مجلة الحكمة للدراسات والأبحاث المجلد 04 العدد 06 (20) 2024/11/15
ISSN print/ 2769-1926 ISSN online/ 2769-1934

الأمن السيبراني في ظل الذكاء الاصطناعي

منصور أحلام *
جامعة الجزائر 03
mansahl2015@gmail.com

تاريخ الارسال : 2024/10/03 تاريخ القبول: 2024/11/05

ملخص:

تهدف هذه الدراسة إلى التعرف على دور الذكاء الاصطناعي باعتباره أحد المدخلات الحديثة في المجال التقني في تعزيز الأمن السيبراني، عبر التعرف على مفهوم الذكاء الاصطناعي وتطبيقاته المختلفة والمتنوعة والهامة في تعزيز الأمن السيبراني، من خلال تحسين كفاءة أمن المعلومات فهو يمكن من تقليل الأخطاء وتعزيز اتخاذ قرارات أمنية مستنيرة بناء على تحليل كميات ضخمة من البيانات بسرعة ودقة، وبناء اعلى الأنماط والتنبؤات، كما يسمح الذكاء الاصطناعي بأتمتة العمليات الأمنية الالكترونية المتكررة مما يحرر الموظفين للتركيز على مهام أكثر استراتيجية، ويوفر أدوات لرصد التهديدات الأمنية وتحليل بيانات الشبكات للكشف عن الأنشطة المشبوهة مما يساعد على حماية المعلومات الحساسة للإدارة.

الكلمات المفتاحية : الأمن السيبراني، الذكاء الاصطناعي، التهديدات الالكترونية.

مقدمة:

مع تعميم الرقمنة، وحركة انتقال المعلومات، واعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات، وانخراط جميع القطاعات، العلمية، والاجتماعية، والأكاديمية، والاقتصادية والحكومية في مجتمع المعلومات، والاتصال الشبكي بين الأنظمة، وبروز الوسائط المتعددة واستعمالها بشكل مكثف، نجد أنفسنا أمام حاجة ملحة إلى الأمن في الفضاء الرقمي. ذلك أن الأمن هو شرط أساسي من شروط تحقق الثقة .وتعتبر هذه الأخيرة، الهدف الأول الذي تسعى إليه الحكومات، التي تسعى إلى الإفادة من إمكانات تكنولوجيا المعلومات والاتصالات في دعم التنمية والتطور والتجارة والاقتصاد. وتكفي مراجعة

* منصور أحلام، mansahl2015@gmail.com

النصوص القانونية التي أقرت، سواء في دول الاتحاد الأوروبي، أو الولايات المتحدة الأمريكية، وغيرها، لملاحظة تشديدها على دعم الثقة في تكنولوجيا المعلومات والاتصالات، تحقيقا لازدهار التجارة الالكترونية، والمبادلات الاقتصادية. (جبور و بربر، 2018، صفحة 01)

مع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة، أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر، أصبح النظر إلى أمن تلك البيانات والمعلومات مهما للغاية عبر أمن المعلومات الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها بالسرقة أو التعديل، وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية، وإتباع المعايير وإجراءات الاتصالات المناسبة؛ لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين، ولضمان أصالة وصحة تلك الاتصالات (https://www.specto.com, 2024, p. 02).

فقد ظهر الذكاء الاصطناعي كمحاولة لمحاكاة الذكاء الفطري للبشر إذ زود الانسان الالة بعدد من التقنيات والبرامج وقواعد البيانات الضخمة والخوارزميات المعقدة التي تسمح لها بتحليل البيانات وتحويلها الى معلومات وإختيار الأنسب منها لحل المشكلة التي تواجهها أي اتخاذ القرار الملائم. ويعود أصل تسمية الذكاء الاصطناعي الى عالم الحاسوب الأمريكي **جون ماكرثي John McCarthy** (1927-2011) الذي طرحه اول مرة عام **1956** أين تم انعقاد مؤتمر علمي في كلية دارثموث **Dartmouth** الامريكية لدراسة إمكانية تصميم الة ذكية بإمكانها محاكاة العقل البشر.

وقد شهدت السنوات الأخيرة تجسيدا لفكرة الذكاء الاصطناعي من خلال عدد كبير من البرامج كبرنامج **ChatGPT** "**المُحوّل التوليديّ المُدرَّب مُسبقًا للدردشة**" و**Amazon Alexa** و**WiziShop** وغيرها العديد من أدوات الذكاء الاصطناعي ليصبح العالم أمام حقيقة الالة الذكية التي تتمتع بمزايا التحليل والتصنيف والمقارنة والاختيار وحتى إبداء بعض المشاعر كالتعاطف وهي الأفعال العقلية والخصائص النفسية التي يتميز بها الانسان. إن الإدارة الرقمية بدورها واكبت هذا التطور الكبير والمتسارع لتحقق أفضل استفادة في سبيل إنجاز وظائف المؤسسة وتحقيق التميز في ظل بيئة ديناميكية سريعة التغير. ومن هنا يمكننا طرح الإشكالية التالية: **ماذا نقصد بالأمن السيبراني؟** و**كيف يساهم الذكاء الاصطناعي في تعزيز الأمن السيبراني؟**

ولتوضيح مضامين الإشكالية يمكن طرح الأسئلة التالية:

- ماهو مفهموم الأمن السيبراني وماهي أبرز التهديدات الالكترونية؟
- فيم تتمثل أنظمة تأمين وحماية المعلومات الالكترونية؟
- ماهو مفهوم الذكاء الاصطناعي؟ وكيف يساهم في تعزيز الأمن السيبراني؟

وبناء عن الأسئلة المطروحة قمنا بصياغة الفرضيات التالية:

الفرضية الأولى: يمثل الامن السيبراني مختلف الأنظمة والبرامج المستعملة في حماية المعلومات.

الفرضية الثانية: تتمثل أنظمة حماية المعلومات الالكترونية في برامج مضادة للجرائم المعلوماتية.

الفرضية الثالثة: يساهم الذكاء الاصطناعي في تعزيز الأمن السيبراني.

وقد حرصنا في دراستنا هذه على تحقيق مجموعة من الأهداف تتمثل في:

- التعرف على مفهوم الأمن السيبراني وتحديد مختلف التهديدات الالكترونية؛
- تحديد مختلف نظم تأمين وحماية المعلومات الالكترونية والتطبيقات المختلفة للذكاء الاصطناعي في تعزيزها؛
- إبراز أهمية الذكاء الاصطناعي في بناء استراتيجية متكاملة لتحقيق أمن المعلومات الالكترونية.

المنهج المتبع:

بغرض دراسة الموضوع ونظرا لطبيعته ولأجل الوصول الى الأهداف المسطرة ارتأينا استعمال المنهج الوصفي في دراسة المفاهيم المتعلقة بالذكاء الاصطناعي وأمن المعلومات الالكترونية؛ وايضاح دور الذكاء الاصطناعي في تعزيز الأمن السيبراني والتحديات المختلفة التي تواجهه.

أولا: أمن المعلومات الالكترونية

1**–مفهوم أمن المعلومات الالكترونية:** يعرف أمن المعلومات على أنه" مجموعة من التدابير والإجراءات التي تتخذها المؤسسة بهدف حماية أصولها الإلكترونية المتمثلة في المعلومات من كل استخدام غير مرخص كالتخريب والتغيير والسرقة والتلف والضياع والاستخدام غير المرخص وغير القانوني وذلك بالاعتماد على وسائل تقنية وأدوات تضمن لها الوصول إلى الحماية" (حديد و كريبط، 2014، صفحة 198). كما تم تعريفه على أنه " القدرة على التفاعل وحماية المعلومات وقواعد البيانات من العبث والتدمير والكشف عن أي مخاطر تتعرض لها ومحاولة معالجتها بالسرعة والدقة الممكنتين ويعد من السياسات الأمنية التي يجب على المؤسسة أن تتبناها من خلال أفضل الممارسات الأمنية وأحدث التقنيات للحفاظ عليها من

الاختراق غير المباشر من قبل غير المخولين ومهاجمة البيانات والمعلومات المخزنة في الحاسوب لإلحاق الضرر بالمؤسسة" (جبوري، 2011، صفحة 76).

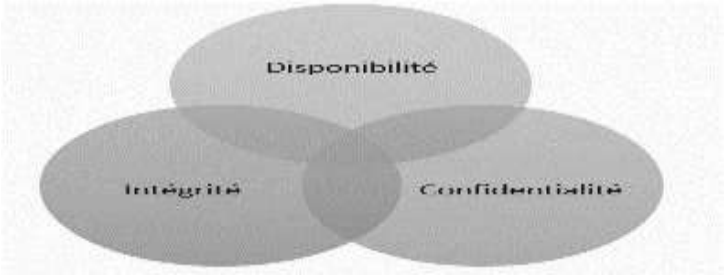
وهناك من عرف أمن المعلومات من خلال زاويتين من وجهة النظر إحداهما أكاديمية وأخرى تقنية حيث أن: "أمن المعلومات من زاوية أكاديمية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)" (www.m5zn.com/newuploads).ويمكننا القول أن أمن المعلومات هو "مجموعة من الاحتياطات التي تتخذها المؤسسة لحماية أنظمة معلوماتها عبر مجموعة من الوسائل الفيزيائية كتأمين أجهزة المؤسسة المادية من التلف أو المنطقية والمتمثلة في مجموعة من برامج الحماية التي تجنب المؤسسة تعرض معلوماتها للسرقة أو القرصنة أو تغيير المحتوى ولكي يكون أمن المعلومات فعالا يجب أن تتوفر فيه ثلاثة عناصر أساسية، تتمثل في(Dorigny, 2024) :

1–الإتاحة (Disponibilité): هو ضمان إمكانية الوصول إلى البيانات (يمكن قراءتها والبحث فيها).

2–النزاهة (Intégrité): تضمن النزاهة أن المعلومات لا تغير جوهرها أو شكلها أثناء النقل أو المعالجة أو التخزين. بشكل عام، هو ضمان أن المعلومات "صحيحة" (بمعنى "غير مشوهة" من قبل طرف ثالث). لذلك نسعى إلى التأكد من أن المعلومات واضحة في دقتها وكذلك في مجملها.

3–السرية (Confidentialité): هي حقيقة أن المعلومات يتم قراءتها والوصول إليها فقط من قبل أولئك الذين لديهم حق الوصول. والشكل التالي يوضح هذه العناصر:

الشكل رقم (01): عناصر أمن المعلومات



Source : Mickael Dorigny, **Qu'est ce que la sécurité de l'information**, 21/10/2024, sur le site : https://www.information-security.fr

حيث تكون الأنواع الكبيرة من البيانات عند خزنها بشكل الكتروني عرضة لأنواع جديدة من التهديدات أكثر مما لو كانت موجودة بشكل يدوي، فالاتصالات المتقدمة وبرمجيات الحاسوب قد وسعت من هذا التعرض للخطر. ووفقا لذلك يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات بالاتي (جبوري، 2011، صفحة 76):

- **الأخطار البشرية:** وهي التي يمكن أن تحدث خلال تصميم التجهيزات أو نظم المعلومات أو أثناء عمليات البرمجة أو الاختبار أو التجميع للبيانات وأثناء إدخالها إلى النظام
- **الأخطار البيئية:** تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق فضلا عن المشاكل القائمة عن تعطل أنظمة التكييف والتبريد وغيرها.
- **الجرائم المحوسبة:** تمثل تحدياً كبيراً لإدارة نظم المعلومات لما تسببه من خسارة كبيرة من خلال الاستخدام والوصول، التعديل، التدمير غير المفوض للماديات والبرمجيات أو البيانات والموارد الشبكية، فضلا عن النشر والنسخ غير المفوض للمعلومات وحرمان المستفيد النهائي من الوصول إلى مادياته وبرمجياته أو بياناته، ومنها:

✓ **فيروسات الحاسوب: وهي** عبارة عن برمجيات مستقلة تقوم بتحميل نفسها ضمن برمجيات الحاسوب ونسخ نفسها بشكل متكرر وبدون معرفة المستفيد.

✓ **القرصنة:** أي اختراق الأجهزة بدون عناء وبمجرد إنزال إحدى برامج القرصنة .

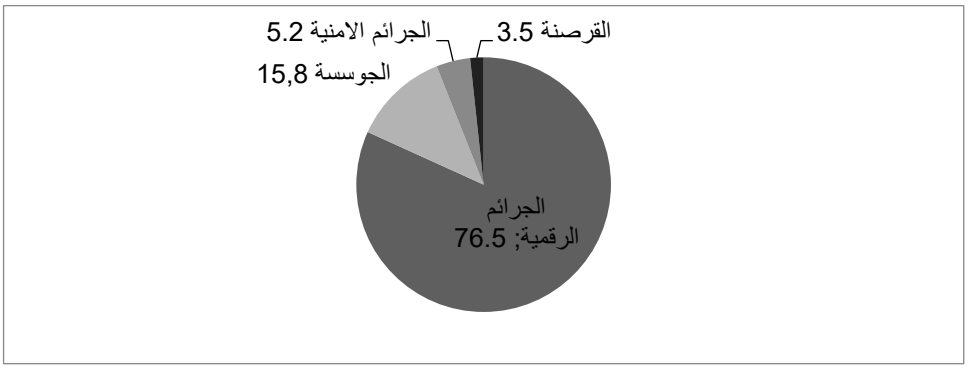
✓ **جرائم الفضاء الرقمي:** تتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات الفيديو) وبطاقات الهوية الالكترونية، قواعد البيانات الشخصية، وسائل رقابة واعتراض

البريد والاتصالات إذ يمكن استرجاع كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الخاصة والحكومية، ونقل المعلومات المؤتمتة في قاعدة البيانات عبر البلد في ثوان وبتكاليف منخفضة نسبيا إذ أن ذلك يكشف إلى أي مدى يمكن أن يكون التهديد للفضاء الرقمي.

- **مشاكل جودة النظام:** فضلا عن الكوارث والفيروسات والخروقات الأمنية لأنظمة المعلومات هناك أيضا تخلف البرمجيات والبيانات الناقصة والتي تسبب تهديدا دائما لنظم المعلومات.

الشكل التالي يوضح أنواع الجرائم المحوسبة التي تمت على مستوى العالم شهر جانفي 2024

الشكل رقم (02): أنواع الجرائم المحوسبة (جانفي2024)



Source :https ://www.hackmageddon.com/

نلاحظ من خلال الشكل السابق أن أكثر نوع من الجرائم المحوسبة الذي تم في شهر جانفي 2024 هو الجرائم الرقمية بنسبة 76.5% تليها الجرائم المتعلقة بالجوسسة بنسبة 15.8% ثم الجرائم الأمنية بنسبة 5.2% وأخيرا جرائم القرصنة بنسبة 3.5%.

2- الأشكال المختلفة للاعتداءات الإلكترونية تأخذ الاعتداءات الالكترونية التي يمكن أن تصيب أجهزة، برامج وشبكات المؤسسة، أشكالا مختلفة وأساليب متعددة وهي في تطور مستمر وتستغل أي ثغرة موجودة في الأنظمة من أجل اختراقها أو إلحاق الضرر بها، وتعد شبكة الإنترنت الوسيلة المفضلة للمخترقين لارتكاب هذه الجرائم، ومن هذه الاعتداءات نذكر ما يلي (حديد و كريبط، 2014، الصفحات 191-193):

2-1-الاعتداء باستعمال البرمجيات الخبيثة: البرمجيات الخبيثة هي عبارة عن برامج أو أجزاء برامج خبيثة، تعمل بعيداً دون مساعدة مستعمل الحاسب، موجهة إلى عرقلة، تغيير أو تخريب أي جزء من مكونات الحاسب .وهي تنقسم إلى البرمجيات غير المتكاثرة كحصان طروادة والبرمجيات المتكاثرة ذاتياً (كالفيروسات والدّيدان).

2-2-الاعتداء باستعمال برامج الجوسسة: هي برامج تعمل خفية عن مستعمل الجهاز، وتقوم بجمع المعلومات عن النظام وإرسالها إلى الخارج من خلال شبكة الإنترنت.

2-3-الاعتداء باستعمال أسلوب اعتراض البيانات: تسمح هذه التقنية باستراق السمع للبيانات التي تنتقل في شبكة المؤسسة، من خلال اعتراض وتحليل البيانات المتنقلة بداخل الشبكة بغرض الاستفادة منها بطريقة غير شرعية.

2-4- الاعتداء باستعمال أسلوب منع تقديم الخدمة: أي الإضرار المادي بالخادم لمنع تقديم الخدمة .

2-5-الاعتداء باستعمال البريد غير المرغوب فيه: إساءة استخدام نظام الرَّسائل الالكترونية بإرسال كم هائل من الرَّسائل العشوائية.

2-6-الاعتداء باستعمال أسلوب انتحال عنوانIP : تعني هذه التقنية تعويض عنوانIP للمرسل بعنوان حاسب آخر، مما يسمح للمعتدي بالقيام بالاعتداء والتخفي وراء عناوين أخرى وبالتالي إخفاء كل أثر يؤدي إلى التعرُّف عليه .

2-7- الاعتداء باستعمال أسلوب انتحال نظام أسماء النطاقاتDNS : توجيه مستخدمي الإنترنت أوتوماتكياً إلى المواقع المحتوية على "برامج الجوسسة" أو المواقع التي تحاكي في تصميمها المواقع التجارية والبنكية الحقيقية والتي تنجز من قبل المعتدين بغرض الإيقاع بهم .ويتم هذا التوجيه من خلال الرسائل الالكترونية غير المرغوب فيها.

2-8- الاعتداء باستعمال أسلوب الاصطياد الالكتروني: ويقصد به سرقة البيانات الشخصية السّرية والحسّاسة عن طريق رسائل البريد الإلكتروني لغرض انتحال الشخصية.

3-التهديدات والمخاطر الالكترونية أما فيما يخص أهم المخاطر والتهديدات التي تتعرض لها مواقع معلومات المؤسسة على شبكة الانترنت فتتمثل فيما يلي (غنيم، 2009، الصفحات 270-273):

3-1-تغيير المحتوى: لهجوم على موقع المؤسسة على شبكة الانترنت واختراقه وتغيير محتوياته وذلك بهدف الإساءة للمؤسسة أو إساءة العلاقة بينها وبين زبائنها.

3-2-إستخدام موقع المؤسسة على شبكة الانترنت لتنفيذ بعض الأعمال غير المشروعة: كتنفيذ بعض الجرائم، إخفاء بعض المسروقات أو بعض الملفات. كما يمكن سرقة المعلومات الخاصة بالمشتركين مثل سرقة أرقام حسابات الزبائن أو أرقام الائتمان، فضلا عن سرقة معلومات الفواتير.

3-3-التعرف على النظم والسياسات الداخلية للمؤسسة: الحصول على بعض المعلومات عن السياسات الداخلية لها واستغلالها استغلالا سيئا، مما يترتب عنه نتائج سلبية للمؤسسة.

3-4-توقف موقع المؤسسة عن العمل: ويتم ذلك من خلال قيام المهاجمين بشغل الموقع الرئيسي للمؤسسة بكثير من المعاملات والاستفسارات والرسائل.

3-5-تخريب موقع المؤسسة: من خلال دخول المهاجمين على البرامج الخاصة بإدارة موقع المؤسسة وتغيير بعض المؤشرات الخاصة به، مما يترتب عليه حدوث أخطاء أو حتى توقف الموقع كليا عن العمل.

ثانيا: مدخل للذكاء الاصطناعي

1-مفهوم *الذكاء الاصطناعي*

التعريف الأول: الذكاء الاصطناعي هو مجموعة من النظريات والتقنيات التي سمحت بتطوير أنظمة معلوماتية معقدة قادرة على محاكاة الذكاء البشري (Robert, 2024, p. 01)

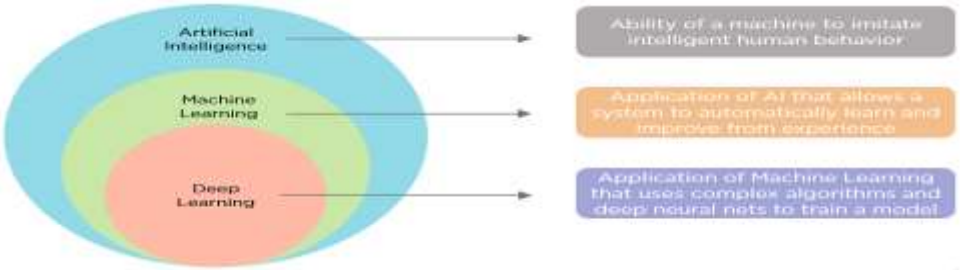
التعريف الثاني: الذكاء الاصطناعي هو محاولة لخق تكنولوجيا جديدة لها علاقة بالسلوك البشري الفريد (Othmani, 2021, p. 14)

يتكون الذكاء الاصطناعي من كلمتين هما: **الذكاء** و**الاصطناعي** ولكل منهما معنى فالذكاء حسب قاموس **Webster**هو: القدرة على فهم الظروف أو الحالات الجديدة والمتغيرة. أي هو القدرة على إدراك وفهم وتعلم الحالات أو الظروف الجديدة، بمعنى اخر أن مفتاح الذكاء هو الإدراك الفهم والتعلم أما كلمة الاصطناعي فترتبط بالفعل يصنع أو يصطنع، وهي تطلق على كل الأشياء التي تنشأ نتيجة النشاط أو الفعل الذي يتم من خلال اصطناع وتشكيل الأشياء تمييزا عن الأشياء الموجودة بالفعل والمولدة بصورة طبيعية دون تدخل الانسان. ومن الجدير بالذكر أن هناك عدة مصطلحات تتداخل وتتشابه مع مصطلح الذكاء الاصطناعي وجب توضيحها وتبيانها وهي كما يلي:

ISSN print/ 2769-1926 ISSN online/ 2769-1934

تعلم الآلة Machine Learning هو فرع من فروع الذكاء الاصطناعي يشير إلى منح الآلات القدرة على التعلم واتخاذ القرار بالاعتماد على نفسها دون الحاجة إلى برمجتها من قبل الإنسان، بحيث يمكنها التعلم من الإجراءات السابقة، وتخزين البيانات للاستفادة منها والتحسين من أدائها في أي عمل مستقبلي .هناك أيضا **التعلم العميق Deep Learning** الذي، الذي تعتمد فكرته على تقليد عمل الخلايا العصبية الموجودة في العقل البشري من خلال ابتكار شبكة عصبية اصطناعية **Neural Artificial Network** تستطيع تحليل كميات ضخمة من البيانات غير المنظمة مثل اللغات المختلفة والصور، وترجمتها عبر تمريرها من خلال الشبكة العصبية للتعرف عليها من خلال عدة مراحل، من تشمل تطبيقات التعلم العميق على سبيل المثال، التعرف على الكلام، والأصوات، والصور .(Othmani, 2021, p. 17) والشكل التالي يوضح العلاقة بين الذكاء الاصطناعي وتعلم الالة والتعلم العميق:

الشكل رقم 01: العلاقة بين الذكاء الاصطناعي وتعلم الالة والتعلم العميق



Source : https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/ai-vs-machine-learning-vs-deep-learning (consulté le: 25/09/2024)

2-أنواع الذكاء الاصطناعي: تختلف أنواع الذكاء الاصطناعي او لنقل مستوياته ومجالاته ويمكن تقسيمها الى ما يلي (محمد و هرموزي، 2024، الصفحات 113-114) :

- **الذكاء الاصطناعي الضيق Artificial Narrow Intelligence (ANI)** وهو مصمم لإكمال إجراءات محددة للغاية غير قادر على التعلم بشكل مستقل؛
- **الذكاء الاصطناعي العام Artificial General Intelligence (AGI)** وهو مصمم للتعلم والتفكير والأداء بمستويات مماثلة للإنسان؛

- **الذكاء الاصطناعي الفائق Artificial Super Intelligence (ASI)** وهو القادر على تجاوز معارف وقدرات البشر؛
- **الذكاء الاصطناعي للألة التفاعلية Artificial intelligence for interactive machine** قادر على الاستجابة للمحفزات الخارجية في الوقت الفعلي غير قادر على بناء الذاكرة أو تخزين معلومات للمستقبل؛
- **نظرية العقل AI** يمكنه استشعار المشاعر البشرية والاستجابة لها بالإضافة الى أداء مهام أجهزة الذاكرة المحدودة؛
- **الذكاء الاصطناعي المدرك لذاته Self-awar artificial intelligence** الذي يمكنه التعرف على مشاعر الاخرين بالإضافة الى الشعور بالذات والذكاء على المستوى البشري وهي المرحلة النهائية للذكاء الاصطناعي.

3–مزايا الذكاء الاصطناعي: يمتلك الذكاء الاصطناعي خصائص ومزايا عديدة قادرة على مساعدة الكثير من القطاعات، نذكر منها (الزهراء و طالب ، 2024، صفحة 361):

- زيادة كفاءة الأعمال على عكس العناصر البشرية يمكن لتقنية الذكاء الاصطناعي العمل على مدار الساعة طوال أيام الأسبوع بدون أن تنخفض معدلات الأداء؛
- اتخاذ قرارات أكثر ذكاء فهو يساعد في اقتراح أفضل مسار للعمل في المستقبل؛
- القدرة على التفكير والإدراك ؛
- القدرة على التعلم والفهم من التجارب والخبارت السابقة؛
- القدرة على اكتساب المعرفة وتطبيقها؛
- القدرة على استخدام التجربة والخطأ لاستكشاف الأمور المختلفة؛
- القدرة على الاستجابة السريعة للمواقف والظروف الجديدة.

ثالثا : دور الذكاء الاصطناعي في تعزيز الأمن السيبراني

يمكن القول أن التهديد السيبراني هو أي نشاط غير قانوني أو ضار يتم تنفيذه عبر الانترنت 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 (دحماني، 2023، الصفحات 602-603).

1-نظم تأمين وحماية المعلومات الالكترونية : قبل الشروع في تأمين وحماية المعلومات على المؤسسة أولا القيام بتقدير لمخاطر، ثم تحديد المخاطر المحتملة من حيث الاحتمالية والشدة وتحديدها كميا وتأهيلها، يحين الوقت لاختيار حلول الوقاية بمقارنة تكلفة الاستخدام والمخاطر التي يتم تغطيتها مع تحديد شامل لوسائل الكشف عن الهجمات والتدخلات في أسرع وقت ممكن. وأخيرا تحديد خطط أمان الكمبيوتر الاحتياطية وكيفية العودة بأسرع ما يمكن إلى الوضع قبل الهجوم (Fernandez, 2024, p. 01).

أما فيما يخص أساليب ونظم تأمين وحماية معلومات المؤسسة من مختلف الأخطار والتهديدات التي ذكرناها سابقا، فيمكن تقسيمها إلى قسمين:

1-1- أساليب الحماية الفيزيائية: تتمثل في اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن (بامفلح، 2018، صفحة 07)

1-2- أساليب الحماية المنطقية: تتمثل أساليب الحماية المنطقية في مختلف الوسائل والبرمجيات التي تهدف إلى حماية النظام والمحافظة على المعلومات التي يحتويها، ويمكن ذكرها كما يلي (حديد و كريبط، 2014، الصفحات 203-204):

1-2-1-التشفير الإلكتروني: يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح تصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها.

1-2-2-التوقيع الإلكتروني: يقصد بالتوقيع الإلكتروني استخدام طريقة أو وسيلة معينة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، ويطلق على هذا التوقيع أيضا البصمة الإلكترونية (غنيم، 2009، صفحة 279).

1-2-3- ضبط الوصول إلى الشبكة وإتاحة مواردها: من الضروري ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحام ولتحقيق ذلك لابد من تخصيص اسم أو رقم تعريف لكل مستخدم للشبكة وكلمة مرور (بامفلح، 2018، صفحة 08) .

1-2-4-جدران المنع: هي مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتشكيل حدود فاصلة بين شبكة المؤسسة الخاصة إنترانت وشبكة الإنترنت يقوم جدار النار بدور المرشح حيث يراقب تدفقات

البيانات التي تمر عبره دخولا وخروجا، ويقوم بتحليلها ومن ثم السماح بمرورها إذا كانت تحقق الشروط، أو منعها في حالة العكس. (غنيم، 2009، صفحة 282)

1-2-5- الشهادات الإلكترونية: أسفرت ممارسات وتطبيقات معاملات التسويق والتجارة الإلكترونية عن ضرورة وجود شهادة من جهة مختصة موثوق فيها تعرف بهيئة الاعتماد، تؤكد وتثبت أن الشخص صاحب المعاملة الالكترونية المعينة هو نفس الشخص المحدد لهذه المعاملة والذي قام بتنفيذها وأن صورته هي نفس الصورة الواردة في وثيقة إثبات الشخصية (غنيم، 2009، صفحة 282).

1-2-6-البرمجيات المضادة للاعتداءات الالكترونية: هي تلك البرمجيات التي تسمح بحماية الحاسب والنظم المعلوماتية ضد الاعتداءات الإلكترونية وتختص بمراقبة وتحليل الملفات وتحطيم البرمجيات الخبيثة (حديد و كريبط، 2014، صفحة 202)

1-2-7- أنظمة كشف الاختراق: إن أنظمة كشف الاختراق فعالة إلى أبعد حد عندما تنصب بشكل صحيح وتراقب بانتظام .ولكن يجب الحفاظ على طريقة عمل هذه الأنظمة بسرية بالغة، ومن الواجب حمايتها بثقة شديدة .تسجل أغلب أنظمة الكشف جميع التعاملات التي تجري داخل موقع الحماية وجميع الطلبات التي تأتي من خارجه. (حديد و كريبط، 2014، صفحة 204).

1-2-8-النسخ الاحتياطي: يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجه، ويتم تحديثها لضمان أقل قدر من الخسائر في حالة فقدان البيانات الأصلية.

1-2-9- **الحوسبة السحابية** هي تكنولوجيا تعتمد على نقل المعالجة ومساحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة وهي جهاز خادم يتم الوصول إليه عن طريق الانترنت (علي، 2024، صفحة 02)

2-دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: يمكن أن يكون للذكاء الاصطناعي دور فعال في حماية المعلومات الالكترونية وتحقيق الأمن السيبراني للمؤسسة عن طريق النقاط التالية : (https://www.europarabct.com)

- **الكشف عن التهديدات** :تظهر فعالية أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي في كشف شفرات البرامج الضارة، وتتمتع هذه الأنظمة بمعدلات أمان تتراوح ما بين (80%-92%) متجاوزة الأنظمة التقليدية بنسبة ما بين (30%-60%) لاعتمادها على التعلم الآلي، ما مكنها من تصنيف رسائل البريد الإلكتروني وفقاً لخطورتها وتحليل شامل لسلوك المستخدم.

- **تعزيز أمن المؤسسات** :يضع الذكاء الاصطناعي نهجاً ديناميكياً بحماية كلمة المرور وأمن حساب المستخدم عبر اللجوء إلى بصمات الوجه والأصابع، خاصة في ظل توسع العمل عن بعد وتزايد مخاطر الهجمات الإلكترونية، ووقوع الحلول التقليدية في خطأ الاكتفاء بالكشف عن الاختراقات التقليدية والشبكات الافتراضية الخاصة"VPN "، وترك أمان نقاط النهاية عرضة للخطر (الكشف عن برامج الفدية وتشفيرها قبل الوصول للمستخدم).
- **تخفيف حدة التهديدات** :يعمل الذكاء الاصطناعي على إنشاء استجابات مبكرة للتهديدات السيبرانية المتوافقة، مع حركة مرور شبكة الإنترنت واتصالات البريد الإلكتروني، لذا يتم إطلاق تدابير استجابة استباقية تلقائياً، وحظر حركة المرور الضارة وعزل الملفات المهددة لأمن المؤسسات والأفراد.
- **تقييم الثغرات الأمنية** :الذكاء الاصطناعي لديه قدرة على تحديد أولويات التهديدات، ومدى خطورة كل ثغرة وتأثيرها، الأمر الذي يسهل على فريق الأمان من تركيز جهوده لمعالجة المخاطر الأشد والأكثر ضرراً.
- **تبسيط العمليات الأمنية** :رغم ارتكاز الذكاء الاصطناعي على خوارزميات التعلم الآلي المتقدمة لأتمتة العمليات الأمنية، إلا أن معالجتها تتم بشكل مبسط لتحديد التهديدات عالية الخطورة عبر التحليل، لتعزيز القدرات الأمنية للدول والمؤسسات بشأن مواجهة أي أنشطة احتيالية.
- **التحليلات التنبؤية** :ساعد الذكاء الاصطناعي على التنبؤ بالمخاطر، بتقديم قوائم دقيقة لأصول تكنولوجيا المعلومات، التي تتضمن بيانات الأجهزة والمستخدمين والتطبيقات والأماكن الأكثر عرضة للهجمات الإلكترونية، ما يحقق رؤية شاملة للوضع الأمني للمؤسسة، ويحسن ظروف البحث الاستباقي عن هذه الهجمات.

3-تحديات أمن المعلومات الالكترونية في ظل استخدام الذكاء الاصطناعي: قد يظن المتابع في مجال الذكاء الاصطناعي أن هذه التقنية المتطورة بإمكانها أن تشكل جدارا منيعا لحماية أمن المعلومات الالكترونية إلا أن الواقع يثبت أن التقدم في الذكاء الاصطناعي قد يشكل تهديدا لأمن المعلومات الالكترونية ويمكننا توضيح ذلك من خلال ما يلي:

3-1التزييف العميق: في هذا النوع المحدد من المعلومات المضللة ومقاطع الفيديو العميقة التي تم إنشاؤها بواسطة الذكاء الاصطناعي أو يمكن استخدام التسجيلات الصوتية لنشر معلومات الكاذبة

3-2-الإعلانات المستهدفة: الاستهداف الدقيق القائم على الذكاء الاصطناعي يمكن استخدام الإعلانات المخصصة للتلاعب بالآراء.

3-3-مخاوف خصوصية البيانات: المعالجة الآلية قد تخلق سبلا لتسرب البيانات الشخصية.

3-4-التلاعب الخوارزمي بوسائل التواصل الاجتماعي: تستطيع خوارزميات الذكاء الاصطناعي الموجودة على منصات التواصل الاجتماعي القيام بالتلاعب بتضخيم سياسة معينة أو قمع الآخرين والتأثير على الرأي العام.

3-5- **التضليل الآلي:** يمكن لخوارزميات الذكاء الاصطناعي توليد ونشر كميات كبيرة من المعلومات المضللة.

خاتمة:

اعتادت الدول على مدار التاريخ أن تعتمد على العنصر البشري في تحقيق الأمن السيبراني، عبر جمع المعلومات وتشديد الرقابة ومطاردة التهديدات وسد الثغرات، والاستجابة لأي احتمالات بشأن وقوع حوادث سيبرانية، ولكن في العقد الأخير تطور الذكاء الاصطناعي بشكل سريع، محققاً فوائد كبيرة للدفاع السيبراني عبر أتمتة العناصر الأساسية للعمل (استخدام الحاسوب والأجهزة المعتمدة على المعالجات والبرمجيات)، وتحويله إلى عملية مبسطة ومستقلة تعمل على تسريع المعالجة وزيادة حماية الأمن القومي للدول. يعتبر العصر الذي نعيشه حاليا عصر المعرفة والتكنولوجيا بامتياز، إلا أن الاتصال بشبكة الانترنت رغم فوائده الكثيرة يحمل عدة أخطار وتهديدات لسلامة معلومات وموارد المؤسسة، من بينها القرصنة والفيروسات وتغيير المحتوى وغيرها، مما يوجب على المؤسسة اتخاذ مجموعة من التدابير والاحتياطات لضمان أمن معلوماتها على شبكة الانترنت وهنا يبرز الذكاء الاصطناعي كعامل مساعد للمؤسسة يمكنها من تحسين كفاءة أمن المعلومات فهو يمكن من تقليل الأخطاء وتعزيز اتخاذ قرارات أمنية مستنيرة بناء على تحليل كميات ضخمة من البيانات بسرعة ودقة وبناء اعلى الأنماط والتنبؤات، كما يسمح الذكاء الاصطناعي بأتمتة العمليات الأمنية الالكترونية المتكررة مما يحرر الموظفين للتركيز على مهام أكثر استراتيجية، ويوفر أدوات لرصد

ISSN print/ 2769-1926 ISSN online/ 2769-1934

التهديدات الأمنية وتحليل بيانات الشبكات للكشف عن الأنشطة المشبوهة مما يساعد على حماية المعلومات الحساسة للمؤسسة. يمكن الخروج ببعض التوصيات نوجزها كالاتي:

- ✓ الذكاء الاصطناعي يعتبر تكنولوجيا المستقبل القريب لذا وجب على كل المؤسسات التركيز على تكوين العاملين والموظفين على هذه التكنولوجيا؛
- ✓ يساهم الذكاء الاصطناعي بشكل فعال في تعزيز الأمن السيبراني من خلال الكشف عن التهديدات والحد منها سد الثغرات والتحليلات التنبؤية لصد أي هجمات سيبرانية محتملة؛
- ✓ الاهتمام بأمن المعلومات الالكتروني أو الأمن السيبراني ضرورة ترافق العمل المعلوماتي؛
- ✓ رغم المزايا العديدة للذكاء الاصطناعي إلا أنه لابد من رقابة بشرية على هذه التكنولوجيا كي لا تحيد عن أهدافها ولتقليص نسبة الخطأ وتوفير الحماية الكاملة لمستعملي النظام المعلوماتي.

CONCLUSION

Throughout history, countries have become accustomed to relying on the human element to achieve cybersecurity, by collecting information, tightening control, chasing threats, filling gaps, and responding to any possibility of cyber incidents. However, in the last decade, artificial intelligence has developed rapidly, achieving great benefits for cyber defense through automation. Basic elements of work
(Using computers and devices based on processors and software), and transforming it into a simplified and independent process that speeds up processing and increases the protection of the national security of countries. The era we currently live in is considered the era of knowledge and technology par excellence. However, Internet connection, despite its many benefits, carries several dangers and threats to the safety of the organization's information and resources.

Among them are hacking, viruses, changing content, etc., which requires the institution to take a set of measures and precautions to ensure the security of its information on the Internet. Here, artificial intelligence emerges as an auxiliary factor for the institution that enables it to improve the efficiency of information security. It enables it to reduce errors and enhance the making of informed security decisions based on quantitative analysis. Huge data quickly and accurately and build the highest patterns and predictions,

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Artificial intelligence also allows the automation of repetitive electronic security operations, freeing employees to focus on more strategic tasks, and provides tools to monitor security threats and analyze network data to detect suspicious activities, which helps protect the organization's sensitive information. Some recommendations can be made, which we can summarize as follows:

- ✓ Artificial intelligence is considered a technology of the near future, so all institutions must focus on training workers and employees on this technology;
- ✓ Artificial intelligence effectively contributes to enhancing cybersecurity by detecting and reducing threats, filling gaps, and predictive analyzes to repel any potential cyberattacks;
- ✓ Interest in electronic information security or cybersecurity is a necessity that accompanies information work;
- ✓ Despite the many advantages of artificial intelligence, there must be human supervision over this technology so that it does not deviate from its goals, reduces the error rate, and provides complete protection for users of the information system.

قائمة المراجع

1-بامفلح, ف .(2018) .حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى. السعودية.

2-جبور, م & .,بربر, ع .(2018) .أمن الشبكات والانترنت .الملتقى العلمي حول الانترنت، مصر.

3-جبوري, ن .(2011) .حماية أنظمة المعلومات، مجلة تكريت للعلوم الاقتصادية والإدارية،المجلد 07 العدد 21، العراق.

4-حديد, ن & .,كريبط, ح .(2014) .أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة . مجلة المؤسسة، الجزائر.

5-حسام حسن. (2024). تاريخ الذكاء الاصطناعي. تم الاسترداد من http://www.noor-book.com

6-دحماني, م .(2023) .الذكاء الاصطناعي كالية لتعزيز الأمن السيبراني .603-602 ,*07 ,(02)* .مجلة الفكر القانوني والسياسي.

7-دعاء خضر. (05 03, 2017). *بين الثقافة والهوية*. تم الاسترداد من ..academia.adu

8-رابح أوكيل. (بلا تاريخ). التغليف المتميز للمنتج وتأثيره على قرار الشراء.(دراسة مقارنة بين مؤسسات المشروبات الغازية: كوكاكولا، بيبسي، حمود بوعلام. *أطروحة دكتوراة*. كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أمحمد بوقرة، بومرداس، الجزائر:.

09-رويشد الزهراء، و أحمد نور الدين طالب . (2024). سبل تحقيق التميز المؤسسي من خلال تطبيق تقنيات الذكاء الاصطناعي. المجلد 07(العدد 01)، مجلة أبحاث اقتصادية ، الجزائر.

10-غنيم, أ .(2009) .التسويق والتجارة الالكترونية .*الطبعة الأولى* .المكتبة العصرية، مصر.

11-عمر بوزيد محمد، و أحلام هرموزي. (2024). استراتيجيات الذكاء الاصطناعي في تحقيق التنمية المستدامة. *المجلد1(العدد2)*، مجلة الجغرافيا الاقتصادية، الجزائر.

12-علي, ع .(2024) .الحوسبة السحابية. البنك المركزي العراقي، دائرة تقنية المعلومات والاتصالات، العراق.

13-نرمين مجدي. (2020). الذكاء الاصطناعي وتعلم الالة.البنك العربي. الامارات العربية المتحدة.

Bibliographie :

01-Dorigny, M. (2024). Qu'est ce que la sécurité de l'information.

02-Fernandez, A. (2024). La sécurité informatique.

03-Othmani, I. (2021). Les défis de l'intégration de l'intelligence artificielle en entreprise: France et Canada. Canada: mémoire préseté en vue de l'optention du grade de maitrise és sciences en gestion.

04-Robert, J. (2024, 09 04). *Intelligence artificielle.* Consulté le 2024, sur https://datasciencetest.com: http:/datascientest.com

05-www.m5zn.com/newuploads. (s.d.).

06-https://www.europarabct.com. (s.d.).

مجلة الحكمة للدراسات والأبحاث المجلد 04 العدد 06 (20) 2024/11/15
ISSN print/ 2769-1926 ISSN online/ 2769-1934

Cybersecurity in light of artificial intelligence

Mansour Ahlem [1]
[1] **University Algiers 03**
mansahl2015@gmail.com

Abstract:

This study aims to identify the role of artificial intelligence in the technical field in enhancing cybersecurity, by identifying the concept of artificial intelligence and its important applications in enhancing cybersecurity, by improving the efficiency of information security, as it enables reducing errors and enhancing decision-making. Informed security based on analyzing huge amounts of data quickly and accurately Building the highest patterns and predictions.

Artificial intelligence also allows for the automation of repetitive electronic security operations, which frees employees to focus on more strategic tasks, and provides tools for monitoring security threats and analyzing network data to detect suspicious activities, which helps protect sensitive information for management.

Keywords: cybersecurity, artificial intelligence, electronic threats.