونية هي في الغالب جرائم سيبرانية، وبعض البلدان ليس لديها إطار قانوني صارم للتعامل معها.

ومحصول القول: ان الأمن السيبراني هو مجموعة من الإجراءات والتدابير التي يتخذها الافراد والشركات والحكومات لحماية الأنظمة الحاسوبية والشبكات والبيانات الإلكترونية من التهديدات السيبرانية، ويشمل الأمن السيبراني حماية المعلومات الحساسة وتأمين الأنظمة والتطبيقات والأجهزة الإلكترونية من التطفل والتلاعب والتدمير.

2 : تطبيقات الذكاء الاصطناعي في الامن السيبراني

من خلال هذا المبحث ستتناول اهم الوظائف الرئيسة في الأمن السيبراني، وهذا من خلال المطلب الاول، ثم نأتي للحديث عن التحديات التي تواجه الذكاء الاصطناعي في الأمن السيبراني، وهذا في المطلب الاخير

1.2: الوظائف الرئيسية للذكاء الاصطناعي في الامن السيبراني

وفقًا لتقرير Capgemini حول تطورات الأمن السيبراني، فإن أهم ميزة رئيسية للذكاء الاصطناعي هي الأمن السيبراني، من خلال هذا المطلب سنناقش اهم الوظائف التي تخص الذكاء الاصطناعي في الأمن السيبراني

1. يمكن التعامل مع كميات كبيرة من البيانات

هناك الكثير من الأنشطة الجارية على خوادمنا، هذا يعني أنه يتم نقل كمية كبيرة من البيانات بين عملائنا ومنشآتنا وبين أجهزتنا وشبكاتنا كل يوم، وهذا يعني أن محللي الأمن السيبراني لا يمكنهم التحقق من كل شيء وبيانات عن المخاطر المحتملة، والذكاء الاصطناعي هو الخيار الأفضل لاكتشاف هذه التهديدات

التي تمر عبر الأنشطة اليومية، بالإضافة إلى فحص كميات كبيرة من البيانات، يمكنه مراقبة حركة المرور تلقائيًا وتحليل نشاط الخادم بدقة وتحديد المخاطر المحتملة في حركة مرور المعلومات.

2. توقع التهديدات المستقبلية

إن كمية البيانات التي تمر عبر محللي الأمن السيبراني تجعل من الصعب التنبؤ بالتهديدات المستقبلية، لكن الذكاء الاصطناعي يمكنه معالجة كميات كبيرة من البيانات في وقت واحد، مما يتيح الكشف المبكر عن الأنشطة الضارة، ويمكن أن يؤدي تحديد الإجراءات الوقائية والتهديدات المحتملة إلى تقليل الوقت الضائع وإهدار الموظفين، ويساعد على البقاء يقظًا من خلال اتخاذ خطوات لحماية المؤسسة.

3. تقليل وقت اكتشاف التهديد

القدرة على اكتشاف التهديدات بسرعة أمر بالغ الأهمية، حيث أبلغ 42٪ من المنظمات عن زيادة في التهديدات الحساسة للوقت، والناس بطيؤون في تبنيها وهم دون المستوى الأمثل، ومن ناحية أخرى، يمكن للذكاء الاصطناعي فحص كميات كبيرة من البيانات في وقت واحد لاكتشاف التهديدات السيبرانية، وبالتالي تسهيل الأمن، وأفادت 56 في المائة من المؤسسات أنها غارقة في ملف تعريف التهديد الذي يواجه المحللين السيبرانيين، وأفاد 23 في المائة منهم بأنهم غير قادرين على التحقق بشكل فعال من التهديدات المحددة.

4. التوفير والتوفير في التكاليف

تتأثر العديد من المؤسسات مالياً بانتهاكات البيانات كل عام، ولا يمكننا تجاهلها ولا يمكننا إيقاف المجرمين، حيث وجدت الدراسة فرقًا بنسبة 80٪ في توفير التكاليف للمنظمات التي تستخدم الذكاء الاصطناعي لأغراض الأمن السيبراني، 2.9 مليون دولار مقارنة بـ 6.71 مليون دولار للمرافق التي لا تستخدم الخدمة.[13]

ولعل من اهم تقنيات الذكاء الاصطناعي التي لها تأثير فعال نجد ChatGPT، وعلى الرغم من المخاوف بشأن مخاطر الذكاء الاصطناعي، هناك مزايا مهمة تجعل من ChatGPT أداة مفيدة لصناعة الأمن، واستخدام ChatGPT له فوائد عديدة في زيادة الإنتاجية، ومساعدة المهندسين، وتدريب الموظفين، وإنفاذ القانون. ومع ذلك، فإنه يحلل بشكل نقدي المخاوف المشروعة بشأن التحيز العنصري، ونقص المقاييس التي تم التحقق من صحتها، واستغلال جرائم الإنترنت، ونقاط الضعف والاستغلال، وقضايا الخصوصية، والهندسة الاجتماعية، والمعلومات المضللة، والحواجز التعليمية.

إن تطوير ChatGPT سيعمل على تحسين قدرة الصناعة على اكتشاف الهجمات الإلكترونية والاستجابة لها في الوقت الفعلي، وبالتالي تعزيز مرونة الأمن السيبراني بشكل عام، كما تبسط ChatGPT المهام كثيفة العمالة عن طريق تقليل إجهاد الانتباه، مما يسمح لموظفي الأمن بالتركيز على التفكير الاستراتيجي والتحليل ، وتتضمن أيضا إمكانات ChatGPT ميزات تساعد الباحثين عن البرامج الضارة على أداء مهام معقدة مثل إنشاء التعليمات البرمجية ومقارنة العقود وتحليل عينة البرامج الضارة، بالإضافة إلى ذلك، تقوم بسد فجوة المعرفة الأمنية من خلال تسهيل تدريب الموظفين وتعليمهم حول الاحتيال والهندسة الاجتماعية وأمن كلمات

المرور، بالإضافة إلى ذلك، قد تساعد ChatGPT جهات إنفاذ القانون في التحقيق والتنبؤ بالنشاط الإجرامي، ومساعدتهم على الاستجابة للتغيرات في تكتيكات وتقنيات الجرائم الإلكترونية ، وعلى الرغم من الفوائد العديدة لاستخدامChatGPT ، تواجه فرق الأمن تحديًا يتمثل في عدم وجود معايير موثوقة لتقييم سلامة أنظمة الذكاء الاصطناعي وأمانها ومرونتها، لقد تم بالفعل تسليح ChatGPT من قبل مجرمي الإنترنت واستخدموا لإنشاء وتوزيع إصدارات وتكتيكات متعددة من البرامج الضارة[14].

2.2: تحديات الذكاء الاصطناعي في الامن السيبراني

من خلال هذا المطلب سنقوم بطرح أبرز التحديات التي تواجه الذكاء الاصطناعي في الأمن السيبراني.

- يأتي دمج الذكاء الاصطناعي في أنظمة الأمن السيبراني مصحوبًا بالعديد من العقبات والقيود الأكثر شيوعًا هي الحواجز التي تحول دون استخدام واعتماد الذكاء الاصطناعي من قبل مجرمي الإنترنت.
- مع وضع هذا في الاعتبار، يعد الذكاء الاصطناعي صناعة جديدة ويجب على المؤسسات استثمار أموال ووقت كبير في قوة الحوسبة والذاكرة ومراكز البيانات لتكون قادرة على بناء أنظمة الذكاء الاصطناعي وصيانتها.
- أصبح دمج الذكاء الاصطناعي في الأمن السيبراني أمرًا ضروريًا للمنظمات، لكن العوائق الرئيسية التي تحول دون اعتماده ونموه هي احتياجات اكتساب المواهب، وتعقيد البيانات، واستخدام أدوات الذكاء الاصطناعي المناسبة
- ووفقًا لشركةIBM ، يعد هذا أحد أكبر العقبات التي تبطئ تبني الذكاء الاصطناعي وتطويره، حيث تكافح حوالي 37٪ من المؤسسات للعثور على أشخاص يتمتعون بالمستوى المناسب من الخبرة والمعرفة في هذا المجال، فإن تطوير الذكاء يؤدي إلى نقص اصطناعي في الإنسان، وهذا مهم جدًا للمؤسسات التي بدأت في تطوير الذكاء الاصطناعي.
- يعد تعقيد البيانات وامتلاك مجموعة الأدوات المناسبة من العوائق الرئيسية التي تواجه المنظمات في المراحل المتقدمة من تطوير الذكاء الاصطناعي في اعتماد الذكاء الاصطناعي.
- يجعل استخدام الذكاء الاصطناعي من قبل مجرمي الإنترنت من الذكاء الاصطناعي سلاحًا ذا حدين يمكن استخدامه ليس فقط كآلية هجوم قوية، ولكن أيضًا كأداة وقائية قوية، ومن جانب المهاجم، يمكن للمهاجمين استخدام الذكاء الاصطناعي لزيادة دقة وفعالية هجماتهم.
- تلتزم المنظمات التي تدمج الذكاء الاصطناعي في أنظمة الأمن السيبراني الخاصة بها بلوائح محددة، وغالبًا ما تحد من نطاق استخدامها، ومن ناحية أخرى، يتمتع مجرمو الإنترنت بملعب لا حدود له، مما يسهل عليهم استغلال التكنولوجيا.

- يعد التعتيم أحد أكثر تقنيات تحليل البرامج شيوعًا التي يستخدمها المتسللون، ويتم استخدامه بشكل أساسي لإيجاد تغييرات أمنية في البرامج المعقدة. الغرض الرئيسي من هذه التقنية هو العثور على ثغرات النظام
- يزيد استخدام الذكاء الاصطناعي في هذه التقنية من دقة وفعالية الهجمات، مما يخلق تهديدات مدمرة، ويمكن أيضًا استخدام الذكاء الاصطناعي في هجمات التصيد الاحتيالي.[15]

مما سبق يمكن القول ان الذكاء الاصطناعي في الأمن السيبراني يشير إلى استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي لتعزيز قدرة الأنظمة والشبكات على اكتشاف ومكافحة التهديدات السيبرانية، ويستخدم الذكاء الاصطناعي في الأمن السيبراني لتحليل البيانات الكبيرة وتحديد الأنماط والسلوكيات غير العادية التي قد تشير الهجمات المحتملة، وباستخدام الذكاء الاصطناعي في الأمن الأنترنت، يمكن تعزيز المنظمات لمواجهة التهديدات السيبرانية وحماية البيانات والمعلومات الحساسة

الخاتمة:

تم تشكيل الفضاء الإلكتروني، وهو فضاء معلومات جديد يستخدمه الأفراد والدول، جنبًا إلى جنب على نطاق واسع، حيث تعتمد الدول بشكل كبير على شبكة الإنترنت وجعلها بيئة مهمة لإنشاء قواعد بيانات للخدمات الوطنية المختلفة، ونظرًا لأن الفضاء الإلكتروني متاح للجميع دون استثناء، فقد أدى ظهور الهجمات السيبرانية ، التي تتخذ أشكالًا وألوانًا عديدة، وخاصة الجرائم الإلكترونية والإرهاب السيبراني والصراع السيبراني بين الدول، إلى تقليل التبادلات الدولية والأمنية إلى حد كبير، و مع ظهور تقنية الذكاء الاصطناعي ، حيث تعد من أحدث التقنيات المستخدمة لتعزيز الأمن السيبراني، سارعت العديد من الدول الى توظيف هذه التقنية في مجال الامن السيبراني غير ان مثل هذه التقنيات تحتاج الى ضوابط وقوانيين تنظمها لذلك وجب على الدول تطوير الأطر القانونية الخاصة باستخدامات هذه التقنية على الصعيدين الإقليمي والدولي.

في النهاية، يمكن القول إن الذكاء الاصطناعي يمثل تقدمًا هائلا في مجال التكنولوجيا وله العديد من الفوائد والتطبيقات المحتملة، ومع ذلك، يجب أن يتم استخدامه بشكل مسؤول وفقًا للقوانين والأخلاقيات، وأن يتم التركيز على حماية الخصوصية وتجنب التأثيرات السلبية المحتملة لاستخدام هذه التكنولوجيا الجديدة وجعلها آلية فعالة لتحقيق الأمن السيبراني وفضاء رقمي أكثر امانا.

الهوامش:

1. درار، خديجة محمد. **أخلاقيات الذكاء الاصطناعي والروبوت**: دراسة تحليلية. المجلة الدولية لعلوم المكتبات والمعلومات، مج6, ع3 271. - 237، 2019). مسترجع من http//: search.mandumah.com/Record1

2. حسن بن محمد حسن العمري، **الذكاء الاصطناعي ودوره في العلاقات الدولية**، المجلة العربية للنشر العلمي، العدد29, 02اذار 2021م على الرابط
https://www.ajsp.net/research/%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A_%D9%88%D8%AF%D9%88%D8%B1%D9%87_%D9%81%D9%8A_%D8%A7%D9%84%D8%B9%D9%84%D8%A7%D9%82%D8%A7%D8%AA_%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9.pdf

3. نرمين مجدي ، **الذكاء الاصطناعي وتعلم الآلة**، سلسلة كتيبات تعريفية العدد 03، صندوق النقد العربي أبو ظبي، ،ص 05, الامارات العربية المتحدة ،2020 على الرابط
https://www.amf.org.ae/sites/default/files/publications/2021-12/artificial-intelligence-machine-learning.pdf

4. نرمين مجدي، نفس المرجع، ص 06

5. عادل عبد الصادق، **أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني**، مكتبة الإسكندرية وحدة الدراسات المستقبلية، الاسكندرية، 2016, ص7.

6. عادل عبد الصادق، نفس المرجع، ص11

7. أحمد عبد الحليم، **أمن الخليج: إلى أين؟** ، اوراق الشرق الأوسط، 1992, ص ،ص 28-29 .

8. تيري ديبيل، **إستراتيجية الشؤون الخارجية...منطق الحكم الأمريكي**، ترجمة :وليد شحادة، دار الكتاب – العربية ومؤسسة محمد بن آل راشد آل مكتوم، بيروت،2009 ، ص258

9. معجم اكسفورد على الرابطhttp:// en.oxforddictionaires.com/ definition/cyber :

10. ادريس عطية، **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**، مجلة مصداقية، جامعة العربي تبسي، تبسة، المجلد 01، العدد 01، 2019، ص 108.

11. لامية طالة، التهديدات **والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها**، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي تندوف، المجلد04, العدد 02، 2020، ص ص 60-61.

12. محمد مختار، الأمن **السيبراني مفاهيم المستقبل**، مجلة اتجاهات الأحداث، العدد 02، 2015، ص06.

13. **فوائد لاستخدام الذكاء الاصطناعي في الأمن السيبراني** على الرابط (thakaa.sa) تمت زيارة الرابط في 08اوت 2023

14. أوبانلا أوبييمي **مزايا واهتمامات ChatGPT في الأمن السيبراني** نشر يوم 8يونيو 2023 – تم الاطلاع على الرابط في 11اوت 2023 -https://tuxcare.com/ar/blog/advantages-and-concerns-of-chatgpt-in-cybersecurity/

15. البانا ايسيني، **الذكاء الاصطناعي والأمن السيبراني**: دراسة فيما يخبئه المستقبل، مركز البيان للدراسات والتخطيط على الرابط87ygh2.pdf