دور الذكاء الاصطناعي في الامن السيبراني

أ.م.د. باسم علي خريسان
جامعة بغداد –مركز الدراسات الاستراتيجية والدولية

المستخلص

يتناول البحث التأثير الكبير للتحول الرقمي ودور الذكاء الاصطناعي في مواجهة التحديات الأمنية التي يفرضها الفضاء السيبراني يشير إلى أن التحول نحو الفضاء السيبراني قد أدى إلى زيادة الهجمات السيبرانية التي تتكرر كل ١٤ ثانية، مما يؤدي إلى خسائر تقدر بتريليونات الدولارات سنوياً يبرز البحث أهمية الذكاء الاصطناعي في بناء منظومة أمنية متكاملة، قادرة على التكيف مع التهديدات السيبرانية المتزايدة كما يستعرض مفهوم الذكاء الاصطناعي وأنواعه وتطبيقاته في الأمن السيبراني، مثل كشف التهديدات بشكل أسرع وتقليل هامش الخطأ وأخيرًا، يناقش البحث مستقبل دور الذكاء الاصطناعي في الأمن السيبراني، مشيراً إلى ضرورة دمجه مع تقنيات أخرى كـ blockchain وإنترنت الأشياء لمواجهة التهديدات المستقبلية.

الكلمات المفتاحية

التحول الرقمي – الذكاء الاصطناعي – الفضاء السيبراني – الأمن السيبراني – الهجمات السيبرانية –إنترنت الأشياء (IoT) .

The Role of Artificial Intelligence in Cybersecurity

Dr.Basim Ali Khrasian

Abstract

This research explores the significant impact of digital transformation and the role of artificial intelligence (AI) in addressing the security challenges posed by cyberspace. It indicates that the shift towards cyberspace has led to an increase in cyberattacks, occurring every 14 seconds, resulting in losses estimated at trillions of dollars annually. The research highlights the importance of AI in building an integrated security system capable of adapting to the growing cyber threats. It also reviews the concept of AI, its types, and its applications in cybersecurity, such as faster threat detection and reducing the margin of error. Finally, the research discusses the future role of AI in cybersecurity, emphasizing the need to integrate it with other technologies like blockchain and the Internet of Things to counter future threats.

Keywords

Digital transformation, Artificial intelligence, Cyberspace, cybersecurity, cyber-attacks, inter net of things.

المقدمـــة

التحول الكبير الذي تشهده البشرية بالانتقال نحو الفضاء السيبراني قد أحدث تغييرات بنيوية واسعة النطاق، أثرت بشكل عميق في جميع جوانب الحياة، هذه التغييرات أوجدت تحديات خطيرة تهدد سلامة الفرد والمجتمع على حد سواء، مما يستدعي استجابة علمية منظمة وقادرة على تقديم حلول دقيقة تقلل من التأثيرات السلبية لهذه التهديدات السيبرانية.

يأتي في مقدمة هذه الحلول بناء منظومة أمنية سيبرانية متكاملة، تلبي متطلبات العصر وتعمل كدرعٍ واقٍ لحماية الأفراد والمجتمعات؛ لتحقيق هذا الهدف يجب تبني أحدث تقنيات العصر، وأهمها الذكاء الاصطناعي في مجال الأمن السيبراني، فقد أصبح من الواضح أن بناء أمن سيبراني فعّال في هذا العصر لا يمكن أن يتم دون الاستفادة من الدور الفاعل والمؤثر للذكاء الاصطناعي في تحقيق ذلك.

اولاً . مجال الذكاء الاصطناعي والامن السيبراني .

تشهد الإنسانية تقدمًا سريعًا وواسعًا ومعقدًا يشمل مجمل مجالات الحياة، ويؤسس لمرحلة حضارية مختلفة عن سابقاتها، هذه المرحلة تعمل على تفكيك الموجود أو إلغائه، وفي المقابل، تسعى إلى إنشاء معمار جديد معرفي-تكنولوجي يُعرف بالفضاء السيبراني، هذا الفضاء يفرض العديد من التحديات الوجودية التي تتطلب التكيف معها من خلال ولوج أدوات العصر، وبالأخص في مجال تكنولوجيا الاتصال والمعلوماتية، ومن أبرز أدوات عصرنا هو الذكاء الاصطناعي، الذي يُعد من أهم الفواعل المعاصرة المطلوبة لتعزيز الحضور في الفضاء السيبراني[1]، وبالأخص في مجال الأمن السيبراني الذي يتطلب حمايته من التهديدات السيبرانية التي تحدث كل ١٤ ثانية، والتي تسببت بتكاليف تصل إلى أكثر من ستة تريليونات دولار سنويًا، التهديد المتزايد والسريع للأمن السيبراني، الذي يتعلق بحماية الفضاء السيبراني بكل ما يحتويه من عناصر مادية ومعلوماتية ومعرفية وتكنولوجية، لا يمكن معالجته دون الاعتماد على أدوات الذكاء الاصطناعي التي تُعد أبرز سمات العصر السيبراني.

من جهة اخرى يُعد كل من الذكاء الاصطناعي والأمن السيبراني من المجالات الصعبة التي تتطلب مستوى عالٍ من الخبرة، ومن الصعب تحديد أيهما أصعب لأنه يعتمد على عوامل مختلفة، فالذكاء الاصطناعي هو عملية تطوير

أنظمة ذكية بما يكفي للتعلم وأداء المهام التي يقوم بها البشر عادةً، يتطلب الأمر معرفة في العديد من المجالات المختلفة مثل الرياضيات وعلوم الكمبيوتر والهندسة، وهناك العديد من المشكلات الصعبة التي يجب حلها عند إنشاء أنظمة الذكاء الاصطناعي، يتضمن ذلك إنشاء خوارزميات يمكنها التعلم من كميات كبيرة من البيانات، وفهم تأثير الذكاء الاصطناعي في الأخلاق والقانون، والتأكد من أن أنظمة الذكاء الاصطناعي آمنة ومأمونة، من ناحية أخرى، يتعلق الأمن السيبراني بالحفاظ على أنظمة الكمبيوتر والشبكات في مأمن من السرقة والتلف والوصول من قبل الأشخاص غير المخولين، ويتطلب خبرة في أنظمة الكمبيوتر والشبكات والبرمجة، ومن المهم البقاء على اطلاع بأحدث التهديدات ونقاط الضعف، يحتاج خبراء الأمن السيبراني أيضاً إلى معرفة كيفية إنشاء تدابير أمنية واستخدامها لحماية الأنظمة من هذه التهديدات، وكذلك كيفية اكتشاف الحوادث الأمنية والتعامل معها ، وفي النهاية يعد كل من الذكاء الاصطناعي والأمن السيبراني مجالين مهمين أصبحا أكثر أهمية مع تغير التكنولوجيا بسرعة ، يتطلب كلا المجالين مستوى عالٍ من الخبرة ويشكلان تحدًا بطريقتهما الخاصة [٢] .

ثانياً . مفهوم الذكاء الاصطناعي .

صُمم مصطلح "الذكاء الاصطناعي" لأول مرة في كلية دارتموث الامريكية عام ١٩٥٦، وذلك خلال مؤتمر تاريخي يعد نقطة انطلاق أساسية في مجال الذكاء الاصطناعي، كان العالم المعرفي (مارفن مينسكي) [٣] متفائلاً بشأن إمكانيات هذه التكنولوجيا المستقبلية، شهدت السنوات من ١٩٧٤ إلى ١٩٨٠ انخفاضاً ملحوظاً في التمويل الحكومي لبحوث الذكاء الاصطناعي، وهي فترة عُرفت باسم "شتاء الذكاء الاصطناعي"، عندما واجهت هذه التكنولوجيا انتقادات عديدة ومع ذلك، تجدد الاهتمام بالذكاء الاصطناعي في الثمانينيات بعد أن بدأت الحكومة البريطانية في تمويل المشاريع مرة أخرى، مدفوعةً بالقلق من التنافس مع اليابان في هذا المجال في العام ١٩٩٧، حقق جهاز "ديب بلو" من شركة آي بي إم إنجازاً تاريخيًا بتفوقه على بطل الشطرنج الروسي الكبير غاري كاسباروف، مما أعاد إشعال الاهتمام بالذكاء الاصطناعي .

يُعرف الذكاء الاصطناعي بأنه "مجال من مجالات علوم الكمبيوتر يهدف إلى منح الآلات القدرة على محاكاة الذكاء البشري" تساعد الأنظمة المعتمدة على الذكاء الاصطناعي، التي تُسمى أحيانًا الأنظمة المعرفية، في أتمتة العديد من الوظائف وتعزيز قدرتنا على معالجة المشكلات المعقدة التي قد يصعب حلها من قبل البشر .

ويعرف الذكاء الاصطناعي كذلك بقدرة الآلات على أداء مهام تتطلب الذكاء الذي يظهره الإنسان والحيوان غالبًا ما يُنسب هذا التعريف إلى مارفن مينسكي وجون مكارثي من الخمسينيات، اللذين يعدان أيضاً من آباء هذا المجال يسمح الذكاء الاصطناعي للآلات بفهم وتحقيق أهداف محددة، ويشمل تقنيات مثل التعلم الآلي والتعلم العميق، يشير التعلم الآلي إلى قدرة الآلات على التعلم تلقائيًا من البيانات المتاحة دون تدخل بشري، أما التعلم العميق، فيتيح للآلة معالجة كميات هائلة من البيانات غير المهيكلة مثل النصوص والصور والصوت، يجب أن يتمتع أي نظام ذكاء اصطناعي ببعض الخصائص الأساسية مثل الملاحظة، والقدرة التحليلية، وحل المشكلات والتعلم، وغيرها [٤].

من جهة اخرى في النصف الأول من القرن العشرين، قدّم الخيال العلمي للعالم مفهوم الروبوتات ذات الذكاء الاصطناعي، بدأ ذلك برجل القصدير "بلا قلب" من "ساحر أوز"، واستمر مع الروبوت الشبيه بالبشر الذي اتخذ شخصية ماريا في فليم "متروبوليس" لحلول الخمسينيات من القرن الماضي، كان هناك جيل من العلماء الرياضيات والفلاسفة المهتمين بمفهوم الذكاء الاصطناعي (AI) كان من بينهم (آلان تورينج)[٥]، الشاب البريطاني المتعدد الثقافات، الذي استكشف الاحتمال الرياضي للذكاء الاصطناعي، اقترح (تورينج) أن البشر يستخدمون المعلومات المتاحة فضلا عن العقلانية لحل المشكلات واتخاذ القرارات؛ فلماذا لا تستطيع الآلات أن تفعل الشيء نفسه؟ كان هذا هو الإطار المنطقي لورقته البحثية عام ١٩٥٠ بعنوان "آلات الحوسبة والذكاء"، حيث ناقش كيفية بناء آلات ذكية وكيفية اختبار ذكائها. [٦].

بعد ذلك شهد الذكاء الاصطناعي(AI) ، وخاصة التعلم الآلي (ML) والتعلم العميق (DL) ، تطورًا هائلًا في السنوات الأخيرة، ومن المتوقع أن يؤثر بشكل كبير في جميع جوانب المجتمع والمهن التي ينخرط فيها الناس، هذا التقدم في قوة الحوسبة، فضلا عن التطورات في الخوارزميات، لم يستثنِ مجال الأمن السيبراني.

كون عملية اكتشاف الأجيال الجديدة من البرمجيات الضارة والهجمات السيبرانية سوف تكون صعبة باستخدام الإجراءات التقليدية للأمن السيبراني، نظرًا لأن هذه التهديدات تتطور بمرور الوقت، من الضروري تبني نهج أكثر قوة، تعتمد حلول الأمان على بيانات استخدام التعلم الآلي من الهجمات السابقة لمواجهة أحدث

التهديدات، من المزايا الأخرى المهمة لأنظمة الذكاء الاصطناعي في الأمن السيبراني أنها توفر قدرًا هائلًا من الوقت لموظفي تكنولوجيا المعلومات، يُستخدم الذكاء الاصطناعي بشكل شائع لاكتشاف التهديدات والهجمات، حيث يتم تطوير الأنظمة بحيث تكون قادرة على التصرف بسرعة وبشكل مستقل خاصة ان أنظمة الذكاء الاصطناعي لا ترتكب أخطاء في إنجاز مهامها، مما يعني أنه يتم الرد على كل تهديد بطريقة فعالة وأدق في المستقبل، من المتوقع زيادة سريعة في التصادمات الدولية في الفضاء السيبراني، والتي قد تشمل هجمات على البنية التحتية والمرافق، فضلاً عن الإضرار بالعمليات العادية للحكومات والهيئات المالية، والمؤسسات التقليدية مثل البنوك والصحافة وإنفاذ القانون والقضاء لذا، من الضروري دراسة الأمن السيبراني كقضية رئيسة، وتحديد التحديات واستكشاف دور الذكاء الاصطناعي والتعلم الآلي والتعلم العميق في تجنب الجرائم السيبرانية المستقبلية [٧].

ثالثاً. مفهوم الفضاء السيبراني.

يعد الفضاء السيبراني أكثر من مجرد إنترنت يشير إلى بيئة الإنترنت حيث يشارك العديد من المشاركين في التفاعلات الاجتماعية ولديهم القدرة على التأثير على بعضهم البعض يتفاعل الناس في الفضاء السيبراني من خلال استخدام الوسائط الرقمية أمثلة على تفاعلات الفضاء السيبراني هي من خلال مواقع الشبكات الاجتماعية القائمة على الإنترنت مثل Facebook و Twitter و Instagram، يمكن للأشخاص البقاء على اتصال بأحبائهم (مثل العائلة والأصدقاء) ومجتمعهم الأكبر (مثل الأقارب البعيدين وزملاء سابقين) وحتى تكوين صداقات جديدة عبر الإنترنت، عندما يكون الأشخاص متصلين بالإنترنت، ينخرط معظمهم في أنشطة تترك بصمة رقمية تشير البصمة الرقمية إلى جميع المعلومات الموجودة على الإنترنت عن الشخص يتم نشره بواسطة هذا الشخص أو غيره، عن قصد أو عن غير قصد . تترك هذه المعلومات علامة دائمة حيث يمكن للآخرين استردادها واسترجاعها ونقلها بسهولة يمكن استخدام البصمة الرقمية من قبل أرباب العمل والجامعات المحتملين الباحثين عن معلومات حول الموظفين والطلاب المحتملين [٨].

يمكن تحديد الفضاء السيبراني بما يأتي [٩]:

١. المساحة غير المادية التي أنشأتها شبكات الكمبيوتر، حيث يمكن للأشخاص التواصل بطرق مختلفة.

٢. تتكون هذه المساحة غير المادية من أجهزة الكمبيوتر وأنظمتها وبرامجها والمستخدمين مثل المبرمجين ومحللي البيانات وفنيي الكمبيوتر، على سبيل المثال لا الحصر.

٣. يستخدم مصطلح الفضاء السيبراني بالاقتران مع الواقع الافتراضي، يحدد المكان الخيالي حيث توجد الأشياء الافتراضية.

٤. يعد شبكة الترابط بين البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المضمنة.

٥. يشير المصطلح إلى البيئة التي يحدث فيها التنمر عبر الإنترنت.

٦. يعد الفضاء السيبراني المساحة التفاعلية التي تم إنشاؤها للتفاعل والتبادل على الإنترنت.

٧. الفضاء السيبراني هو البيئة النظرية التي يحدث فيها الاتصال عبر شبكات الكمبيوتر.

٨. الفضاء السيبراني هو البيئة الافتراضية حيث يحدث الاتصال الرقمي عبر شبكات الكمبيوتر.

٩. يستخدم مصطلح الفضاء السيبراني لوصف الشبكة الافتراضية العالمية للأجهزة الرقمية المتصلة.

١٠. أصبح مصطلح الفضاء السيبراني مرادفاً للإنترنت و/أو شبكة الويب العالمية.

١١. يتميز الفضاء السيبراني باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين البيانات وتعديلها وتبادلها عبر أنظمة الشبكات والبنى التحتية المادية المرتبطة بها.

١٢. يمثل الفضاء السيبراني البيئة التي تم إنشاؤها بواسطة الروابط الملموسة مثل الكمبيوتر، وغير الملموس مثل التطبيقات والخدمات، والشبكات مثل الإنترنت والاتصالات.

رابعاً. مفهوم الامن السيبراني.

ما الأمن السيبراني؟ يبدو وكأنه سؤال بسيط في قلب التحدي السياسي الذي أصبحت عليه هذه القضية، يتجلى في الصعوبات التي يعترف بها العديد من الجهات الحكومية عندما يتعلق الأمر بالموافقة على التعاريف الرسمية، الأمن السيبراني من الصعب تحديده وهو محل نزاع سياسي في الساحات الوطنية والدولية[١٠].

هنالك أكثر من (٤٠٠) مفهوم للامن السيبراني تم تصنيفها بواسطة مجموعة متنوعة من الجهات الفاعلة، بما في ذلك الحكومات والشركات والمنظمات الدولية والمجتمع التقني والمجتمع المدني. تؤثر تهديدات الأمن السيبراني على النظام البيئي للإنترنت بأكمله، بما في ذلك البنية التحتية المادية والبرامج/الأجهزة والتطبيقات. يتعلق الأمر بحماية المعلومات التي نشاركها ونحتفظ بها عبر الإنترنت وفي الفضاء السيبراني، بما في ذلك الاتصالات والمعلومات المالية

والسجلات الطبية وبيانات الملكية الى الخ. بعض هذه التهديدات لها تأثيرات أكثر بكثير من إغلاق موقع أو الوصول إلى البيانات، يمكن أن يكون لها آثار خطيرة على حياة الناس – من المحامين والصحفيين والمستهلكين[١١].

وفقًا للاتحاد الدولي للاتصالات، يشير الأمن السيبراني إلى مجموعة الأدوات والسياسات ومفاهيم الأمن، والضمانات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة وأصول المستخدم، تشمل المنظمة وأصول المستخدم أجهزة الحوسبة المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المرسل و / أو المعلومات المخزنة في البيئة السيبرانية، يسعى الأمن السيبراني إلى ضمان تحقيق وصيانة الخصائص الأمنية لأصول المنظمة والمستخدم ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية– الإنترنت، يمكن أيضاً وصف الأمن السيبراني بأنه مجموعة التقنيات والعمليات والممارسات المصممة لحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، يلاحظ الاتحاد الدولي للاتصالات أيضاً أن الأهداف العامة للأمن السيبراني هي: التوفر، النزاهة (والتي قد تشمل المصداقية وعدم التنصل) والسرية من أجل فهم مفهوم الأمن السيبراني بشكل كامل ، سنقوم بفحص مختلف مكونات الأمن السيبراني والتدابير الواجب اتخاذها لضمان لتأمين الفضاء السيبراني [١٢].

ينظر للأمن السيبراني بانه ممارسة تأمين الشبكات والأنظمة وأي بنية تحتية رقمية أخرى من الهجمات الخبيثة. من المتوقع أن تتجاوز الأضرار الناجمة عن الجرائم السيبرانية مبلغاً مذهلاً يبلغ أكثر (٦) تريليون دولار مستقبلاً، فلا عجب أن تستثمر البنوك وشركات التكنولوجيا والمستشفيات والوكالات الحكومية وكل قطاع آخر تقريباً في البنية التحتية للأمن السيبراني لحماية ممارسات أعمالهم والملايين من العملاء الذين يثقون بهم، ما هي أفضل استراتيجية للأمن السيبراني ؟ تتضمن البنية التحتية الأمنية القوية طبقات متعددة من الحماية موزعة عبر أجهزة الكمبيوتر والبرامج والشبكات الخاصة بالشركات مع وقوع هجمات سيبرانية في كل (١٤) ثانية، يجب أن تعمل جدران الحماية وبرامج مكافحة الفيروسات وبرامج مكافحة برامج التجسس وأدوات إدارة كلمات المرور في وئام لتتفوق على المجرمين السيبرانيين المبدعين بشكل مدهش مع وجود الكثير من المخاطر ، ليس من المبالغة الاعتقاد بأن الادوات

وخبراء الأمن السيبراني بمثابة خط الدفاع الأخيرين المعلومات الأكثر أهمية لدينا والفوضى الرقمية [١٣] لذلك يعرف الامن السيبراني بانه ممارسة الدفاع عن أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الخبيثة يُعرف أيضاً باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكتروني، ويشمل مجالات واسعة من النشاطات المختلفة ويمكن تقسيمها خمسة مجالات [١٤] .

١. أمن الشبكة هو ممارسة تأمين شبكة الكمبيوتر من المتسللين، سواء كانوا مهاجمين مستهدفين أم برامج ضارة انتهازية.
٢. أمن البيانات يركز على إبقاء البرامج والأجهزة خالية من التهديدات، يبدأ الأمان الناجح في مرحلة التصميم، قبل نشر البرنامج أو الجهاز بوقت طويل.
٣. أمن المعلومات يحمي سلامة وخصوصية البيانات، سواء في التخزين أو في النقل.
٤. الأمن التشغيلي يشمل العمليات والقرارات للتعامل مع أصول البيانات وحمايتها الأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة والإجراءات التي تحدد كيفية ومكان تخزين البيانات أو مشاركتها تقع جميعها تحت هذه المظلة.
٥. يحدد التعافي من الكوارث واستمرارية الأعمال كيفية استجابة المنظمة لحادث الأمن السيبراني أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات تملي سياسات التعافي من الكوارث كيفية استعادة المنظمة لعملياتها ومعلوماتها للعودة إلى نفس القدرة التشغيلية التي كانت عليها قبل الحدث، استمرارية الأعمال هي الخطة التي ترجع إليها المنظمة أثناء محاولتها العمل بدون موارد معينة.
٦. عالج تعليم المستخدم النهائي أكثر عوامل الأمن السيبراني التي لا يمكن التنبؤ بها: الأشخاص. يمكن لأي شخص إدخال فيروس إلى نظام آمن عن طريق الفشل في اتباع ممارسات الأمان الجيدة. يعد تعليم المستخدمين حذف مرفقات البريد الإلكتروني المشبوهة، وعدم توصيل محركات أقراص USB غير المعروفة، والعديد من الدروس المهمة الأخرى أمراً حيوياً لأمان أي مؤسسة ،اما ابرز الاتجاهات في الامن السيبراني ،فيمكن ان نسلط الضوء على ثلاثة اتجاهات تشير إلى الطبيعة المتغيرة للجناة، اولاً اقتصاد الجريمة الاقتصادية السيبرانية الجديد المتزايد ،الثانية تتلاقى القدرات الجهات الحكومية والمنظمة والجماعات الإجرامية: الجهات الحكومية توظف بشكل متزايد مثل هذا المجموعات باسم "المرتزقة السيبرانيين" ،ثالثاً لأن الدول تطور بسرعة القدرات الهجومية ، التهديد بأن تصبح الأسلحة السيبرانية مكوناً رئيساً في الحرب هو في ازدياد [١٥] .

خامساً . التهديدات الامنية في الفضاء السيبراني .

تؤثر التهديدات الأمنية السيبرانية على الأفراد والمجتمعات والدول بشكل متزايد ، مما يفرض عليهم مواجهة تحديات ذاتية وموضوعية تتطلب استجابة فعّالة وسريعة للتخفيف من آثار هذه التهديدات على مدار العقدين الماضيين، شهدنا زيادة ملحوظة في الهجمات السيبرانية التي استهدفت البنية التحتية الحيوية في الدول المتقدمة، مما ألحق خسائر فادحة بعدد كبير من الشركات سنويًا ، يتم تسجيل أكثر من (٢٠٠٠) انتهاك مؤكد للبيانات على مستوى العالم، حيث يكلف كل خرق منها في المتوسط أكثر من (٣,٩) مليون دولار، و(٨,١) مليون دولار في الولايات المتحدة الأمريكية . منذ العام ٢٠٠٠ ، تعرضت معلومات خاصة لأكثر من (٣,٥) مليار شخص للسرقة من قبل مجرمي الإنترنت، مما يعادل نصف سكان العالم تقريبًا يمكن أن تؤثر هذه الانتهاكات والتهديدات الأمنية على أي نظام تقريبًا ، بما في ذلك [١٦] :

١ . **الاتصالات** . يمكن استخدام المكالمات الهاتفية ورسائل البريد الإلكتروني والرسائل النصية وتطبيقات المراسلة في الهجمات السيبرانية .

٢ . **التمويل** . بطبيعة الحال، تعد المؤسسات المالية هدفاً أساسياً للمهاجمين، وتتعرض أية مؤسسة تعالج معلومات البنوك أو بطاقة الائتمان أو تتعامل معها للخطر

٣ . **الحكومات** . عادة ما يتم استهداف المؤسسات الحكومية بواسطة مجرمي الإنترنت، للحصول على معلومات المواطنين الخاصة أو البيانات العامة السرية .

٤ . **النقل** . السيارات المتصلة وأنظمة التحكم في حركة المرور والبنية التحتية للطرق الذكية كلها معرضة لخطر التهديدات السيبرانية .

٥ . **الرعاية الصحية** . السجلات الطبية في اي عيادة محلية إلى أنظمة الرعاية الحرجة في المستشفى العام تكون عرضة للهجوم .

٦ . **التعليم** . تتعرض المؤسسات التعليمية وبياناتها البحثية السرية والمعلومات التي بحوزتها عن الطلاب أو الموظفين لخطر الهجوم السيبراني .

إن التحضير والدفاع ضد تهديدات الأمن السيبراني يجب أن يكون أحد أهم المجالات، الهدف الأساس للأمن السيبراني هو حماية البيانات، يشير مجتمع الأمان عموماً إلى مثلث من ثلاثة مبادئ ذات صلة تضمن أمان البيانات، والمعروف باسم ثالوث وكالة المخابرات المركزية:

١. **السرية**. ضمان عدم إمكانية الوصول إلى البيانات الحساسة إلا لأولئك الأشخاص الذين يحتاجونها بالفعل، ويُسمح لهم بالوصول إليها وفقاً للسياسات التنظيمية، مع حظر الوصول إلى الآخرين.

٢. **النزاهة**. التأكد من عدم تعديل البيانات والأنظمة بسبب الإجراءات التي تتخذها الجهات المهددة، أو التعديل العرضي، ينبغي اتخاذ تدابير لمنع الفساد أو فقدان البيانات الحساسة، والتعافي السريع من مثل هذا الحدث في حالة حدوثه.

٣. **التوفر**. ضمان بقاء البيانات متاحة ومفيدة لمستخدميها النهائيين، وعدم إعاقة هذا الوصول بسبب عطل في النظام أو الهجمات السيبرانية أو حتى الإجراءات الأمنية نفسها [١٧].

لا تتساوى الجهات الفاعلة في التهديد السيبراني من حيث القدرات والتطور، حيث تمتلك كل منها مستويات مختلفة من الموارد والتدريب والدعم لأنشطتها قد تعمل الجهات الفاعلة في التهديد السيبراني بشكل فردي أو كجزء من منظمة أكبر، مثل برامج الاستخبارات التابعة لدولة قومية أو الجريمة المنظمة أحياناً، حتى الجهات الفاعلة المتقدمة تستخدم أدوات وتقنيات أقل تطوراً ومتاحة بسهولة لأنها قد تكون فعّالة لمهمة معينة و/أو تجعل من الصعب على المدافعين القيام بمهامهم، أما أهم الأدوات المستخدمة في إحداث تهديد للأمن في الفضاء السيبراني فهي كالاتي:

١. **البرمجيات الخبيثة**. وهي البرامج التي تؤدي مهمة ضارة على جهاز أو شبكة مستهدفة، على سبيل المثال إفساد البيانات أو الاستيلاء على نظام.

٢. **التصيد**. هجوم عبر البريد الإلكتروني يتضمن خداع مستلم البريد الإلكتروني للكشف عن معلومات سرية أو تنزيل برامج ضارة بالنقر فوق ارتباط تشعبي في الرسالة.

٣. **التصيد بالرمح**. تكون أكثر تعقيداً من التصيد الاحتيالي حيث يتعرف المهاجم على الضحية وينتحل شخصية شخص يعرفه الضحية ويثق به.

٤. **هجوم "رجل في الوسط" (MitM)** . حيث ينشأ المهاجم موقعاً بين مرسل الرسائل الإلكترونية ومتلقيها ويعترضها، وربما يغيرها أثناء النقل. يعتقد المرسل والمتلقي أنهما يتواصلان مباشرة مع بعضهما البعض. يمكن استخدام هجوم MitM في الجيش لإرباك العدو.

٥. **حصان طروادة.** تم تسميته على اسم حصان طروادة في التاريخ اليوناني القديم، وهو نوع من البرامج الضارة التي تدخل نظاماً مستهدفاً يشبه شيئاً واحداً، على سبيل المثال قطعة قياسية من البرامج، ولكنها تسمح بعد ذلك بإخراج الشفرة الضارة مرة واحدة داخل النظام المضيف، (هي شفرة صغيرة يتم تحميلها مع برنامج رئيس من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته)

٦. **برامج الفدية.** هجوم يتضمن تشفير البيانات على النظام المستهدف والمطالبة بفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى، تتراوح هذه الهجمات من الإزعاج منخفض المستوى إلى الحوادث الخطيرة مثل إغلاق مدينة أتلانتا في الولايات المتحدة الامريكية بالكامل لبيانات الحكومة البلدية في عام ٢٠١٨.

٧. **هجوم رفض الخدمة أو هجوم رفض الخدمة الموزع (DDoS)** . حيث يستولي المهاجم على العديد (ربما الآلاف) من الأجهزة ويستخدمها لاستدعاء وظائف النظام المستهدف، على سبيل المثال موقع ويب، مما تسبب في تعطله بسبب زيادة الطلب.

٨. **الهجمات على أجهزة إنترنت الأشياء.** أجهزة إنترنت الأشياء مثل المستشعرات الصناعية عرضة لأنواع متعددة من التهديدات السيبرانية، يتضمن ذلك المتسللين الذين يستولون على الجهاز لجعله جزءاً من هجوم (DdoS) والوصول غير المصرح به إلى البيانات التي يتم جمعها بواسطة الجهاز نظرًا لأعدادها وتوزيعها الجغرافي وأنظمة التشغيل القديمة في كثير من الأحيان، تعد أجهزة إنترنت الأشياء هدفاً رئيساً للجهات الفاعلة الخبيثة.

٩. **خروقات البيانات.** خرق البيانات هو سرقة البيانات من قبل جهة فاعلة ضارة، تشمل دوافع انتهاكات البيانات الجريمة (أي سرقة الهوية)، والرغبة في إحراج مؤسسة (مثل إدوارد سنودن أو اختراق DNC)، والتجسس.

١٠. **البرامج الضارة على تطبيقات الجوال.** الأجهزة المحمولة عرضة لهجمات البرامج الضارة تماماً مثل أجهزة الحوسبة الأخرى قد يقوم المهاجمون بتضمين البرامج الضارة في تنزيلات التطبيقات أو مواقع الويب للجوال أو رسائل البريد الإلكتروني المخادعة والرسائل النصية بمجرد اختراق الجهاز المحمول، يمكن أن يمنح الفاعل الضار إمكانية الوصول إلى المعلومات الشخصية وبيانات الموقع والحسابات المالية والمزيد اما مصادر تهديدات الأمن السيبراني فهي تأتي من مجموعة متنوعة من الأماكن والأشخاص والسياقات، تشمل الجهات الخبيثة: الأفراد الذين يقومون بإنشاء ناقلات هجوم باستخدام أدوات البرامج الخاصة بهم، المنظمات الإجرامية التي تدار مثل الشركات ، حيث يقوم عدد كبير من الموظفين بتطوير ناقلات هجوم وتنفيذ هجمات الدول إرهابيون جواسيس المجال الصناعي، جماعات الجريمة المنظمة المطلعين غير سعداء، القراصنة والمنافسون في العمل [١٨].

سادساً. مواجهة التهديدات السيبرانية باستخدام الذكاء الاصطناعي.

يعد إدخال الذكاء الاصطناعي في الأمن السيبراني مفيداً بشكل لا يصدق لأتمتة عمليات صنع القرار بسرعة وإنشاء أنماط من البيانات غير المكتملة أو المعدلة تتعلم هذه الخوارزميات من بيانات العالم الحقيقي مثل التهديدات الأمنية الحالية أو الأمثلة التي وجدها الباحثون، ونتيجة لذلك، فإنها توفر مزايا عديدة مثل:

١. تتمثل إحدى المشاكل الكبيرة في الصناعة في نقص المهنيين المدربين، لذلك يمكن للذكاء الاصطناعي أن يكمل هذه الفجوة إنه أيضاً حل قابل للتطوير لأدوات الأمان الأخرى ويحرر الموارد القيمة عن طريق تحديد التهديدات بسرعة، مما يسمح للعمال بالتركيز على المهام الأكثر تعقيدًا .

٢. **كشف التهديدات بشكل أسرع.** قد تستغرق التحقيقات في التنبيهات الفردية أياماً حتى تكتمل؛ لذلك فإن أدوات الأمان التي تعمل بالذكاء الاصطناعي قادرة على تصنيف الأحداث في وقت أقل بكثير، مما يتيح الاستجابة السريعة للحوادث توفر هذه الأنظمة رؤى التهديدات العالمية، وكذلك الخاصة بالصناعة، من أجل صياغة قرارات تحديد الأولويات الحيوية بشكل أفضل بناءً على الهجمات المحتملة الحالية والمستقبلية .

٣. **هامش الخطأ الأدنى.** على الرغم من أن أنظمة التعلم الالي ليست سحرية ويمكن أن ترتكب أخطاء، إلا أن هامش الخطأ فيها ضئيل ينعكس هذا في حقيقة أن عملية اتخاذ القرار السريعة تقلل من

احتكاك المستخدم ولا تؤثر سلبًا على تجربة المستخدم، يؤدي ذلك إلى تحسين الأمن السيبراني على نطاق واسع ويغطي مساحة كبيرة في مشهد التهديدات.

٤. **الحماية من الهجمات الجديدة.** غالبًا ما تتطور تهديدات الأمان والبرامج الضارة والأساليب العدائية بناءً على نفس البرامج الضارة والتهديدات القديمة نظرًا لأنها تتطور خطيًا، يعد الذكاء الاصطناعي أداة مفيدة للغاية، ونادرًا ما يتم إجراء تعديلات على التهديدات الجديدة كافية لهزيمة الخوارزميات يتيح الذكاء الاصطناعي الذكاء التنبئي الفائق من خلال معالجة اللغة الطبيعية، والتي توفر رؤى حول الحالات الشاذة الجديدة والهجمات الإلكترونية واستراتيجيات الوقاية.

٥. **قتال الروبوتات.** تمثل الروبوتات جزءًا كبيرًا من حركة المرور الرقمية، ولكنها قد تكون خطيرة، حيث يمكنها سرقة بيانات الاعتماد أو إنشاء حسابات مزيفة أو الاحتيال على البيانات لا يمكن معالجة التهديدات الآلية من خلال الاستجابات اليدوية، لذلك يساعد الذكاء الاصطناعي في فهم حركة المرور على كل موقع ويب والتمييز بين الروبوتات "الجيدة" والخبيثة.

٦. **حماية أفضل لنقاط النهاية.** زاد عدد الأجهزة التي تعمل عن بُعد بشكل كبير منذ بداية وباء كورونا، ويمكن أن يكون الذكاء الاصطناعي عاملاً رئيسا في حمايتها على الرغم من أن حلول مكافحة الفيروسات تساعد في مكافحة البرامج الضارة وهجمات برامج الفدية، إذا تأخر تحديد الفيروسات، فقد يكون ذلك خطيرًا، تتخذ حماية نقطة النهاية المستندة إلى الذكاء الاصطناعي نهجًا مختلفًا من خلال إنشاء خط أساس للسلوك لنقطة النهاية من خلال عملية تدريب متكرر، إذا حدث شيء خارج عن المألوف، فإنه يكتشفه ويتخذ الإجراءات، ويوفر حماية استباقية[١٩].

سابعاً. مستقبل دور الذكاء الاصطناعي في مجال الامن السيبراني.

مستقبل الذكاء الاصطناعي في مجال الأمن السيبراني مثير للغاية، حيث يوجد مجال واسع للنمو والابتكار. مع ازدياد حالات الاستخدام والتطبيقات، من المحتمل أن يتوسع دور الذكاء الاصطناعي في هذا المجال أحد المجالات المحتملة التي يمكن دمج الذكاء الاصطناعي فيها مع التقنيات الأخرى هو تقنيات البلوكشين وإنترنت الأشياء (IoT). ومع تزايد أهمية الذكاء الاصطناعي في الأمن السيبراني، سيزداد الطلب على الأشخاص الذين يعرفون كيفية استخدام الذكاء الاصطناعي في هذا المجال سيكون من الضروري لهؤلاء المحترفين فهمًا عميقًا لتقنيات الأمن

السيبراني والذكاء الاصطناعي، نظرًا لوجود العديد من المخاطر الأمنية المرتبطة بأنظمة الذكاء الاصطناعي وهي:

أ. **عرضة الذكاء الاصطناعي للهجمات.** يمكن أن تكون أنظمة الذكاء الاصطناعي هدفًا للهجمات، وفي حال تعرضها للخطر، قد تتحمل المؤسسات المسؤولية وفقًا لتقرير صادر عن شركة (Deloitte)، يعتقد ٩٠٪ من المؤسسات التي شملتها الدراسة أن الذكاء الاصطناعي معرض للهجمات السيبرانية، و٤٤٪ منها قد تعرضت بالفعل لهجوم على أنظمة الذكاء الاصطناعي الخاصة بها.

ب. **الافتقار إلى الشفافية وقابلية التفسير.** قد يؤدي الافتقار إلى الشفافية وقابلية التفسير في خوارزميات الذكاء الاصطناعي إلى صعوبة فهم كيفية اتخاذها للقرارات، مما يجعل تحديد المشكلات المحتملة ومعالجتها أمرًا صعبًا، في استطلاع أجرته شركة (O'Reilly)، قال ٥٧٪ من المشاركين إن الذكاء الاصطناعي عمل معقد يصعب فهمه.

ج. **التحيز في الخوارزميات.** يمكن أن تكون خوارزميات الذكاء الاصطناعي متحيزة بناءً على البيانات المستخدمة لتدريبها، مما قد يؤدي إلى عواقب غير مقصودة وتمييز لذا، يجب على المنظمات التي تطور أنظمة الذكاء الاصطناعي أن تضع الاهتمامات الأخلاقية في مقدمة أولوياتها.

رغم وجود المشكلات، فإن إمكانات الذكاء الاصطناعي في الأمن السيبراني كبيرة وتأثيره محسوس بالفعل من الضروري استخدام الذكاء الاصطناعي في الأمن السيبراني لتحسين الحماية ضد التهديدات السيبرانية، حيث يمكن للذكاء الاصطناعي اكتشاف التهديدات والاستجابة لها بشكل أسرع وأكثر دقة من خلال تحليل كميات ضخمة من البيانات والبحث عن التهديدات المحتملة.

وبالرغم من التحديات والمخاوف المرتبطة باستخدام الذكاء الاصطناعي في الأمن السيبراني، إلا أن هناك فوائد كبيرة يمكن أن تأتي من استخدام هذه التقنية يجب على المنظمات مراعاة المخاوف الأخلاقية ومعالجة المشكلات لضمان أن تكون أنظمة الأمن السيبراني التي تعتمد على الذكاء الاصطناعي آمنة وعادلة وشفافة، مما سيساعد على توفير حماية أفضل ضد التهديدات السيبرانية على المدى الطويل [٢٠].

الخاتمـــــــة

يمثل التطور السريع والمتنامي في مجال الذكاء الاصطناعي تحديًا وفرصةً غير مسبوقة في عالمنا الحديث من جهة، يحمل هذا التطور في طياته مخاطر جدية إذا لم يتم التعامل معه بحذر وإدراك عميقين؛ حيث يمكن أن يؤدي إلى فقدان السيطرة على العديد من العمليات الحيوية إذا لم تتوفر البنية التحتية والقدرات البشرية اللازمة لإدارته بفعالية ومن جهة أخرى، يوفر الذكاء الاصطناعي فرصة هائلة للاستفادة منه في مختلف مجالات الحياة، بما في ذلك الصحة والتعليم والصناعة، ولكنه يتجلى بشكل خاص في المجال السيبراني الذي بات يشكل العمود الفقري للعالم الرقمي اليوم.

لقد أدى التحول الرقمي السريع نحو الفضاء السيبراني إلى إعادة تشكيل كل من الحياة الشخصية والمهنية بشكل جذري فالعديد من التعاملات التي كانت تتم وجهًا لوجه في الواقع المادي، انتقلت الآن إلى الفضاء السيبراني، سواء في مجالات الأعمال أو الاتصالات أو حتى الترفيه هذا التحول لم يأتِ دون ثمن، إذ إنه جلب معه مجموعة متزايدة من التهديدات السيبرانية التي أصبحت جزءًا لا يتجزأ من الحياة اليومية هذه التهديدات لم تعد مجرد مخاوف نظرية، بل تحولت إلى واقع ملموس يؤثر على الأفراد والمؤسسات والحكومات بشكل مباشر.

في ظل هذه التحديات المتزايدة، أصبح من الضروري تطوير استراتيجيات جديدة لحماية الفضاء السيبراني الأدوات التقليدية للأمن السيبراني، التي كانت فعالة في الماضي، لم تعد كافية لمواجهة التعقيد والتطور السريع للتهديدات الحديثة هنا يأتي دور الذكاء الاصطناعي الذي يوفر إمكانيات غير محدودة في تحسين كفاءة الدفاعات السيبرانية، فالذكاء الاصطناعي قادر على تحليل كميات هائلة من البيانات بسرعة ودقة غير مسبوقتين، مما يمكنه من التعرف على التهديدات المحتملة في وقت قياسي، بل وحتى التنبؤ بها قبل وقوعها.

علاوة على ذلك، يمكن للذكاء الاصطناعي أن يسهم في تطوير أنظمة حماية ذاتية التعلم قادرة على التكيف مع التهديدات الجديدة بشكل مستمر هذه الأنظمة تعتمد على تحليل الأنماط واكتشاف السلوكيات غير الطبيعية، مما يسمح باتخاذ إجراءات استباقية لمنع الهجمات السيبرانية قبل أن تتسبب في أضرار كبيرة بالإضافة إلى ذلك، يمكن للذكاء الاصطناعي أن يسهم في تعزيز الوعي الأمني لدى المستخدمين من خلال تطوير أنظمة تعليمية ذكية تتيح للفرد التعرف على التهديدات السيبرانية وكيفية التعامل معها بفاعلية.

في النهاية، يمكن القول أن الذكاء الاصطناعي يمثل سلاحًا ذا حدين في العالم السيبراني. فبينما يوفر حلولًا فعالة لمواجهة التهديدات السيبرانية المتزايدة، يتطلب أيضا استخدامه بحذر ومسؤولية لضمان أن يكون أداة لحماية المجتمعات وتعزيز الأمان السيبراني، وليس مصدرًا جديدًا للتهديدات.

المصادر والهوامش

1. Martin Ford, the Age of Artificial Intelligence: And the Fourth Industrial Revolution, Basic Books, 2021, 32-47.
2. Artificial Intelligence and Cybersecurity: The Future is now, https://www.eccu.edu/blog/cybersecurity/artificial-intelligence-the-future-of-cybersecurity/.

٣. مارفن مينسكي: (Marvin Minsky)عالمًا أمريكيًا رائدًا في مجال الذكاء الاصطناعي وعلوم الحاسوب. وُلد في ٩ اب ١٩٢٧، وتوفي في ٢٤ كانون الثاني ٢٠١٦ . يعتبر مينسكي أحد المؤسسين الرئيسيين لمجال الذكاء الاصطناعي، حيث شارك في تأسيس مختبر الذكاء الاصطناعي في معهد ماساتشوستس للتكنولوجيا (MIT) في عام ١٩٥٩ . قام مينسكي بتطوير العديد من النظريات والأبحاث التي أسست لفهم كيفية عمل العقل البشري من خلال محاكاة الحوسبة، كتب مينسكي العديد من الكتب والمقالات المؤثرة، من أشهرها كتاب (The Society of Mind)(مجتمع العقل) الذي يعرض فيه نظريته حول كيفية عمل العقل البشري كنظام من وحدات صغيرة بسيطة تعمل معًا . https://www.britannica.com/biography/Marvin-Lee-Minsky

4. Artificial intelligence,What is a Artificial intelligence?, https://www.business-standard.com/about/what-is-artificial-intelligence

٥. الان تورينج (Alan Turing) عالم رياضيات، وعالم حاسوب، وعالم منطقيات بريطاني، ويُعتبر أحد الآباء المؤسسين لعلم الحاسوب الحديث. وُلد في ٢٣ يونيو ١٩١٢ وتوفي في ٧ يونيو ١٩٥٤ . قدم تورينج مساهمات هامة في العديد من المجالات، وكان أبرزها تطوير مفهوم "آلة تورينج" التي تعتبر نموذجًا نظريًا للحاسوب من بين إنجازاته البارزة، دوره الكبير في فك شيفرة "إنيجما" الألمانية خلال الحرب العالمية الثانية، وهو ما يُعتقد أنه ساهم بشكل كبير في اختصار مدة الحرب وإنقاذ العديد من الأرواح. https://www.britannica.com/biography/Alan-Turing https://www.biography.com/scientists/alan-turing

6. Rockwell Anyoha, The History of Artificial Intelligence, AUGUST 28, 2017, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.

7. B. Geluvaraj, P. M. Satwik & T. A. Ashok Kumar, The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine

Learning, and Deep Learning in Cyberspace, https://link.springer.com/chapter/10.1007/978-981-10-8681-6_67.
8. About the Cyber World, https://ictconnection.moe.edu.sg/cyber-wellness/cyber-wellness-101/about-the-cyber-world.
9. https://www.igi-global.com/dictionary/cybersecurity-new-challenge-information-society/6619
10. Myriam Dunn Cavelty and Florian J. Egloff, The Politics of Cybersecurity: 37 Balancing Different Roles of the State, Center for Security Studies, ETH Zürich, St Antony's International Review 15 no.1 (2019),P27.
11. Cybersecurity and Human Rights, https://www.publicknowledge.org/cybersecurity-and-human-rights/

12. UNDERSTANDING THE
CONCEPT OF CYBER SECURITY
Policy Competition & Economic Analysis Department, P7.
13. https://builtin.com/cybersecurity.
14. What is Cyber Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

15. Maarten Gehem, Artur Usanov, Erik Frinking, Michel Rademaker, ASSESSING CYBER SECURITY A META-ANALYSIS OF THREATS, TRENDS, AND RESPONSES TO CYBER ATTACKS, The Hague Centre for Strategic Studies,2015,p10.
16. CYBERSECURITY, https://www.imperva.com/learn/application-security/cyber-security/.

17. CYBERSECURITY, https://www.imperva.com/learn/application-security/cyber-security/.OP.Cit.
18. CYBER SECURITYINTRODUCTION TO CYBERSECURITY, JUN 16 2021, https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.
19. The Important Role of Artificial Intelligence in Cybersecurity, https://www.plainconcepts.com/artificial-intelligence-cybersecurity/.
20. Artificial Intelligence and Cybersecurity: The Future is Now, https://www.eccu.edu/blog/cybersecurity/artificial-intelligence-the-future-of-cybersecurity/