

## دور الذكاء الاصطناعي في تحقيق الأمن السيبراني

### *The role of artificial intelligence in the achievement of cybersecurity*

بوقريط عمر

bougrit.omar

السبتي آسيا\*

sebti.assia

مخبر الدراسات القانونية والتطبيقية

*Laboratory of Legal and Applied Studies*

جامعة الإخوة منتوري قسنطينة 1 - الجزائر-

University of Mentouri Constantine1 -Algeria-

bougrit.omar@gmail.com

sebti.assia@doc.umc.edu.dz

تاريخ الاستلام

Submission date

10/10/2024

تاريخ القبول للنشر

Acceptance date

25/12/2024

تاريخ النشر

Publication date

31/12/2024

#### ملخص:

إن الذكاء الاصطناعي أصبح اليوم يستخدم في جميع جوانب حياتنا اليومية كالاقتصادية والصناعية والتقنية والتعليمية، وانطلاقا من ذلك، يهدف بحثنا هذا إلى توضيح أهمية الذكاء الاصطناعي في تعزيز الأمن السيبراني وحماية البيانات والمعلومات الخاصة بمستخدمي الانترنت من الانتهاك والاختراق.

ويهدف هذا البحث أيضا إلى عرض المفاهيم الأساسية للذكاء الاصطناعي وتطبيقاته في ظل الفضاء الرقمي ثم الانتقال إلى أهميته في تحقيق الأمن السيبراني وحماية خصوصيات الأفراد في مختلف المجالات.

**الكلمات المفتاحية:** الذكاء الاصطناعي; الأمن السيبراني; الفضاء الرقمي; الاختراق.

#### Abstract:

Artificial intelligence is now used in all aspects of our daily lives, such as economic, industrial, technical, and educational. Based on this, this research aims to clarify the importance of artificial intelligence in enhancing cybersecurity and protecting Internet users' data and information from violation and hacking.

This research also aims to present the main concepts of artificial intelligence and its applications in the digital space and then move on to its importance in achieving cybersecurity and protecting the privacy of individuals in various fields.

\* المؤلف المراسل

**key words:** artificial intelligence ; cyber security ; digital space ; hacking.

#### مقدمة:

يعد الذكاء الاصطناعي خطوة هامة للتقدم في مستوى حماية البنية التحتية لتكنولوجيا المعلومات؛ فقد أثبتت الأبحاث أن الذكاء الاصطناعي يعزز الحاجز بين الأنظمة الإلكترونية والتهديدات، حيث تبحث الشركات عن طرق لحماية بياناتها وأنظمتها التكنولوجية، وللقيام بذلك يجب عليها إتباع نهج أكثر استباقية للتغلب على التهديدات، وبذلك أثبت الذكاء الاصطناعي قدراته.

إن الذكاء الاصطناعي هو مجال من مجالات علوم الحاسوب يهدف إلى تطوير وإدارة تكنولوجيا قادرة على التعلم واتخاذ قرارات بشكل مستقل وتنفيذ الأعمال نيابة عن الإنسان، وفي مجال الأمن السيبراني يعتبر الذكاء الاصطناعي سلاحا ذو حدين، لأسباب أمنية حيث يمكن أن يساعد في حماية المرافق، ولكن يمكن أيضًا إساءة استخدامه من قبل المجرمين لشن هجمات ضارة عن بعد.

إذن فالعالم الرقمي أصبح ساحة معركة دائمة التغير. وأصبحت التهديدات الإلكترونية مؤخرًا أكثر انتشارًا من أي وقت مضى، حيث يطوّر قراصنة الإنترنت مهاراتهم الإجرامية باستمرار، ويستغلون نقاط الضعف في الأنظمة، فيشتون هجمات متطورة، ويتجاوزون الإجراءات الأمنية التقليدية إلى درجة أن الحكومات والدول بأسرها تتعرض لبياناتها إلى القرصنة والسرقة.

في الآن ذاته، يستمر الذكاء الاصطناعي في تغيير وتثوير عدد لا يحصى من الصناعات والمجالات تحقيقًا للأمن السيبراني وبينما نستمر في التكيف مع الطابع الرقمي المتنامي لعصرنا هذا، يغدو من الأهمية أن نفهم كيف يمكن للذكاء الاصطناعي تعزيز جهود الأمن السيبراني، حتى يكون وجودنا وتجاربنا عبر الإنترنت أكثر أمانًا.

في هذه الورقة، سوف نتطرق إلى مفهوم الأمن السيبراني والذكاء الاصطناعي وأهميتهما والمفاهيم المرتبطة بكليهما ثم نتناول بالدراسة دور الذكاء الاصطناعي في تعزيز الأمن السيبراني، مما يقودنا إلى طرح الإشكالية التالية: كيف يساهم الذكاء الاصطناعي في تحقيق الأمن السيبراني؟

#### أهداف البحث:

أولاً - التعرف على أساسيات الذكاء الاصطناعي وشرح مفهوم الذكاء الاصطناعي السيبراني.  
ثانياً - توضيح كيف يستطيع الذكاء الاصطناعي أن يخدم الأمن السيبراني في مواجهة التهديدات التي يتعرض إليها.

ثالثا إعطاء تصور عن مستقبل الذكاء الاصطناعي السيرياني ودوره الكبير المتوقع في صد مثل هذه الهجمات.

### منهجية البحث:

اتبعت هذه الدراسة المنهج الوصفي التحليلي. ويعد هذا المنهج هو الأنسب لتناول مختلف المواضيع الاجتماعية والإنسانية بشكل عام.

### المبحث الأول:

#### مفهوم الذكاء الاصطناعي

إن الالتزام المنهجي الذي يتعين على الباحث أن يتقيد به يدفعه إلى تحديد جملة من المفاهيم الأساسية المؤطرة لنسق الخطاب العلمي المنتج في بحثه، وضمن هذا السياق، سنعرج على المفاهيم الأساسية المشكلة لمفردات بنية موضوع البحث والمتمثلة في الذكاء الإنساني والذكاء الاصطناعي في مطلب أول ثم، نتطرق إلى أنواع وتطبيقات الذكاء الاصطناعي المختلفة وكذلك إلى الفرص التي يقدمها والمخاطر التي يسببها في المطلب الثاني.

#### المطلب الأول: تعريف الذكاء الاصطناعي

لتعريف الذكاء الاصطناعي، ينبغي أولا التطرق لتعريف الذكاء الإنساني.

#### الفرع الأول: الذكاء الإنساني

يعرف على أنه القدرة على التفكير المجرد بالاعتماد على المفاهيم العامة والاستعانة بالرموز اللغوية والعديدية إلى جانب القدرة على التصرف الهادف والتفكير المنطقي، كما يعرف بأنه المهارة في وضع حلول للمشكلات من خلال استخدام الرموز وطرق البحث المختلفة وكذلك القدرة على استغلال الخبرة المكتسبة لاشتقاق معارف جديدة تساهم في حل المشكلات في مجال محدد. وبذلك يعتبر الذكاء الإنساني المحرك الرئيسي للتطور والإبداع لدى الحضارات المختلفة<sup>1</sup>.

إن الخبراء والمختصين في مجال علم نفس الدماغ البشري يرون أن الذكاء يعد مصطلحا شاملا يضم العديد من القدرات العقلية مثل القدرة على التحليل والتخطيط وحل المشكلات وسرعة الذكاء الحسي، كما يشمل التفكير المجرد، جمع وتنسيق الأفكار، تعلم اللغات بسرعة والتعلم بشكل عام، ويشير بعض العلماء أيضا إلى أن الذكاء يتضمن القدرة على الإحساس والتعبير عما يدور في النفوس وكذا القدرة على إبداع وفهم مشاعر الآخرين<sup>2</sup>.

## الفرع الثاني: الذكاء الاصطناعي

يعرف الذكاء الاصطناعي على أنه: علم يشمل طرق تصميم وصنع الأجهزة والبرامج الذكية بهدف إنتاج آلات مستقلة قادرة على أداء المهام المعقدة بطريقة مشابهة للتفكير البشري، ويتم تطوير برامج وتطبيقات الذكاء الاصطناعي من خلال دراسة آلية تفكير العقل البشري وكيفية تعلمه واتخاذ القرارات والعمل على حل المشكلات ثم استخدام النتائج المتحصل عليها كأسس لتطوير الأنظمة الذكية<sup>3</sup>. وعرفه الشرفاوي بأنه فرع من علوم الكمبيوتر يختص بإنشاء وتصميم برامج تحاكي ذكاء الإنسان بهدف تمكين الكمبيوتر من أداء مهام معينة تتطلب التفكير والفهم والاستماع والتحدث والتحرك بطريقة منطقية ومنظمة<sup>4</sup>.

ويعتبر الذكاء الاصطناعي حديثا مقارنة بالحقول العلمية والتطبيقية الأخرى، ولكنه يظل نتاجا لتطور تاريخي في مختلف مجالات الفلسفة والفكر والعلوم الإنسانية والتطبيقية، والهدف المحدد من الذكاء الاصطناعي يتمثل في تطوير أجهزة ونظم الحاسبات، حيث تصبح أكثر ذكاء، والعمل في هذا المجال يتأسس على الأبحاث العلمية التي تغطي مختلف فروع المعرفة مثل علوم الكمبيوتر وعلم النفس واللغويات والرياضيات والهندسة، ويمكن القول بأن التعريف الشامل لمفهوم الذكاء الاصطناعي هو أنه علم وتكنولوجيا تستند إلى مجالات معينة كعلوم الحاسوب والرياضيات والبيولوجيا وعلم النفس واللسانيات والهندسة وذلك بهدف تطوير نظم حاسوبية تستطيع أن تفكر وترى أو تسمع وتمشي وتتحدث وتشعر وبالتالي تتصرف بذكاء، أي أن حقل الذكاء الاصطناعي يشير إلى الجهود المبذولة في تطوير نظم الحوسبة لتتمكن من التصرف والتفكير بأسلوب مشابه للبشر، وتهدف هذه النظم إلى تعلم اللغات الطبيعية وإنجاز المهام بفعالية وبأسلوب متكامل بالإضافة إلى استخدام الصور والأشكال الإدراكية لتوجيه السلوك الفعلي وتساهم أيضا في تخزين الخبرات والمعارف الإنسانية المتراكمة واستغلالها في عمليات اتخاذ القرار<sup>5</sup>.

## المطلب الثاني: أنواع وتطبيقات وفرص ومخاطر الذكاء الاصطناعي

سنتطرق في هذا المطلب إلى أنواع الذكاء الاصطناعي وتطبيقاته المختلفة، ثم نعرض على فرص تطبيقه ومخاطره.

## الفرع الأول: أنواع الذكاء الاصطناعي وتطبيقاته

سنتطرق في هذا الفرع إلى أنواع الذكاء الاصطناعي ثم إلى تطبيقاته.

## أولاً: أنواع الذكاء الاصطناعي

هناك نوعان رئيسيان من الذكاء الاصطناعي هما الذكاء الاصطناعي العام والذكاء الاصطناعي المحدود.

الذكاء الاصطناعي العام أو القوي هو مصطلح يشير إلى الآلات التي تستطيع تنفيذ مهام عقلية، جسدية أو عاطفية مشابهة لتلك التي يقوم بها البشر، ومع ذلك، فإن هناك آراء مثل رأي الباحث "يان لي كون" الذي يعتقد أن مفهوم الذكاء العام لا يوجد في الواقع.

أما الذكاء الاصطناعي المحدود أو الضعيف، فهو يشير إلى أنظمة متخصصة قادرة على التعامل مع مجموعة محدودة من المهام، فعلى الرغم من قدرة نظام "ألفا جو" على سبيل المثال، على هزيمة أي إنسان في لعبة "جو"، إلا أنه غير قادر على لعب "البوكر"<sup>6</sup>.

ويقدم آخرون تصنيف مشابه لأنواع الذكاء الاصطناعي محدد في ثلاثة أشكال رئيسية تتنوع من رد الفعل البسيط إلى الإدراك الذاتي على النحو التالي:

\* **الذكاء الاصطناعي الضيق أو الضعيف:** وهو الشكل الأبسط، يرمج لأداء وظائف محددة داخل بيئة معينة، يتسم سلوكه بالاستجابة لمواقف معينة ولا يعمل إلا في محيطه الخاص، وكمثال على ذلك، هو الروبوت "ديب بلو" من شركة IBM الذي هزم بطل الشطرنج العالمي "جاري كاسباروف" في 1996.

\* **الذكاء الاصطناعي القوي أو العام:** يتميز بالقدرة على جمع وتحليل المعلومات واكتساب الخبرات التي تمكنه من اتخاذ قرارات مستقلة مثل السيارات ذاتية القيادة وروبوتات المحادثة الفورية وبرامج المساعدة الشخصية.

\* **الذكاء الاصطناعي الخارق:** لا يزال تحت التجربة، يسعى لمحاكاة البشر، ينقسم إلى نمطين: الأول يحاول فهم الأفكار والانفعالات البشرية ولديه قدرة محدودة على التفاعل الاجتماعي. أما الثاني هو نموذج لنظرية العقل، حيث يمكن لهذه النماذج التعبير عن حالتها الداخلية والتنبؤ بمشاعر الآخرين والتفاعل معها، لذلك، فهي تعتبر الجيل القادم من الآلات فائقة الذكاء<sup>7</sup>

## ثانياً: تطبيقات الذكاء الاصطناعي:

من المجالات والتطبيقات التي استخدم فيها الذكاء الاصطناعي مايلي:

\* **معالجة اللغات الطبيعية:**

تتمثل في تطوير برامج ونظم لفهم أو توليد اللغة البشرية بهدف تسهيل التواصل بين الإنسان والحاسب، وينقسم إلى:

- فهم اللغات الطبيعية: يسعى إلى محاولة فهم الحاسب للغة الإنسان.  
- إنتاج اللغات الطبيعية: يسعى إلى البحث عن الطرق التي تساعد للحاسب على إنتاج جمل بلغة طبيعية مثل العربية أو الانجليزية<sup>8</sup>.

#### \* التعرف على الكلام:

يقصد به تطوير تقنيات تسمح للحاسب بالتعرف على حديث الإنسان بحيث يمكن للأوامر الصوتية أن تفهم وتنفذ.

#### \* البرمجة الآلية:

تعني القدرة على إعداد مفسرات أو مترجمات تتيح للحاسوب استلام برنامج مكتوب بلغة طبيعية ثم القيام بإنتاج برنامج يمكنه تشغيله.

#### \* الرؤية بالحاسوب:

يقصد بها تزويد الحاسوب بأجهزة استشعار ضوئية لتحديد الأشخاص أو الأشكال المحيطة عبر تحليل الصور والتمييز بينها الوجوه بهدف جعل الحاسب قادر على رؤية الوسط المحيط والتعرف عليه.

#### \* النظم الخبيرة:

هي نظم كمبيوتر تجمع معلومات من خبراء لتطبيقها في حل مشكلات مشابهة.

#### \* الإنسان الآلي:

وهو عبارة عن تكنولوجيا متقدمة تستخدم الذكاء الاصطناعي لتحريك الروبوت وفهم محيطه، إضافة إلى تطوير ألعاب الكمبيوتر مثل ألعاب الشطرنج التي تستند إلى برمجيات قادرة على دراسة الأساليب الفنية للألعاب<sup>9</sup>.

ومن تطبيقات الذكاء الاصطناعي في البيئة الرقمية الجديدة:

1- **الذكاء الاصطناعي يهدف تعزيز الوصول وتعزيز قدرات الإنسان:** يعد من الجوانب الإنسانية المهمة لاستخدام الذكاء الاصطناعي والذي شهد اعتمادا متزايدا مؤخرا، فقد تمكن عبر أدواته من تمكين الأشخاص ذوي الاحتياجات الخاصة من تحقيق استقلالية وإنتاجية أكبر، وكمثال على ذلك تطبيق "الذكاء الاصطناعي لمساعدة المكفوفين" الذي يتيح قراءة النص بصوت عال والتعرف على الأشخاص وعواطفهم إلى جانب إلى وصف المشاهد اليومية، وكذا تطبيق "سوندسكيب Soundscape" الذي يمنح الأفراد المكفوفين أو ضعيفي البصر القدرة على استكشاف محيطهم باستخدام تجربة صوتية ثلاثية الأبعاد<sup>10</sup>.

2- **الذكاء الاصطناعي لدعم العمل الإنساني:** حيث يمكن أيضا استخدام الذكاء الاصطناعي لدعم الفئات المهمشة في المجتمع، مثلا أقامت مؤسسة "ساج" sage شراكة مع معهد مدينة سول للعدالة الاجتماعية في جنوب إفريقيا لإطلاق برنامج "Rainbow" المدعوم بالذكاء الاصطناعي، يعمل هذا البرنامج على مساعدة ضحايا العنف الأسري للحصول على فهم كيفية طلب المساعدة وتوفير بيئة آمنة لهم من خلال التعرف على حقوقهم وخيارات الدعم المتاحة لهم...الخ

3- **الذكاء الاصطناعي لمواجهة فيروس كوفيد 19:** منذ بدء الوباء، استخدم القطاع العام والخاص حول العالم الذكاء الاصطناعي كأداة فعالية لمكافحة فيروس كوفيد 19، ففي مجال الرعاية الصحية، أسهم في التشخيص وتطوير الأدوية واللقاحات، بالإضافة إلى تحديد وتشخيص المرضى وتحديث معلوماتهم تلقائيا<sup>11</sup>.

### الفرع الثاني: فرص ومخاطر الذكاء الاصطناعي:

سننظر في هذا الفرع إلى الفرص التي يقدمها الذكاء الاصطناعي والمخاطر التي قد تنجم عنه.

#### أولا: فرص الذكاء الاصطناعي

تقدم نظم الذكاء الاصطناعي العديد من الحلول والفرص المستقبلية التي تدعم الاقتصاد وتعمل على تقدم المجتمعات، ففي دراسة للاتحاد الأوروبي نشرت في شهر جون 2020 حول موضوع الفرص التي يمكن أن يقدمها الذكاء الاصطناعي، ذكر مؤلفوها عدد من المجالات التي ستحسن فيها تقنياته من مستقبل الاتحاد، أهمها ما يلي:

\* **البيئة:** من خلال المساهمة في خفض انبعاثات غازات الاحتباس الحراري العالمية بنسبة تتراوح بين 1.5 و4 بالمئة بحلول عام 2030.

\* **الصحة:** من خلال المساهمة في تسريع عملية تحديد الأدوية الجديدة وتطويرها، بالإضافة إلى إعادة استخدام الأدوية الحالية لأغراض أخرى، كما يمكنه زيادة وتحسين التشخيص والعلاج، تحسين صحة الجنين، التنبؤ ومراقبة الأوبئة والأمراض المزمنة، تحسين خدمات الرعاية الصحية الأولية، تعزيز البحث الطبي واكتشاف الأدوية.

\* **الإنتاجية والعمل:** من المتوقع أن تحقق نظم الذكاء الاصطناعي فوائد كبيرة فيما يتعلق بالإنتاجية، على سبيل المثال، يتوقع أحد التقديرات زيادة في إنتاجية العمل بنسبة تتراوح بين 11 بالمئة و37 بالمئة بحلول عام 2035، وعلاوة على ذلك، من المتوقع أن يدعم الذكاء الاصطناعي المساهمات الإيجابية في أهداف الأمم المتحدة للتنمية المستدامة<sup>12</sup>.

## ثانياً: مخاطر الذكاء الاصطناعي

يقصد بها المخاطر أو التهديدات التي قد يسببها الاستخدام السلبي لبعض نظم الذكاء الاصطناعي، حيث سنتطرق إلى ثلاثة من أهم المجالات المهددة بهذه المخاطر كما يؤكد على ذلك العديد من الخبراء:

### 1- العمل والتوظيف:

يؤدي توسع استخدام الذكاء الاصطناعي في مختلف القطاعات الاقتصادية والاجتماعية والسياسية إلى تقليل الاعتماد على القوى العاملة البشرية، خاصة مع تطور الروبوتات لتصبح قادرة على تنفيذ مهام كانت في السابق مقتصرة على البشر، وفي هذا السياق، أظهرت دراسة أجريت من قبل باحثين في جامعة أكسفورد ونشرت في المنتدى الاقتصادي العالمي في عام 2018 أن حوالي 1.4 مليون وظيفة في الولايات المتحدة تواجه خطر الزوال بسبب التقنيات الجديدة بحلول عام 2026، وأن 47 بالمئة من الوظائف مهددة بالتحول إلى وظائف تعتمد بشكل أكبر على الحواسيب<sup>13</sup>

### 2- الأمن القومي:

في دراسة أجراها باحثون من جامعة "هارفارد كينيدي سكول" الأميركية عام 2017، تحت عنوان: الذكاء الاصطناعي والأمن الوطني، جاء في نتائجها أنه: "من المحتمل أن يصبح التقدم المستقبلي في الذكاء الاصطناعي تقنية تحويلية للأمن الوطني مثلها مثل الأسلحة النووية والطائرات وأجهزة الحاسوب والتكنولوجيا الحيوية".

وفي التقرير النهائي للجنة الأمن القومي للذكاء الاصطناعي الأميركية، والذي صدر مع مطلع العام 2021، جاء فيه أن تقنيات الذكاء الاصطناعي تؤدي إلى تفاقم تحديين للأمن القومي: \* الأول: يزيد الاعتماد على التكنولوجيا الرقمية في جميع مناحي حياتنا، من التعرض للتطفل الالكتروني عبر كل شريحة من شرائح المجتمع كالشركات، الجامعات، الحكومات، المنظمات الخاصة، منازل المواطنين والأفراد، وبالموازاة مع ذلك، غمرت أجهزة الاستشعار الجديدة العالم الحديث، ف"انترنت الأشياء" والسيارات والهواتف والمنازل ومنصات التواصل الاجتماعي تجمع تدفقات البيانات والتي يمكن بعد ذلك إدخالها في أنظمة الذكاء الاصطناعي، والتي يصبح بإمكانها تحديد المواطنين واستهدافهم والتلاعب بهم أو ارضاخهم.

\* الثاني: يتحدى الخصوم سواء من الدول أو غيرها، الولايات المتحدة باستخدام الهجمات الالكترونية والتجسس بدلا من المواجهة العسكرية المباشرة، وعلاوة على ذلك، سيتم استخدام

هذه القدرات التي يدعمها الذكاء الاصطناعي عبر مسار الصراع، إذ يمكن استخدامها كأدوات الملاذ الأول في النزاعات غير العسكرية كمقدمة للأعمال العسكرية أو بالتنسيق مع الأعمال العسكرية في الحرب<sup>14</sup>.

### 3- الأسلحة ذاتية التشغيل:

أحد التطبيقات العسكرية البارزة للذكاء الاصطناعي هو ظهور "الأسلحة ذاتية التشغيل" والتي تعرف على أنها: " أنظمة تسليح يمكنها أداء وظائفها الأساسية بالاستقلالية بشكل مستقل، أي القدرة على اتخاذ قرارات بشأن البحث والرصد وتحديد وتعقب واختيار ومهاجمتها دون تدخل بشري".

تعرف هذه الأسلحة أيضا باسم "الروبوتات المستقلة الفتاكة" أو "الروبوتات القاتلة"، حيث يمكنها البحث عن الأهداف وتحديد مهاجمتها، بما في ذلك البشر، من دون تدخل من أي إنسان في توجيهها.

ويؤكد البرلمان الأوروبي في أحد تقاريره حول مخاطر الذكاء الاصطناعي على السلامة والأمن بأن: "الاستخدام السيئ للتنظيم للذكاء الاصطناعي في مجال الأسلحة، يمكن أن يؤدي إلى فقدان السيطرة البشرية على الأسلحة الخطيرة"<sup>15</sup>.

### المبحث الثاني: أهمية الذكاء الاصطناعي في تحقيق الأمن السيبراني

نتناول في هذا المبحث مفهوم الأمن السيبراني من خلال التطرق إلى تعريفه وإلى المفاهيم المرتبطة به ونشأته وأبعاده وأهميته وأهدافه في مطلب أول، وفي المطلب الثاني، نتطرق إلى دور الذكاء الاصطناعي في تحقيق الأمن السيبراني.

#### المطلب الأول: مفهوم الأمن السيبراني

نتطرق في هذا المطلب إلى تعريف الأمن السيبراني وإلى المفاهيم المرتبطة به ونشأته وأبعاده في فرع أول، وفي الفرع الثاني نتناول أهميته وأهدافه.

#### الفرع الأول: تعريف الأمن السيبراني ونشأته وأبعاده

سوف نتناول في هذا الفرع تعريف الأمن السيبراني والمفاهيم المرتبطة به مثل الفضاء السيبراني، الجريمة السيبرانية، الردع السيبراني، الهجمات السيبرانية، التجسس السيبراني....، ثم نتطرق إلى نشأة وتطور فكرة الأمن السيبراني وأبعاده.

#### أولا: تعريف الأمن السيبراني والمفاهيم المرتبطة به

سوف نقسم هذا العنوان الى قسمين: تعريف الأمن السيبراني، المفاهيم المرتبطة به.

## 1- تعريف الأمن السيبراني

نتناول فيه التعريف اللغوي أولاً، ثم التعريف الاصطلاحي، ثم التعريف القانوني

### التعريف اللغوي:

لم تشر أغلب معاجم اللغة الحديثة إلى مصدر كلمة السيبرانية، ويتضح من ذلك أن السيبرانية كلمة يونانية الأصل ترجع إلى مصطلح (kybernetes) الذي ورد في مؤلفات الخيال العلمي ويعني القيادة والتحكم عن بعد.

واستناداً على ما سبق، عرف قاموس المورد السيبرانية بأنها علم الضبط وتعود إلى كلمة (cybernetics) التي تتلأّم مع مفهوم الهجات السيبرانية أي التحكم عن بعد والسيطرة على الأشياء،

أما قاموس مصطلحات الأمن المعلوماتي، فقد تم فيه تعريف السيبرانية كهجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على المواقع الإلكترونية، أو البنى المحمية لإعاقتها، أو تدميرها، أو الإضرار بها.

وفي اللغة العربية يستخدم مصطلح السيبرانية كما هو في اللغة الانجليزية (cyber) ولا يوجد مصطلح مرادف له في اللغة العربية.

وبالنظر في القواميس المتخصصة في المصطلحات العسكرية، نجد أنه لم يتم إرجاع كلمة ساير إلى مصدرها الأصلي، بل عرفت ضمن استخدامهما العسكري كما ورد في قاموس المصطلحات العسكرية الأمريكية بأنها أي عملية تستخدم عبر شبكات الكترونية بهدف السيطرة أو تعطيل برامج الكترونية أخرى<sup>16</sup>.

### التعريف الاصطلاحي:

جاء به عالم الرياضيات الأمريكي نوربرت وينر (norbertwiener) عام 1948 حيث استخدمت كلمة سيبرانية لوصف نظام التغذية الراجعة feedback أين لاحظ وينر وغيره من العلماء أن الإنسان والآلة يشتركان في المنهجية والنظام والسعي لاكتساب المعلومات واستخدامها<sup>17</sup> ورأى أن هذا النظام يمكن تطبيقه في مختلف المجالات العملية والإنسانية على حد سواء، ومن هنا يعتبر العلم المتعلق بقيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل هو المصدر الاصطلاحي للسيبرانية<sup>18</sup>.

## التعريف القانوني:

عرف الاتحاد الدولي للاتصالات الأمن السيبراني في تقريره حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 بأنه مجموعة مهام تشمل تقديم وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر إلى جانب التدريب والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وموارد المؤسسات والمستخدمين<sup>19</sup>.

كما عرفته المنظمة الدولية للتوحيد القياسي بأنه: (الحفاظ على سرية وسلامة وتوافر المعلومات في الفضاء السيبراني).

وقد قدم المشرع الجزائري أيضا تعريفا له في الفقرة الثالثة من المادة العاشرة من القانون 04-18 الذي يوضح القواعد العامة التي تتعلق بالبريد والاتصالات الالكترونية<sup>20</sup> بأنه مجموعة من الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق إدارة المخاطر والأعمال والتدريب والممارسات الجيدة والضمانات والتكنولوجيات المستخدمة لحماية الاتصالات الالكترونية من أي أحداث قد تؤثر على توافر وسلامة البيانات المخزنة أو المعالجة أو المرسلة.

من هذا المنظور، يمكن إعطاء تعريف شامل للأمن السيبراني بأنه مجموع القوانين والأدوات والنصوص والمفاهيم المستخدمة لحماية مصالح الدول والأشخاص، ويظل الهدف النهائي هو قدرة هذه الأدوات على الدفاع ضد التهديدات المتعمدة من قرصنة المعلومات والبيانات أو سوء استخدام تكنولوجيا المعلومات والاتصالات<sup>21</sup>.

## 2 - المفاهيم المرتبطة بالأمن السيبراني

### \* الفضاء السيبراني:

هو مصطلح تستخدمه الوكالة الفرنسية لأنظمة الإعلام ANSSI وهي هيئة حكومية مسؤولة عن الدفاع السيبراني في فرنسا يشير إلى بيئة الاتصال التي يشكلها الربط العالمي لمعدات معالجة البيانات الرقمية.

### \* الجريمة السيبرانية:

تعرف بأنها الأفعال غير القانونية التي تنفذ باستخدام أجهزة الكترونية أو عبر الأنترنت أو يتم نشر محتواه من خلال هذه الوسائط<sup>22</sup>.

### \* الردع السيبراني:

هو عملية منع الهجمات الضارة التي تستهدف الأصول الوطنية في الفضاء أو تلك التي تدعم العمليات الفضائية.

### \* الهجمات السيبرانية:

تشير إلى الأفعال التي تهدف إلى تقويض وظائف شبكات الكمبيوتر لتحقيق أغراض قومية أو سياسية من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.<sup>23</sup>

### \* التجسس السيبراني:

يتضمن المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة لدولة معادية أو خصم لسرقة معلومات سرية، على سبيل المثال، تجسست وكالة الأمن القومي الأمريكية بالتجسس على 35 قائد عالميا وأكثر من 60 مليون مكالمة هاتفية في دول مختلفة بما فيها بعض الدول الأوروبية، وقد كشفت هذه الحادثة كشفت أن التجسس لم يعد يقتصر على مواطني الدولة فحسب، بل يشمل مواطني دول أخرى وحلفاء تلك الدول مما يزيد من مشاعر عدم الثقة بين الحلفاء.<sup>24</sup>

### \* أمن المعلومات:

يقصد به الحفاظ على سرية المعلومات والبيانات على مواقع التواصل الاجتماعي وجميع المنصات الإلكترونية من أي اختراق أو تجسس.

وتتمثل العلاقة بين أمن المعلومات والأمن السيبراني في أن أمن المعلومات يشمل حماية المعلومات غير المصرح به، بينما الأمن السيبراني أوسع من ذلك، حيث يشمل أيضا الحفاظ على توافر وأمن الخدمات المقدمة عبر الفضاء السيبراني مثل الطاقة الكهربائية، وسائل الاتصال. وبذلك، فلا يمكن استخدام مصطلحي الأمن السيبراني وأمن المعلومات كمصطلحين مترادفين تماما.<sup>25</sup>

### ثانيا: نشأة الأمن السيبراني وأبعاده

نتناول في هذه النقطة نشأة الأمن السيبراني ثم نتناول أبعاده

#### 1- نشأة الأمن السيبراني

لقد ظهرت النواة الأولى للفضاء السيبراني أثناء اندلاع الحرب الأهلية الأمريكية عام 1861، حيث تم استخدام التلغراف لأول مرة لإدارة الحرب، وفي عام 1888، أظهر علماء ألمان بأن الطاقة الكهربائية تولد ترددات في الفضاء كإشارات يمكن تبنيها ومراقبتها أطلق عليها اسم ترددات هيرتز التي طورها البريطانيون إلى نظام الراديو.

وكان أول تطبيق عملي لهذه التقنية عام 1904 أثناء الحرب الروسية اليابانية عندما قصفت سفينتين حربيين يابانيين (كاسوجاوينسين) القاعدة البحرية الروسية في ميناء آرثر.<sup>26</sup>

كما أن الحربين العالميتين اللتين شهدهما العالم في النصف الأول من القرن العشرين كانتا نقطة الانطلاق في التفكير في دور التكنولوجيا في إدارة الصراع وتحقيق النصر. كذلك ما نجم عن التنافس بين القطبين المتعارضين الولايات المتحدة والاتحاد السوفياتي من تطوير في الأدوات الالكترونية وأنظمة الأسلحة وأنظمة التحكم عن بعد. وفي أوائل التسعينات، أصبح التركيز على المعلومات مصدرا للميزة التنافسية، حيث بدأت التطبيقات الأمنية في حماية كل ما يتعلق بجمع المعلومات وتخزينها ومعالجتها (أمن المعلومات) ليتطور هذا المفهوم بعد ذلك إلى (أمن الشبكات) مع انتشار استخدام تكنولوجيا المعلومات والاتصالات<sup>27</sup>.

## 2- أبعاد الأمن السيبراني

### \* الأبعاد العسكرية

يكن خطر الهجمات السيبرانية هنا في قدرتها على التسبب في نشوب الحروب والنزاعات المسلحة وكذلك اختراق نظم المنشآت النووية، مما يؤدي إلى تهديدات لأمن الدول والحكومات.

### \* الأبعاد السياسية

تتمثل مهمة الأمن السيبراني في حماية نظام سياسي للدولة وكيانها من خطر الهجمات السيبرانية التي تهدد استقرار أمن الدول والحكومات.

### \* الأبعاد الاقتصادية

من الناحية الاقتصادية، يرتبط الأمن السيبراني بشكل وثيق بالحفاظ على المصالح الاقتصادية لكل دولة، حيث إن اعتماد معظم الدول على إنتاج المعرفة وتداولها لتعزيز وتنمية اقتصادها يبرز أهمية الدور الحيوي الذي يلعبه الأمن السيبراني في حماية الاقتصاد.

### \* الأبعاد القانونية

تتمثل في القوانين والتشريعات التي تعد البيئة الحامية للمجتمع المعلوماتي، كما تساعد وتوجه في تطبيق وتنفيذ هذه التشريعات.

## الفرع الثاني: أهمية وأهداف الأمن السيبراني

نتناول في هذا الفرع أهمية الأمن السيبراني ثم نتناول أهداف الأمن السيبراني

### أولا: أهمية الأمن السيبراني

- الحفاظ على المعلومات وسلامتها من خلال منع التدخل غير المصرح به.
- ضمان توافر البيانات وسهولة الوصول إليها.

- تأمين الأجهزة والشبكات من الهجمات الإلكترونية.
- التعرف على نقاط الضعف في الأنظمة والعمل على اصلاحها.
- توفير بيئة عمل آمنة عند استخدام الأنترنت<sup>28</sup>.

### ثانيا: أهداف الأمن السيبراني

تتجسد أهداف الدفاع السيبراني الردعي في حماية قدرات الدولة التكنولوجية الخاصة بالأمن القومي بما في ذلك خطوط الاتصال والشبكات المعلوماتية والبنية التحتية بشقيها المدني والعسكري، كما تركز الجهود لتأمين البيانات الحيوية، مما يسهم في تحقيق الأمن الإلكتروني للدولة، ويمكن تحديد أهداف الأمن السيبراني كما يلي:<sup>29</sup>

1- **حماية المنشآت العسكرية:** مثل أنظمة الإدارة والمراقبة والتحكم والتوجيه بما في ذلك الأسلحة الآلية مثل الطائرات بدون طيار، بالإضافة إلى حماية المنشآت العسكرية الحيوية مثل محطات الطاقة النووية من أي اعتداء سيبراني.

2- **حماية البيانات العسكرية:** تشمل معلومات حساسة تتعلق بأفراد القوات المسلحة مثل الأسماء والرتب والمرتبات والاختصاصات، إلى جانب خطط التسليح وخرائط انتشار القوات وتوزيع الأسلحة.

3- **حماية البنية التحتية الأساسية:** ويتضمن ذلك قطاع الاتصالات ووسائل النقل ومحطات الطاقة وقواعد البيانات الحكومية والمؤسسات المالية.

4- **دعم وحدات الحرب السيبرانية:** تشمل تلك الوحدات المسؤولة عن إدارة الحروب السيبرانية للدولة، حيث تتمثل مهمة الدفاع السيبراني في تأمين الخطوط الخلفية لهذه الوحدات لحماية الأهداف الإستراتيجية للدولة عند وقوع هجوم سيبراني، كما يتضمن ذلك توفير الغطاء السيبراني للوحدات المقاتلة لتحقيق التمويه والخداع وصعوبة تعقب مصدر الهجوم.

5- **تحقيق الردع السيبراني:** يتم ذلك من خلال زيادة كلفة الهجوم السيبراني على الدولة المهاجمة عن طريق تطوير أنظمة دفاع إلكترونية معقدة وصعبة الاختراق، مما يتطلب وقتا وجهدا كبيرا لاختراقها، إضافة إلى تحسين القدرات على تعقب الهجمات السيبرانية وتحديد مصدرها لتعزيز القدرة على التأثير على قرارات الخصم وردعه عن شن هجمات سيبرانية على الدولة.

### المطلب الثاني: دور الذكاء الاصطناعي في تحقيق الأمن السيبراني

في هذا المطلب نتناول كيفية مساهمة الذكاء الاصطناعي في تحقيق الأمن السيبراني.

## الفرع الأول: مستقبل الأمن السيبراني مرتبط بالذكاء الاصطناعي:

مع تزايد الهجمات الإلكترونية على المؤسسات والشركات في السنوات الأخيرة، أصبح واضحاً أن الأسلوب الحالي للأمن السيبراني يعاني من ضعف في مواجهة التهديدات الإلكترونية، وبعد الهجمات الأخيرة التي تمكن فيها قراصنة روس من اختراق عدد من الوكالات الحكومية الأمريكية، دعا العديد من الخبراء الأمنيين إلى إجراء تغيير جذري في استراتيجيات اكتشاف ومعالجة التهديدات الإلكترونية، بحيث يتم استبدال الاعتماد على مجموعات بيانات ثابتة بنماذج ذكاء اصطناعي مرنة قادرة على فهم السلوك الطبيعي وغير الطبيعي للموظفين.

في هذا السياق، أشارت "أرتي بركار" نائبة رئيس القسم الأمني في شركة أي بي أم إلى زيادة عدد الأجهزة المحمولة في مواقع العمل وتحول الشركات إلى استخدام تقنيات السحابة الإلكترونية أدى إلى وجود ما لا يحصى من الطرق للوصول إلى مساحات العمل الافتراضية، ما تسبب بالتبعية في تزايد فرص الاختراق الرقمي<sup>30</sup>.

وفي مقال نشرته على الموقع الإلكتروني لمجلة "فاست كومباني" تحت عنوان: "مستقبل الأمن مرتبط بالذكاء الاصطناعي وليس بكلمات المرور"، أوضحت بركار أن هذا الواقع الجديد يفرض علينا من الآن فصاعداً إعادة تصميم الأنظمة الأمنية بحيث لا تعتمد الطرق التقليدية للمصادقة مثل كلمات المرور، وإنما تلجأ إلى الذكاء الاصطناعي للتحقق من الهويات والسلوكيات الرقمية، مشيرة إلى أن عملية تسجيل الدخول يجب ألا تتم بعد ذلك دون أن تثار حولها الشكوك. وأضافت، أن أحد أبرز التحديات الحالية التي تواجه المؤسسات والشركات للحفاظ على مواردها وبياناتها هو تلاشي الخط الفاصل بين من الذي يمكن اعتباره جزءاً من فريق الشركة ومن الذي لا يعد كذلك، وذلك وسط تزايد أعداد الموظفين الذين يعملون عن بعد وعمليات الاندماج المستمرة والاعتماد على تقنيات السحابة الإلكترونية، كما أضافت أنه في هذا العالم الذي لا يمكن فيه تمييز شخصيات المستخدمين بسهولة، لا يكفي أن تكون فعلاً من تدعي أنه أنت، وإنما يجب أن تتوافق تصرفاتك مع ذلك أيضاً<sup>31</sup>.

## الفرع الثاني: الذكاء الاصطناعي كبديل لكلمات المرور في حماية البيانات والخصوصيات:

ترى بركار أنه إذا أراد قراصنة الانترنت اختراق فقاعة الذكاء الاصطناعي التي تحمي المستخدم، فلن تكون مراقبة عاداته الرقمية كافية وحدها، بل سيحتاجون أيضاً إلى مراقبة هذا المستخدم جسدياً لمعرفة أدق خصوصياته، وأوضحت أن الذكاء الاصطناعي ليس تقنية جامدة، فهو يتعلم في الوقت الفعلي ويتطور باستمرار بناءً على البيانات التي يتلقاها، ومن ثم فإننا نحتاج

إلى إجراء تحليلات لملايين التهديدات المحتملة التي تحدث كل يوم، لأن الذكاء الاصطناعي يقوم بتحليلها باستمرار ويعمل على أتمتة الاستجابة الأمنية المناسبة لها وهو ما يحول النظام الأمني في نهاية المطاف إلى أداة استباقية.

واختتمت بركار مقالها بالقول أن العصر الذي كانت فيه الأجهزة الموثوقة وكلمات المرور المكونة من 14 حرف كافية لضمان الأمن قد انتهى، وينبغي علينا أن نبتكر تقنيات قادرة على التكيف بسرعة، لأنه مثلما تتغير نماذج العمل على نحو متزايد، تتغير كذلك الأساليب والتكتيكات التي يتبعها قراصنة الانترنت لاختراقها<sup>32</sup>.

### الخاتمة:

يعتبر الذكاء الاصطناعي أحد أهم انجازات الثورة الصناعية الرابعة، حيث يتوقع أن يستمر في النمو ويكتسب أهمية على مستوى عالمي نظراً للخدمات والتقنيات السريعة التي يوفرها، وعلى الرغم من فوائده، إلا أنه يثير تحديات ومخاطر تتعلق بالأمن السيبراني للدول العربية التي تعد الأضعف تكنولوجياً وقد تواجه صعوبة في مواكبة هذا التطور السريع.

لذلك، فالحديث عن مستقبل آمن للدول العربية في ظل استخدام الذكاء الاصطناعي يتطلب مواكبة التقدم في هذا المجال عبر وضع قوانين سريعة وفعالة تنظم خطوات تطوير أدوات الذكاء الاصطناعي، كما يتطلب تعزيز التعاون الرقمي بين الدول لإنشاء فضاء إلكتروني عالمي مشترك والاستفادة من نقل التكنولوجيا الرقمية ليتماشى مع تطورات الذكاء الاصطناعي ودمجها في بنية النظم الإلكترونية العربية.

ومن خلال هذه الورقة البحثية، توصلنا إلى بعض الاقتراحات والتوصيات نشير إليها في النقاط التالية:

- فرض عقوبات صارمة على سوء استخدام الذكاء الاصطناعي لتعزيز الأمن السيبراني
- تشجيع الدراسات والأبحاث في مجال الذكاء الاصطناعي لضمان حماية خصوصيات مستخدمي الانترنت.
- الاستفادة من خبرات الدول المتقدمة في مجال الذكاء الاصطناعي وتفجير الطاقات الإبداعية لدى الشباب للابتكار في هذا المجال.

## الهوامش:

- 1- عبد الرحمن تلي، علياء قاسمي الحسني: التطبيقات التربوية للذكاء الاصطناعي -التعليم الذكي نموذجاً- مجلة التربية والصحة النفسية، الجزائر، المجلد 06، العدد 02، 2020، ص 98.
- 2 - يوسف بن نافلة: المحولة المعرفية للذكاء الاصطناعي والتعليم الإلكتروني وأهميتها في تصميم التدريس، مجلة اللسانيات والترجمة، الجزائر، المجلد 02، العدد 03، 2022، ص 85.
- 3 - بكاري مختار: تحديات الذكاء الاصطناعي وتطبيقاته في التعليم، مجلة المنتدى للدراسات والأبحاث الاقتصادية، الجزائر، المجلد 06، العدد 01، 2022، ص 290.
- 4 - نفس المرجع، ص 290.
- 5 - شريرو رمضان، بوقلقول الهادي، باسي الهام: الذكاء الاصطناعي وتغير الثقافة التنظيمية: التحديات والمتطلبات، مجلة أبحاث، الجزائر، المجلد 07، العدد 02، 2022، ص 97-98.
- 6 - الأسد صالح الأسد: الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية، مجلة إضافات اقتصادية، الجزائر، المجلد 07، العدد 01، 2023، ص 168.
- 7 - نفس المرجع، ص 168-169.
- 8 - سعاد بوبجة: الذكاء الاصطناعي: تطبيقات وانعكاسات، مجلة اقتصاد المال والأعمال، الجزائر، المجلد 06، العدد 04، 2022، ص 98.
- 9 - نفس المرجع، ص 98.
- 10 - خليل سعيدي، مرزوق بن مهدي: الذكاء الاصطناعي كنوجه حتمي في حماية الأمن السيبراني، مجلة دراسات في حقوق الإنسان، الجزائر، المجلد 06، العدد 01، 2022، ص 31.
- 11 - نفس المرجع، ص 34.
- 12 - الأسد صالح الأسد: المرجع السابق، ص 170-171.
- 13 - نفس المرجع، ص 171.
- 14 - نفس المرجع، 172.
- 15 - نفس المرجع، ص 172-173.
- 16 -طلال ياسين العيسى، عدي محمد عناب : المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ظل قانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، مصر، المجلد 19، العدد 2019، ص 83
- 17 - قطاف سليمان: الأمن السيبراني والمضامين المفاهيمية المرتبطة به، مجلة طبنة للدراسات العلمية الأكاديمية، الجزائر، المجلد 05، العدد 02، 2022، ص 40

- 18- ادريس عطية: مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، الجزائر، العدد 01، 2019
- 19- قطاف سليمان: المرجع السابق، ص 41.
- 20- الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 27 الصادر في 13 ماي 2018، ص 03.
- 21- قطاف سليمان: المرجع السابق، ص 42.
- 22- مني عبد الله السمحان: متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود، جامعة المنصورة، الأ، العدد 111، مجلة كلية التربية، جويلية 2020، ص 11.
- 23 - قطاف سليمان: نفس المرجع، ص 48.
- 24- شريفة كلاع: الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الانسانية، الجزائر، المجلد 15، العدد 01، 2022، ص 295-296.
- 25- قطاف سليمان: المرجع السابق، ص 50.
- 26- علي عبد الرحيم العبودي: هاجس الحروب السيبرانية وتداعياتها على السلم والأمن الدوليين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العراق، العدد 57، ص 93-94.
- 27- أشرف محمد عبده: البيئة الأمنية للحكومة الالكترونية (بين المخاطر ومتطلبات الأمن والحماية)، دار الكتب والدراسات العربية، الاسكندرية، مصر، 2018، ص 117.
- 28- مني عبد الله السمحان: المرجع السابق، ص 12.
- 29- شريفة كلاع: المرجع السابق، ص 308
- 30 - خليل سعدي، مرزوق بن مهدي: المرجع السابق، ص 35.
- 31 - نفس المرجع، ص 35.
- 32 - نفس المرجع، ص 36.