

تأثير تقنيات الذكاء الاصطناعي على تحقيق الأمن السيبراني

د. فؤاد جدو

جامعة بسكرة

ملخص:

يعد الأمن السيبراني من أبرز التحديات الحالية التي ظهرت نتيجة للتغيرات التي طالت تهديدات الأمن غير المتماثلة، مما زاد من تعقيدها وتشابكها مع تزايد استخدام الذكاء الاصطناعي في شتى المجالات. وجاءت هذه التحولات في سياق ما بعد حروب الجيل الرابع، التي تزداد فيها استخدامات التقنيات الحديثة من هجمات سيبرانية وتهديدات لسيادة الدول الرقمية وخصوصية الأفراد والمجتمعات. وبالتالي، أصبح من الضروري التكيف مع هذه التحولات والتحضير لها في المستقبل. وفي هذه الدراسة نسعى الى تقديم مقاربات مفاهيمية حول الأمن السيبراني والذكاء الاصطناعي لكي تتمكن من فحص الحركات السببية لتفاعل كل من الأمن السيبراني والذكاء الاصطناعي في إدارة الحروب ما بعد الجيل الرابع. هذه التحولات تفرض علينا تبني استراتيجيات استباقية للتصدي لهذه التهديدات، من خلال تطوير أنظمة سيبرانية ذات مستويات عالية من الأمان، بالإضافة إلى وضع أسس علمية للحفاظ على السيادة الرقمية وتعزيز البحث العلمي، وتطوير مستوى التدريب لأفراد الأجهزة الأمنية، فضلاً عن الاستثمار في التقنيات الحديثة مثل أنظمة وأجهزة وبرامج الذكاء الاصطناعي.

الكلمات المفتاحية: الأمن السيبراني، الذكاء الاصطناعي، التهديدات السيبرانية، حروب ما بعد الجيل الرابع.

Abstract:

Cybersecurity is one of the most prominent challenges that have emerged due to changes in asymmetric security threats, which have increased their complexity and interconnectedness with the increasing use of artificial intelligence in various fields. Many researchers have placed these shifts in the context of post-4th generation wars, in which the use of modern technologies increases the use of cyber-attacks and threats to the sovereignty of digital states and the privacy of individuals and communities. Consequently, it has become necessary to adapt to these shifts and prepare for them in the future. In order to understand these changes, we aim to present conceptual approaches to cybersecurity and AI to examine the causal dynamics of the interaction between cybersecurity and AI in the management of post-4G warfare. These transformations force us to adopt proactive strategies to address these threats by developing cyber systems with high levels of security, in addition to establishing scientific foundations to preserve digital sovereignty, promoting scientific research, developing the level of training for members of the security services, and investing in modern technologies such as AI systems, devices, and programs.

Keywords: Cybersecurity, Artificial Intelligence, Cyber Threats, Post Fourth Generation Warfare

1. مقدمة

شهدت العديد من المفاهيم المتعلقة بالأمن تغييرات كبيرة، حيث أصبحت المقاربات النظرية للأمن تتكيف مع التحولات في التهديدات الأمنية غير المتماثلة. فقد انتقلت التهديدات من تهديدات الدول إلى تهديدات مرتبطة بالجريمة المنظمة، الإرهاب، والجريمة الإلكترونية. وهذه الأخيرة ارتبطت بتطور الأمن السيبراني (Cyber Security)، الذي أصبح يشمل نطاقاً أوسع من الجريمة الإلكترونية، كما أصبح أكثر تعقيداً مع انتشار استخدام الذكاء الاصطناعي في مختلف المجالات.

من جانب آخر، شهدت الحروب والنزاعات تغييرات في طبيعتها ونوع الأسلحة المستخدمة، حيث انتقلت من الحروب التقليدية إلى حروب الجيل الرابع والخامس والسادس. هذا التحول يتماشى مع التطور التكنولوجي والأنظمة المعلوماتية، مما جعل السيادة الرقمية لا تقل أهمية عن السيادة التقليدية التي تتطلب وجود أسلحة ومعدات ثقيلة وجيوش مدربة. وفي المقابل، تواجه السيادة الرقمية تهديدات سيبرانية تمس المعلومات الشخصية للمواطنين، والمعلومات الرقمية الحساسة للإدارات الحكومية وأنظمة الإدارة الأخرى. كما أصبح التجسس أكثر سهولة بفضل الأنظمة المتطورة التي تشهد ديناميكية متزايدة.

إشكالية الدراسة:

في هذا المقال، نسعى إلى معالجة إشكالية أساسية تتمثل في: ما هي محددات العلاقة بين الأمن السيبراني والذكاء الاصطناعي في ظل التحولات الدولية الحالية؟

تتفرع عن هذه الإشكالية عدة تساؤلات، هي كالتالي:

- 1- ما هو مفهوم الأمن السيبراني والذكاء الاصطناعي؟
- 2- ما هي خصائص حروب ما بعد الجيل الرابع؟
- 3- ما هي محددات العلاقة بين الأمن السيبراني والذكاء الاصطناعي؟

فرضية الدراسة:

تتأثر العلاقة بين الأمن السيبراني والذكاء الاصطناعي بشكل كبير بتطور الحروب غير التقليدية، حيث تسهم التحولات التكنولوجية الحديثة في تعزيز القدرة على مواجهة التهديدات السيبرانية، مما يفرض ضرورة تكامل الأمن السيبراني والذكاء الاصطناعي في استراتيجيات الأمن الدولي لمواجهة تحديات حروب الجيل الرابع وما بعدها.

أهمية الدراسة وأهدافها:

تكمن أهمية هذه الدراسة في تسليط الضوء على التفاعل بين الأمن السيبراني والذكاء الاصطناعي في سياق التحولات العالمية الحديثة، خاصة فيما يتعلق بالحروب غير التقليدية والتحديات السيبرانية. مع التطور السريع للتكنولوجيا والأنظمة المعلوماتية، فمن الضروري تحقيق الأمن السيبراني كأولوية ملحة لحماية المعلومات الحساسة ولحفظ سيادة الدول.

الرقمية، مما يبرز أهمية فهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني. الدراسة تقدم إسهاماً في مجال الأبحاث العلمية المتعلقة بالتحديات السيبرانية، كما تساهم في بناء استراتيجيات أكثر فعالية لمواجهة التهديدات الرقمية التي تؤثر على الأمن الشخصي والسيادي في عصر التكنولوجيا الحديثة.

أما أهداف الدراسة فنوردها في النقاط الآتية:

✓ تحليل العلاقة بين الأمن السيبراني والذكاء الاصطناعي: وذلك بدراسة كيف يتفاعل كلا المجالين في مواجهة التهديدات الرقمية.

✓ استكشاف خصائص حروب الجيل الرابع وما بعدها: من خلال فهم كيف أثرت هذه الحروب على سياسات الأمن السيبراني.

✓ تحليل التحولات العالمية: من خلال دراسة كيف تغيرت ملامح الأمن السيبراني في ظل التقدم التكنولوجي والذكاء الاصطناعي.

منهج الدراسة:

استخدمنا في دراستنا هذه المنهج الاستقرائي من أجل تحليل المفاهيم المرتبطة بالأمن السيبراني والمفاهيم المتقاطعة من أجل تفكيك وإعادة تركيب هذه المفردات. يساعد هذا المنهج في اكتشاف الأنماط والعلاقات الجديدة بين الأمن السيبراني والذكاء الاصطناعي ويساهم في تحليل وتحقيق فهم أعمق للتطورات المستمرة في المجال الرقمي وتأثيراتها على الأمن الدولي. ليسهل الوصول إلى استنتاجات دقيقة وموضوعية بناءً على دراسة الظواهر الأمنية والتكنولوجية المتغيرة. وبالتالي، يوفر المنهج الاستقرائي في هذه الدراسة تحليلاً معمقاً وموضوعياً للعلاقة بين الأمن السيبراني والذكاء الاصطناعي، ويساعد في استنتاج استراتيجيات فعالة لمواجهة التحديات السيبرانية في المستقبل.

هندسة الدراسة:

تعتمد هذه الدراسة على خطة بحثية منهجية تهدف إلى تحليل العلاقة بين الأمن السيبراني والذكاء الاصطناعي، وفهم كيفية توظيف الذكاء الاصطناعي في التصدي للتهديدات السيبرانية المتزايدة. وتتمثل هذه الخطة في المحاور التالية:

الإطار المفاهيمي للدراسة.

العوامل المحددة للعلاقة بين الأمن السيبراني والذكاء الاصطناعي.

توظيف الذكاء الاصطناعي في التصدي للتهديدات السيبرانية: الآليات والمستقبل

2. الإطار المفاهيمي للدراسة:

يهدف الإطار المفاهيمي لهذه الدراسة إلى تقديم تعريف دقيق للمفاهيم الأساسية التي تشكل محور البحث، مما يساعد في بناء فهم علمي للعلاقة بين الأمن السيبراني والذكاء الاصطناعي، واستكشاف دورهما في مواجهة التهديدات الرقمية في ظل التحولات التكنولوجية والأمنية المعاصرة.

1.2 تعريف الأمن السيبراني:

تتطلب الدراسة ضبطاً منهجياً ومفاهيمياً للأمن يحتم علينا تقديم مفاهيم دقيقة له، فحسب تعريف باري بوزان للأمن "هو تواصل التحرر من التهديد" (عطية، 2019، صفحة 15). فالأمن يعتبر مفهوماً ديناميكياً متحركاً حسب التغيرات والتهديدات؛ ولهذا الأمن مفهومه نسبي وليس مطلقاً، حيث ينطلق من السعي المستمر للدول إلى زيادة القوة مقابل انعدام الأمن؛ مما يؤدي إلى بروز تفاعلات متصاعدة والتي يطلق عليها المعضلة الأمنية.

ومع أحداث 11 سبتمبر 2001 والتي غيرت العديد من المفاهيم الجديدة للأمن وهي:

- تغيّر مصادر التهديدات والمشكلات الأمنية لتشمل أيضاً الجماعات الصغيرة والأفراد الذين أصبحوا قادرين على تهديد الأمن.

- إثبات أهمية الأمن بشكل مطلق في كل زمان ومكان.

- اتساع نطاق التهديدات الأمنية وارتفاع درجة خطورتها (مراد، 2016، صفحة 9).

يعرف ريتشارد أولمان (Richard Ullman) الأمن بأنه الفعل أو الحدث الذي يهدّد بطريقة كارثية وفي مدة زمنية قصيرة مستوى حياة سكان الدولة، ويهدد مجموعة الخيارات الخاصة بصيغة السياسة العامة المتاحة أمام دولة ما أو التنظيمات الأخرى. هذا التعريف يحتوي ثلاث محددات رئيسية وهي:

• ربط الأمن بالتهديدات الحاضرة بمعنى أنه يتعامل مع التهديدات الواقعة في الحاضر، ولا ينظر إلى تلك التي يمكن أن تحدث في المستقبل.

• مؤشر حياة المواطنين حيث أخذ التعريف تهديد حياة الناس كمعيار أساسي للأمن.

• كما أن التهديد يؤثر على صانع القرار سواء رسمي أو غير رسمي (الهاشمي، 2023، صفحة 17).

مع التطور التكنولوجي المتسارع والانتشار الواسع لاستخدام مواقع التواصل الاجتماعي كمنصة للتفاعلات الرسمية والاجتماعية، نشأت فضاءات رقمية جديدة مثل الحكومة الرقمية. وقد أدى هذا التشابك المتزايد للعالم الافتراضي في مختلف القطاعات إلى ظهور ثغرات أمنية متزايدة وتهديدات جديدة في الفضاء السيبراني.

لقد أضافت الأنترنت بعداً جديداً وهو البعد السيبراني؛ حيث أصبحت الأبعاد الآن الفضاء والجو والبحر والأرض والفضاء السيبراني. فكلمة السيبراني ليست كلمة عربية؛ بل هي كلمة أصلها إنجليزية وهي مشتقة من علم cybernetics ومنها cyberspace أي الفضاء السيبراني وهو المكان الذي تتم فيه الاتصالات وليس هو الأنترنت. هذه الكلمة cyber ظهرت في الثمانينيات من القرن الماضي في رواية من روايات الخيال العلمي اسمها cyberpunk للمؤلف William Gibson وهي سلسلة روائية تتحدث عن تكنولوجيا المعلومات والمستقبل وتأثير هذه التقنية على المجتمع. من هنا انتشر مصطلح الفضاء الإلكتروني والذي يتكوّن من الشبكات المادية مثل الكوابل والخوادم والأجهزة، أما الجانب الآخر فيتكوّن من البرمجيات والخدمات الإلكترونية والتطبيقات وهي ليست ملموسة، بالإضافة إلى البيانات الموجودة في

الفضاء السيبراني، وآخر عنصر هو الإدراك الذي تتم فيه العمليات أو ما يعرف بالذكاء الاصطناعي. (الجندی، 2023، صفحة 61).

عرف الأمن السيبراني تطوراً من بداية السبعينيات من القرن الماضي؛ إذ لم يكن هناك الكثير من المعلومات حول برامج التجسس والاختراق، ولكن بدأ يتشكل بشكل واضح عندما قدم المفكر روبرت توماس (Robert Thomas) برنامج الحاسب الآلي المعروف بالزاحف؛ وهو عبارة عن برنامج قادر على التحرك من خلال شبكة إلكترونية تعرف بشبكة تنيكس (The Tenex)، وبعدها تم وضع حد لهذا البرنامج الفيروسي من طرف راي توملينسون (Ray Tomlinson) الذي اخترع البريد الإلكتروني عبر برنامج جديد أطلق عليه الحصاد؛ والذي وضع حداً له واعتبر أول نظام لمكافحة الفيروسات (الرمحي، 2023، صفحة 18).

كما يعرف الأمن السيبراني بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات. كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن؛ بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة. وفي تعريف آخر "هو النشاط أو العملية أو نظم المعلومات واتصالات الدولة؛ حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف أو الاستخدام غير المصرح به أو التعديل أو الاستغلال" (سميرة، 2017، صفحة 257).

تعريف آخر للأمن السيبراني هو "حماية الأنظمة المتصلة بالإنترنت بما في ذلك الأجهزة والبرامج والبيانات من الهجمات الإلكترونية؛ وذلك لضمان الحفاظ على السرية والنزاهة وتوافر البيانات".

الأمن السيبراني هو عملية تأمين البرامج والشبكات والأنظمة ضد الهجمات الرقمية. يمنع هذا التمرين النشاط الخبيث الذي يهدف إلى تدمير الشحن أثناء الوصول إلى البيانات الحساسة، أو إساءة استخدام معلومات المستخدم، أو مقاطعة العمليات اليومية. وهو أيضاً يعرف أنه ممارسة لمنع التهديدات المحتملة أو الهجمات الخبيثة التي تسعى إلى الوصول غير القانوني إلى البيانات أو إتلاف المعلومات أو تعطيل العمليات الرقمية. حيث يتم تعريف المفهوم هنا من خلال نوع الأنشطة التي يقوم بها المهاجم (Schiliro, 2023, p. 5).

تزداد أهمية الأمن السيبراني في الوقت الحالي نظراً لدوره الحاسم في حماية المعلومات والأنظمة التكنولوجية من التهديدات المتنوعة، والتي تشمل الهجمات الإلكترونية التخريبية. إذ تلجأ بعض الجماعات والتنظيمات الإجرامية إلى شن هجمات على الشبكات، وأنظمة الكمبيوتر، ووسائل الاتصالات، والبنى التحتية الإلكترونية، سواء بهدف التخريب أو لاختراق البيانات السرية والحصول عليها، مما يجعل تعزيز الأمن السيبراني ضرورة استراتيجية لمواجهة هذه المخاطر المتزايدة. يقدم (Schiliro, F) تعريفاً للأمن السيبراني على أنه جمع وتوحيد الموارد بما في ذلك الأفراد والبنية التحتية والهيكل والعمليات لحماية الشبكات وأنظمة الكمبيوتر السيبرانية من الأحداث التي تعرض سلامتها للخطر وتتداخل مع حقوق الملكية، مما يؤدي إلى قدر من الخسارة (Schiliro, 2023, p. 11).

هنا تظهر مفاهيم مرتبطة بالأمن السيبراني كمفهوم الجرائم السيبرانية والتي تعني الجرائم التي تحدث عن طريق الأنترنت والحواسيب، ومفهوم الحرب السيبرانية التي يقصد بها التعدي على شبكات وحواسيب ومعلومات بقصد السرقة أو التخريب والتدمير التي تحدث بين الدول أو الجماعات. (الحكيم، 2022، صفحة 55).

الأمن السيبراني هو تنظيم وتجميع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الإلكتروني والأنظمة التي تدعمه من الأحداث التي تعارض مع حقوق الملكية الفعلية بحكم القانون (Craig, 2014, p. 17).

الأمن السيبراني هو مجموعة من التدابير والتقنيات والإجراءات التي تهدف إلى حماية الأنظمة الرقمية، والشبكات، والبيانات من الهجمات الإلكترونية والتهديدات السيبرانية المختلفة. ويشمل ذلك حماية المعلومات الشخصية، والبنى التحتية الحيوية، والأنظمة الحساسة من الاختراق، التجسس، التخريب، والبرمجيات الخبيثة. وبعد الأمن السيبراني ركيزة أساسية لضمان سلامة وأمان الفضاء الرقمي، سواء على المستوى الفردي أو المؤسسي أو الوطني.

2.2. مفهوم الذكاء الاصطناعي:

يعود ظهور مصطلح الذكاء الاصطناعي إلى عالم الكمبيوتر جون مكارثي (John McCarthy) من كلية دارتموث ومجموعة من الباحثين في مشروع بحثي بعنوان "proposal for the Dartmouth summer project on artificial intelligence" سنة 1955، والذي يشير إلى محاكاة للذكاء البشري في الآلات بحيث يستطيع أداء مهام متعددة بطريقة مماثلة لما يفعله البشر؛ بناء على المعلومات التي يجمعها ويعمل على تحسين هذا الأداء كلما زادت البيانات والمعلومات التي يحصل عليها. هذا بالإضافة إلى القدرة على التعامل مع عدد ضخم من البيانات الكبيرة. (عمران، 2023، صفحة 15)

الذكاء الاصطناعي (Artificial Intelligence) يعرف "قدرة الآلات والحواسيب الرقمية على القيام بمهام معينة تحاكي وتشابه تلك التي تقوم بها الكائنات البشرية كالقدرة على التفكير أو التعلم وغيرها من العمليات الأخرى التي تتطلب عمليات ذهنية؛ حيث تقدم هذه الأنظمة خدمات مختلفة من التعليم والإرشاد والتفاعل" (البابلي، 2023، صفحة 103).

ثمة حاجة إلى الإلمام بالتطور التاريخي للذكاء الاصطناعي حتى نتمكن من فهم أهميته. إن هذا يستلزم فهم التاريخ الحافل للذكاء الاصطناعي والذي ينطوي على محطات بارزة وتطورات مهمة حيث تعود جذور الذكاء الاصطناعي إلى منتصف القرن العشرين؛ حيث شهدت هذه الفترة تحول الأساس النظري للاستدلال الرياضي إلى نقطة محورية في تطوير الذكاء الاصطناعي وهو ما وضع الأساس للسعي الفكري نحو إنشاء آلات قادرة على محاكاة الوظائف المعرفية للعقل البشري. فظهر الذكاء الاصطناعي في أعقاب تطور علم السيبرنيتيقا (Cybernetics) أي علم التحكم الآلي؛ ففي التكنولوجيا والذكاء الاصطناعي تستخدم السيبرنيتيقا في تصميم الروبوتات والأنظمة الذكية التي تعتمد على التعلم الآلي

واتخاذ القرار الذاتي. وفي الأمن السيبراني يتم توظيفها في تطوير أنظمة الحماية الرقمية التي تستطيع التعلم والتكيف مع الهجمات السيبرانية والتصدي لها بطرق متطورة.

في فترة منتصف السبعينيات تطورت أجهزة الحاسوب وأصبحت أسرع وأخذت تقنيات تعلم الآلة وهي فرع من فروع الذكاء الاصطناعي. وبعد 2011 كانت هناك تطورات في أبحاث الذكاء الاصطناعي مدفوعة بتوافر كميات هائلة من البيانات؛ ليشهد هذا المجال تطوراً كبيراً (كيلاني، 2024، صفحة 12).

كما يعرف الذكاء الاصطناعي على أنه "الذكاء الذي تظهره الآلات مقابل الذكاء الطبيعي الذي يملكه البشر أي أنه دراسة العوامل الذكية، وهو محاكاة الوظائف المعرفية التي يرتبط بها البشر بالعقل البشري مثل التعلم وحل المشكلات" (شيخ، 2023، صفحة 17).

كما يعرف نيلز جون نيلسون (Nils John Nilsson) الذكاء الاصطناعي بأنه "النشاط الذي من شأنه أن يجعل الآلة الذكية والذكاء هو الصفة التي تنسحب على أي كيان قادر على التصرف بشكل مناسب، ويستخدم بصيرته في البيئة التي يتواجد فيها" (عمران، 2023، صفحة 15).

يشير الذكاء الاصطناعي إلى "الأنظمة التي تظهر سلوكاً ذكياً من خلال تحليل بيئتها واتخاذ إجراءات -بدرجة معينة من الاستقلالية- لتحقيق أهداف محددة" (Russell & Norvig, 2023, p. 20).

في نوفمبر 2022 أطلقت شركة Open AI الأمريكية برنامج دردشة جديد هو CHAT GPT، والجديد في هذا البرنامج هو أنه يعتمد كلياً على الذكاء الاصطناعي؛ فهو يتحاور مع المستخدم ويجيب على ما يطرح عليه من أسئلة بشكل مفصل وينتج نصوصاً أشبه بالنصوص البشرية (عمران، 2023، صفحة 37).

كما يمكن أن نعرف الذكاء الاصطناعي "بأنه أحد فروع علم الحاسوب ويعرف على أنه المجال الذي يسعى إلى فهم طبيعة الذكاء البشري عن طريق تكوين برامج على الحواسيب التي تقلد الأفعال أو الأعمال أو التصرفات الذكية" (عمر، 2024، صفحة 154).

يتكون مفهوم الذكاء الاصطناعي من مجموعة من العناصر؛ وهي:

- التعلم الآلي: الذي يعني بتزويد الآلات بالقدرة على التعلم باستخدام الخوارزميات التي تكتشف أنماطاً من البيانات والمعطيات التي تتعرض لها الآلة لتطبيقها في المستقبل واتخاذ القرارات والتنبؤات.
- التعلم العميق: وهو تقنية اخترعها الإنسان من أجل محاولة تقليد الطريقة التي يعمل بها العقل البشري؛ فالتعلم العميق يحاول أن يحاكي العقل البشري في جميع قدراته ويتم تدريب النماذج باستخدام مجموعة كبيرة من البيانات المصنفة وبنيات الشبكات العصبية.
- الشبكات العصبية: ويرمز لها باختصار ANN وتتكون الشبكات العصبية من مجموعة من الخوارزميات يتم من خلالها محاكاة الدماغ البشري، وتصنيع أدمغة إلكترونية قادرة على التعلم والتطور تشبه الدماغ البشري. والمميز

في الشبكات العصبية الاصطناعية هو وجود طبقات عديدة تعمل على التعلم العميق (البابلي، 2023، صفحة 104).

التعلم الآلي هو فرع محدد من الذكاء الاصطناعي يركز على الأساليب التي تتعلم من البيانات أو من التجارب السابقة، على سبيل المثال، لاكتساب المعرفة من البيانات أو لإجراء التنبؤات. ويشمل ذلك طرق التعرف على الأنماط مثل التصنيف والتجميع العنقودي، والتي يمكن إجراؤها باستخدام أساليب مختلفة مثل الشبكات العصبية وأشجار القرار وآلات ناقلات الدعم، بالإضافة إلى النماذج الإحصائية مثل الانحدار. يمكن تدريب هذه الأساليب باستخدام التعلم الخاضع للإشراف أو غير الخاضع للإشراف أو التعلم المعزز. في الآونة الأخيرة، تم تطوير مناهج التعلم العميق، والتي هي في الأساس مزيج من التطورات على الشبكات العصبية، والتي تستخدم في العديد من التطبيقات المختلفة من رؤية الكمبيوتر إلى معالجة اللغة الطبيعية للأجسام الكبيرة من النص. كانت أحدث التطورات في الذكاء الاصطناعي في شكل نماذج لغوية كبيرة (LLMs) مثل ChatGPT، التي طورها OpenAI و Gemini من Google وعائلة نماذج LLaMA من Meta. تستخدم LLMs التعلم العميق ومعالجة اللغة الطبيعية جنبًا إلى جنب مع مجموعات البيانات الضخمة لاستنتاج العلاقات وإنشاء أنواع جديدة من المحتوى (Dilek, April 2024, p. 3).

في محصلته الذكاء الاصطناعي يحقق مجموعة من الأهداف الأساسية؛ ومنها:

- تمكين أجهزة الكمبيوتر من تنفيذ المهام التي يستطيع العقل تنفيذها مثل التفكير والإدراك الحسي والربط بين الأفكار.
- استخدام أجهزة الكمبيوتر لإنجاز مهام مفيدة باستخدام طرق مختلفة عن التي يستخدمها العقل البشري.
- استخدام مفاهيم الذكاء الاصطناعي ونماذجها للمساعدة في الإجابة عن أسئلة تتعلق بالإنسان وغيره من الكائنات الحية.
- تمكين الآلة من معالجة المعلومات بشكل أقرب إلى طريقة الإنسان أي المعالجة المتوازية لعدة مهام في نفس الوقت (خليفة، 2024، صفحة 132).

3. العوامل المحددة للعلاقة بين الأمن السيبراني والذكاء الاصطناعي:

توجد علاقة جوهرية بين الأمن السيبراني والذكاء الاصطناعي، وهو ما نسعى إلى دراسته في هذا المحور من الدراسة، حيث يمثل كل منهما امتدادًا للآخر، لا سيما أن كلاهما يرتبط ارتباطاً وثيقاً بالإنترنت والفضاء السيبراني باعتباره مجاًلاً رئيسياً للتفاعلات الافتراضية.

يعد الذكاء الاصطناعي أداة رئيسية في مجال الأمن السيبراني، حيث يتم تطوير أنظمة ذكية لتعزيز الحماية الرقمية، وفي المقابل، يتم تطبيق تدابير أمنية صارمة لحماية أنظمة الذكاء الاصطناعي نفسها من الاختراق والتلاعب. مع تصاعد الجرائم الإلكترونية مثل سرقة البيانات والتصيد الاحتيالي، أصبحت المنظمات والدول تعتمد على تقنيات متطورة لمكافحة

هذه التهديدات، من خلال فرق متخصصة في الأمن السيبراني مزودة بأحدث الأدوات، بما في ذلك تقنيات الذكاء الاصطناعي. تساهم هذه التقنيات في الكشف السريع عن الأنشطة الضارة والتصدي لها، إلى جانب تأمين الشبكات من الهجمات الإلكترونية. إضافة إلى ذلك، تعمل الدول على تطوير الأنظمة والمناهج التدريبية المتخصصة لإعداد كوادر قادرة على مواجهة التهديدات السيبرانية بفعالية.

في مجال الأمن السيبراني، يلعب الذكاء الاصطناعي دورا محوريا في تطوير تطبيقات آمنة قادرة على القضاء على الثغرات الأمنية، وتحسين دقة اكتشاف المشكلات، وتسريع عمليات التحقيق، بالإضافة إلى أتمتة (Automation)) - عملية استخدام التكنولوجيا والأنظمة الذكية لأداء المهام والعمليات بشكل تلقائي دون تدخل بشري مباشر، مما يساهم في تحسين الكفاءة، وتقليل الأخطاء، وتسريع الإنجاز في مختلف المجالات - الاستجابات الأمنية. هذا التكامل يعزز من قدرة الشركات والمؤسسات على بناء بنية تحتية سيبرانية قوية، قادرة على مواجهة التحديات الرقمية المتزايدة بفعالية وكفاءة.

1.3. تطور أجيال الحروب والأمن السيبراني:

ما يهمنا هنا هو البعد الدولي والتفاعلي للفضاء السيبراني والذكاء الاصطناعي من خلال الحروب خاصة بعد الجيل الرابع. وهو ما يجعلنا بحاجة لاستعراض أجيال الحروب وتطوراتها لفهم علاقة الذكاء الاصطناعي بالأمن السيبراني. شهدت الحروب عبر التاريخ تطورا كبيرا، بدءا من الحروب التقليدية التي تعتمد على المواجهة المباشرة، وصولاً إلى الحروب الحديثة التي تركز على التكنولوجيا المتقدمة، ومنها الذكاء الاصطناعي والأمن السيبراني. وقد تأثرت طبيعة الصراعات العسكرية والأمنية بتطور التقنيات الرقمية، مما جعل الأمن السيبراني والذكاء الاصطناعي عنصرين أساسيين في استراتيجيات الحروب المعاصرة.

حروب الجيل الأول conventional war: وهذا الجيل من الحروب ظهر عقب اتفاقية وستفاليا عام 1648م التي أنهت حوالي ثلاثين عاما من الحروب في القارة الأوروبية وأنتجت الدولة القومية بمفهومها الحديث؛ والذي ارتبط بظهورها مفهوم السيادة الوطنية الذي أفرز بدوره مرحلة الجيوش بشكلها الحديث للدفاع عنها. أطلقت تسمية الجيل الأول على الحروب التقليدية التي تقع بين جيشين نظاميين ويعرفها الخبير العسكري الأمريكي وليم. س. ليند (William S. Lind) بأنها حروب الحقبة من 1648 إلى 1860 وهي حروب تتميز بالأسلحة البسيطة والمواجهة (محمد، 2021، صفحة 18).

حروب الجيل الثاني guerilla war: والتي كانت نتيجة تطور التكنولوجيا الحربية، خاصة في الأسلحة المستخدمة أي انتشار الآليات العسكرية. ظهر مبدأ وضعته فرنسا وهو أن المدفعية تحزم والمشاة تحتل وهذا ما جعل النيران الكثيفة هي السلاح الحاسم في المعركة، والتي بدأت مع الحرب العالمية الأولى. وتقوم هذه الحروب على التنسيق بين أسلحة المدفعية والمدرمات والمشاة بالإضافة إلى التركيز على الانضباط كما يقوم على إعداد منهج يتم تدريب الجنود عليه لتحقيق

الأهداف. كما ارتبط هذا الجيل بظهور سلاح الطائرات والاقتصاد الصناعي أي الجمع بين المدفعية والضربات الجوية. (منصور، 2019، صفحة 26)

حروب الجيل الثالث preventive war: تعرف بالحروب الوقائية أو الاستباقية ويعتبر الجيش الألماني هو من طور هذا النمط في الحرب العالمية الثانية، وتتميز بعنصر المفاجأة والسرعة والمرونة وتسمى بحرب المناورة وتسعى للوصول إلى عمق العدو. (الحكيم، 2022، صفحة 19)

حروب الجيل الرابع 4GW: تعتبر هذه الحروب حديثة؛ أطلق هذا المصطلح لأول مرة سنة 1989 حيث تتميز باستخدام تقنيات غير عسكرية منها وسائل الإعلام والسياسة. ولكن هناك من يرى بأنها حرب طورها الخبراء العسكريون بعد أحداث 11 سبتمبر؛ وبالتالي هي الحرب على المنظمات الإرهابية ويكون الطرف الآخر جيش نظامي. ويطلق عليها أيضا اسم الحرب اللاتماثلية خاصة أن الجيش النظامي للدول لا يحارب جيش واضح بل تنظيم غير محدد بوسائل غير واضحة، ولهذا تسمى غير تماثلية. (محمد، 2021، صفحة 30)

حروب الجيل الخامس 5GW: فهي تقوم على احتلال العقول فحسب توماس اكس هامز (Thomas X. Hammes) أحد المختصين في الدراسات الأمنية يرى أن بروز الجيل الخامس جاء بسبب تراجع الدولة لاستخدام القوة المسلحة وظهور فواعل مسلحة من غير الدولة؛ فهي حرب تستخدم فيها كل أنواع الأسلحة بما فيها السيبرانية، كما تعتبر حرب بلا قيود؛ أين يتم توظيف هذا النمط من الحرب لتحقيق المفاجأة للعدو وهذا عبر وكلاء يصعب نسب أفعالهم إلى الدولة الداعمة لهم، والهدف منها أيضا إسقاط الدولة من الداخل (منصور، 2019، صفحة 45).

هذا أدى إلى الترابط بين الفضاء السيبراني والجريمة الإلكترونية من جهة والحروب التي بدأت تتطور مع تطور التكنولوجيا؛ خاصة مع تزايد مجال استخدام الذكاء الاصطناعي مما أنتج حروب الجيل السادس.

حروب الجيل السادس: أول من أطلق تسمية حروب الجيل السادس الجنرال الروسي فلاديمير سليبتشيك حيث قال بأن الحروب ستدار بأنظمة ذكية وستحصل نتائج ذكية؛ حيث تعمل هذه الحروب على تجنيد كامل لشبكة الأنترنت وتخلق عصابات مهمتها الاحتيال وسرقة الهويات وممارسة العمليات الإجرامية، وهي حروب جمعت ما بين الإرهاب والإدارة عن بعد. وهناك من يطلق عليها اسم منظومة الجن الفضائي لأنها تعتمد على تقنيات عالية التطور تشبه الخيال المحض والأقمار الصناعية والتوجه إلى التحكم في البشر وخياراتهم (الحكيم، 2022، صفحة 22). وهذا يعتبر تحدي صعب وقد بدأت بوادره من خلال استغلال منصات التواصل الاجتماعي لتوجيهات ورغبات المستخدمين في المجال التجاري وتوجيه الرأي العام الإلكتروني، وغيرها من التأثيرات التي تأتي مع الذكاء الاصطناعي الآن ومستقبلا.

عرف العالم تحولات مع بدء إرهابات الثورة الصناعية الرابعة إذ بدأ الجيل الرابع من العولمة لينشأ مفهوم جديد وهو العولمة الرقمية وأفضل وصف لتكنولوجياته الرائدة الذكاء الاصطناعي؛ والذي يعتمد على جزء من الجيل الخامس (5G) للأنترنت كأحدث تقنيات شبكات الاتصالات اللاسلكية، بما فيها العملة الرقمية المشفرة والتكنولوجيا البيولوجية؛ وبالتالي أصبح التركيز على الذكاء الاصطناعي باعتباره محرك النمو الاقتصادي وتراكم الثروة، كما يساهم في

تحقيق الرقابة المجتمعية من طرف الحكومة، بالإضافة إلى التدقيق في البيانات والسلوكيات وحتى توقع ردود أفعالهم. وهناك بعض الدول التي تقوم بحماية نفسها عبر استخدام الذكاء الاصطناعي مثل الصين والتي وضعت نظاما رقميا يعرف بسور الصين الرقمي والذي عزل الأنترنت في الصين عن بقية العالم بواسطة جدار حماية ضخمة تستخدم فيها الحكومة الصينية خوادم تراقب الفضاء الرقمي للدولة ضد أي تهديد سيبراني خارجي يهدد الأمن الوطني الصيني. (عباس، 2021، صفحة 106).

بناء على ما سبق اتجاه نحو إعادة تعريف القوة من المنظور الدولي في ظل تزايد استخدام الذكاء الاصطناعي بعيدا عن الحروب وتطورها، إلا أننا نجد أن هناك حالة من التنافس الدولي للاستحواذ على مقدرات الذكاء الاصطناعي وتطوير تطبيقاته في المنظومة الدفاعية والهجومية داخل الجيوش الحديثة، وتساعد التحالف ما بين الشركات التقنية والجيوش. وهذا ما يفسر بروز اتجاهين في هذا الإطار، الأول والذي يدعو إلى عسكرة الخوارزميات لتحقيق أهداف أمنية ناعمة ذات تأثير عميق عابر للحدود، والاتجاه الثاني يدعو إلى تطوير القوة الصلبة من أجهزة ومعدات تلعب دورا قتاليا في الحروب مثل المسيرات أو الروبوتات والأسلحة ذاتية القيادة؛ وبالتالي التحكم في الأمن الدولي والوطني عبر توظيف الذكاء الاصطناعي (الصادق، 2024، صفحة 78).

2.3. العلاقة بين تطور أجيال الحروب والذكاء الاصطناعي والأمن السيبراني:

يمكن أن تتكامل أساسيات الذكاء الاصطناعي والأمن السيبراني من خلال العناصر التالية:

- يمكن للذكاء الاصطناعي أن يقوم بمراقبة ومتابعة المجتمع، من خلال تحليل القياسات الحيوية والتحكم في المعلومات السرية والقومية للدول.
- تحويل تطبيقات الذكاء الاصطناعي إلى خدمات وبنية تحتية في الجانب العسكري والاستخباراتي وتعزيز التصنيع الحربي وبناء أنظمة الردع وتزايد العسكرة في الذكاء الاصطناعي وحماية الأمن السيبراني.
- كما يوظف الذكاء الاصطناعي الحرب الإلكترونية على الموجات الكهرومغناطيسية وأنظمة الاتصالات.
- يمكن توظيف الذكاء الاصطناعي في شن هجمات سيبرانية كثيفة وعميقة، وفي الوقت نفسه تعزيز الدفاع السيبراني واختراق الشبكات الإلكترونية للجيوش الأخرى، بالإضافة إلى الكشف عن الثغرات الأمنية والتنبيه بالتهديدات السيبرانية ورصد الأنشطة المعادية (الصادق، 2024، صفحة 88).

للذكاء الاصطناعي تأثير إيجابي على الأمن السيبراني من خلال:

1. **اكتشاف التهديدات:** يمكن للأنظمة التي تعمل بالذكاء الاصطناعي تحليل كميات هائلة من البيانات من مصادر مختلفة - مثل حركة المرور على الشبكة وسجلات البيانات وسلوك المستخدم - بسرعات لا تصدق لتحديد الأنماط والشذوذ التي تشير إلى التهديدات السيبرانية. وهذا يسمح باكتشاف أسرع وأكثر دقة للهجمات مقارنة بالأنظمة التقليدية القائمة على القواعد، مما يتيح اكتشاف الشذوذ والتهديدات المحتملة في

الوقت الفعلي. من خلال أتمتة عملية اكتشاف التهديدات، يمكن للذكاء الاصطناعي تحديد الأنماط والارتباطات التي قد يتجاهلها المحللون البشريون، مما يؤدي إلى اكتشاف أكثر دقة وكفاءة للهجمات السيبرانية.

2. **استجابة محسنة للحوادث:** يمكن للذكاء الاصطناعي مساعدة فرق الأمن في الاستجابة للحوادث السيبرانية واحتوائها وتخفيفها بشكل أكثر فعالية وسرعة من خلال أتمتة مهام معينة، مثل تحليل السجلات وارتباط البيانات وإعطاء الأولوية للتنبيهات. يمكن للأدوات التي تعمل بالذكاء الاصطناعي تحليل طبيعة الهجوم وتحديد الاستجابة الأكثر فعالية وحتى بدء إجراءات الإصلاح، وبالتالي تمكين فرق الأمن من تقليل التأثير المحتمل لخرق الأمن.

3. **التحليلات التنبؤية:** من خلال تحليل البيانات التاريخية والتعلم من الحوادث الأمنية السابقة، يمكن للذكاء الاصطناعي المساعدة في التنبؤ بالهجمات المستقبلية ومنعها. وهذا يمكن المؤسسات من معالجة الثغرات الأمنية بشكل استباقي وتحسين وضعها الأمني العام.

4. **أتمتة الأمان:** يمكن للذكاء الاصطناعي أتمتة المهام المتكررة والمستهلكة للوقت، مثل تحليل السجلات ومسح الثغرات الأمنية، مما يوفر وقتًا ثمينًا لخصري الأمن للتركيز على قضايا أكثر استراتيجية.

5. **تقييم المخاطر وإدارتها المتقدمة:** يمكن لخوارزميات الذكاء الاصطناعي معالجة وتحليل كميات هائلة من البيانات من مصادر مختلفة، مثل سلوك المستخدم وحركة المرور على الشبكة وتكوينات الأجهزة، لتحديد الثغرات الأمنية المحتملة وتقييم المخاطر الإجمالية للمؤسسة. وهذا يمكن فرق الأمن من تحديد أولويات جهودها وتخصيص الموارد بشكل أكثر فعالية، مما يؤدي في النهاية إلى وضع أمني أكثر قوة (Wilson, April 2023, p. 16).

أصبح إدخال الذكاء الاصطناعي في الصراع السيبراني عنصرا حاسما، حيث يساهم في تعزيز القوة السيبرانية ويوفر مزايا استراتيجية. يساعد ذلك الدولة في استخدام قوتها المسلحة لتحقيق أهدافها في الحفاظ على أمنها القومي، وتحويل ذلك إلى مكاسب جيوسياسية واقتصادية. وبذلك، أصبح الذكاء الاصطناعي جزءا أساسيا في قياس القوة العسكرية للدول وتصنيف الجيوش.

مع تطور الحروب، أصبح الذكاء الاصطناعي والأمن السيبراني عاملين أساسيين في استراتيجيات الدفاع والهجوم، حيث يمكننا توضيح العلاقة كالتالي:

✓ الذكاء الاصطناعي أصبح جزءا أساسيا من الأنظمة العسكرية الحديثة:

حيث يتم استخدامه في:

1. تحليل البيانات الضخمة لتحديد استراتيجيات الهجوم والدفاع.
2. تطوير أنظمة الأسلحة الذكية، مثل الطائرات بدون طيار والروبوتات القتالية.

3. أنظمة المراقبة والتجسس المتقدمة، مثل استخدام الذكاء الاصطناعي في تحليل الصور والفيديوهات الاستخباراتية.
4. الحرب النفسية والدعاية الرقمية، من خلال التلاعب بالرأي العام باستخدام الخوارزميات الذكية.

✓ الأمن السيبراني كأحد ركائز الحروب الحديثة:

مع الانتقال إلى الحروب الرقمية، أصبح الأمن السيبراني عنصراً أساسياً في استراتيجيات الدفاع والهجوم، حيث يتم استخدامه في:

1. حماية الأنظمة العسكرية من الاختراقات والتجسس الإلكتروني.
2. مكافحة الهجمات السيبرانية التي تستهدف البنية التحتية للدول (مثل الهجمات على محطات الطاقة وشبكات الاتصالات).
3. تطوير أنظمة دفاع سيبراني ذكية قادرة على اكتشاف الهجمات السيبرانية والتصدي لها قبل وقوعها.
4. شن الهجمات السيبرانية ضد الأعداء من خلال تعطيل أنظمتهم الرقمية وإضعاف قدرتهم العسكرية.

✓ التداخل بين الذكاء الاصطناعي والأمن السيبراني في الحروب:

يعمل الذكاء الاصطناعي على تحسين قدرات الأمن السيبراني عبر:

1. التنبؤ بالهجمات الإلكترونية من خلال تحليل الأنماط السيبرانية المشبوهة.
 2. أتمتة أنظمة الحماية، مما يسمح بالاستجابة السريعة للتهديدات السيبرانية.
 3. تعزيز أنظمة الدفاع السيبراني باستخدام تقنيات التعلم العميق وتحليل البيانات في الوقت الحقيقي.
 4. توظيف الذكاء الاصطناعي في التصدي للتهديدات السيبرانية: الآليات والمستقبل
- من الضروري استغلال الذكاء الاصطناعي لمواجهة التهديدات السيبرانية، ولكن قبل ذلك يجب أولاً تحديد ماهية هذه التهديدات من أجل وضع إطار مناسب لمواجهتها.

1.4. التهديدات السيبرانية:

التهديدات السيبرانية هي محاولات خبيثة ومخططة لاختراق الأنظمة الرقمية أو استغلال الثغرات الأمنية بهدف الوصول إلى المعلومات أو تدمير الأنظمة التكنولوجية. مع تطور التكنولوجيا، أصبحت التهديدات السيبرانية أكثر تعقيداً، وتستهدف المؤسسات الحكومية والشركات والأفراد على حد سواء. يمكن تصنيف هذه التهديدات إلى أنواع متعددة، أبرزها:

أولاً: اختراق المواقع الإلكترونية: يتم اختراق المواقع الإلكترونية لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل في الموقع تعلن اختراقه.

ثانياً: الفيروسات: وهي فيروسات الحاسب الآلي التي تنتشر بسرعة كبيرة عن طريق شبكة الأنترنت؛ وذلك يرجع إلى عدد الملفات الهائل التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية. وهذه الفيروسات هي عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط هذه الفيروسات تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها، ولها أضرار مختلفة تتمثل في فقد الملفات المخزنة، وقد تصل تلك الأضرار إلى تحطيم نظام التشغيل في الجهاز.

ثالثاً: الحرب الإعلامية: فالفضاء الإلكتروني له تأثير هائل على الرأي العام العالمي؛ لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتى أنحاء العالم بوسائل مختلفة "الصوت - الصورة - النص"؛ وبالتالي أي جماعة أو منظمة يمكن لها إنشاء مواقع إلكترونية تروج أفكارها وتنشرها في مختلف أنحاء العالم.

رابعاً: التجسس الإلكتروني: لقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات ومراقبة المعلومات التي يتم تداولها حول العالم.

خامساً: التهديد الإلكتروني: يوجد العديد من الأساليب التي تستخدم في التهديد عبر الشبكة العنكبوتية، وتنوع تلك الأساليب بين تهديدات باغتيال شخصيات سياسية، وتهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل.

سابعاً: تدمير أنظمة المعلومات: تشير إلى محاولة اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وصنع أنواع جديدة من الفيروسات التي تسبب الدمار لأجهزة الكمبيوتر وللمعلومات. (أحمد، 2011، صفحة 54)

2.4. آليات مواجهة التهديدات السيبرانية:

مواجهة التهديدات السيبرانية تتطلب استخدام مجموعة من الآليات المتطورة لضمان حماية الأنظمة الرقمية والمعلومات الحساسة. هذه الآليات تتراوح من التقنيات الحديثة إلى الأساليب التنظيمية والإدارية التي تعمل على تعزيز الدفاعات السيبرانية. وفيما يلي أبرز الآليات المستخدمة في مواجهة التهديدات السيبرانية:

✓ **سياسة أمن المعلومات:** وهي عبارة عن مجموعة من القواعد والقوانين يتم تطبيقها عند التعامل مع المعلومات والتقنيات المرتبطة بها داخل المنشأة، وهي توضح ما هو مسموح به وما لا يسمح به، وهذا يتم من خلال التحقق من الصحة وجدوان الحماية؛ أي تصفية حركة حزم البيانات وسد الثغرات في أنظمة التشغيل كالحوادم والحسابات. بالإضافة إلى سياسة الحماية عبر وضع برمجيات خاصة بمكافحة التجسس وحماية معلومات المواطنين. (البابلي ع.، 2020، صفحة 113)

✓ **تطبيقات الذكاء الاصطناعي في الأمن السيبراني:** يكون عبر:

- **التحقق من الهوية:** يساعد الذكاء الاصطناعي المطورين في رفع فاعلية التقنيات الحيوية وزيادة دقتها.

- **خفض هجمات التصيّد:** يستخدم الذكاء الاصطناعي وتعلّم الآلة في صنع أدوات تحدد وتتابع هجمات التصيّد وتحدّ من حدوثها بطريقة أكثر فاعلية من الإنسان.
- **تحليل السلوك:** تُصمم خوارزميات تعلّم الآلة بطريقة تمكنها من تعلّم سلوك المستخدم وخلق نمط خاص به يستفاد منه في تحليل الهجمات.
- **إدارة الثغرات:** يستخدم الذكاء الاصطناعي وتعلّم الآلة في تقييم الأنظمة بشكل سريع وتحديد نقاط الضعف في الأنظمة والشبكات، وكذلك في تصميم أنظمة استباقية لإدارة الثغرات.
- **أمن الشبكات:** يعمل الذكاء الاصطناعي على تسريع عملية إنشاء السياسات الأمنية وتحديد تصميم شبكات المؤسسات، بالإضافة إلى إدارة عدد كبير من الأجهزة وتحديثها وتصحيح الأمان فيها تلقائياً (السيبراني، 2021).

- ✓ **أتمتة مهام الأمان:** يساعد التعلم الآلي على تحسين الأمن السيبراني من خلال أتمتة المهام المتكررة، مثل المراقبة والاستجابة للتنبيهات الأمنية؛ وبالتالي يكون هناك المزيد من الوقت للفرق الأمنية للتركيز على المهام الأكثر تعقيداً.
- ✓ **تعزيز الكشف عن التهديدات:** يُستخدم التعلم الآلي في تحديد الأنماط في البيانات التي قد تشير إلى تهديد محتمل، إذ تحلل هذه التقنية مجموعات كبيرة من البيانات، ومن ثم تستطيع الكشف عن الحالات الشاذة التي يمكن أن تكون مؤشراً على هجوم أو احتيال، وهو ما يزيد من احتمالية التصدي لتلك التهديدات بسرعة أكبر.
- ✓ **تعزيز الكشف عن البرامج الضارة:** فمن خلال التعلم الآلي، يمكن تحليل كميات هائلة من البيانات والتي تتيح اكتشاف البرامج الضارة الجديدة وغير المعروفة بسرعة وإزالتها من الأنظمة.
- ✓ **اكتشاف برامج الفدية:** برامج الفدية هي أحد البرامج الضارة التي تشقّر ملفات الضحية، وترهن فك هذا التشفير بدفع فدية؛ ومن خلال التعلم الآلي تستطيع الروبوتات اكتشاف برامج الفدية قبل أن تقوم بتشفير ملفات الضحية، كما يمكنها التعرف على النشاط الضار وإيقافه.
- ✓ **الحماية من التصيد الاحتيالي:** والمقصود منه رسائل البريد الإلكتروني التي يتلقاها الضحية ويظن أن مصدرها موثوق، وعند فتحها يفاجأ بسرقة هويته أو اختراق بياناته. ويساعد التعلم الآلي على تحديد رسائل البريد الإلكتروني غير المرغوب فيها وتصنيفها، واكتشاف رسائل التصيّد فيها وحظرها قبل وصولها إلى المستخدم.
- ✓ **تقليل أعباء وتكاليف تكنولوجيا المعلومات:** تساعد قدرات أتمتة التعلم الآلي على تقليل الوقت الذي يستغرقه توزيع التحديثات الأمنية واستكمال اختبارات الاختراق وأجهزة المراقبة، وهو ما يوفر الوقت لدى فرق تكنولوجيا المعلومات للتركيز على قضايا الأمان الأكثر إلحاحاً.

✓ **تسجيل مخاطر الشبكة:** تُستخدم خوارزميات التعلم الآلي في تحليل مجموعات بيانات الهجمات الإلكترونية السابقة وتحديد مناطق الشبكات التي شاركت في هجمات معينة، وهو ما يمكن من تحديد تأثير الهجوم فيما يتعلق بمنطقة شبكة معينة، وبالتالي تستطيع المنظمات تقليل فرص التعرض لهجمات أخرى. (بكه، 2025)

3.4. تأثير الذكاء الاصطناعي على مستقبل الأمن السيبراني:

يمكننا النظر في مستقبل العلاقة بين الذكاء الاصطناعي والأمن السيبراني في ضوء التطور السريع للبنية التحتية السيبرانية، التي أصبحت أحد العوامل الرئيسة التي تحدد توازنات القوة في البيئة الاستراتيجية الرقمية. يشكل الذكاء الاصطناعي عنصراً حاسماً بفضل الإمكانيات الواسعة التي يوفرها، حيث يتطور بشكل مستمر وبمعدل متسارع. ومع زيادة تعقيد الجيوش وتطور تقنياتها، يبرز فجوة واضحة في القدرة على مواكبة الابتكارات والأنظمة الجديدة، مما يخلق تحديات كبيرة في الحفاظ على التكافؤ التكنولوجي في هذا المجال.

تعمل الدول على استهداف واستنزاف الموارد لدولة أخرى؛ لذا فإن مستقبل الحرب السيبرانية مرتبط بمظاهر القوة العصرية في القرن 21م عن طريق قيام دولة أو فواعل من غير الدول بشن هجوم سيبراني في إطار متبادل، هذا التطور النوعي جعل مسارات الحرب السيبرانية أكثر اتساعاً وهذا ما يجعل الدول تسعى إلى كسب أقوى الإمكانيات لمواجهة هذه التهديدات (العلي، 2023، صفحة 248).

مع تزايد الحروب الهجينة التي أصبحت تتجه نحو الاستمرارية كأحد السيناريوهات المحتملة في المستقبل، تعمل القوى الكبرى على إبقاء الحروب غير المتماثلة جزءاً من البيئة الاستراتيجية العالمية. تزداد أهمية هذا التوجه في ظل وجود الإرهاب كمصدر رئيسي للتهديدات، خاصة أن المنظمات والجماعات الإرهابية تفتقر إلى القدرة على تشكيل جيوش نظامية لمواجهة الدول بشكل مباشر. لذلك، تظل الحروب السيبرانية خياراً استراتيجياً فعالاً لهذه الجماعات لمواجهة التهديدات الراهنة، مما يجعل الأمن السيبراني أحد المجالات الحيوية في الصراعات المستقبلية.

هناك سيناريو ثاني وهو البقاء على القوة التقليدية؛ خاصة أن هناك العديد من الدول لا تمتلك القدرات على التحول للقوة السيبرانية بسبب ضعف البنية التكنولوجية. بالإضافة إلى ما يتطلبه الأمن السيبراني من تكلفة مادية عالية وتكوين عالي للعناصر البشرية (شاكر، 2023، صفحة 246).

إن هذا التأثير يطرح العديد من الفرص:

1. **تعزيز اكتشاف التهديدات والوقاية منها:** يمكن للذكاء الاصطناعي تحليل كميات هائلة من البيانات في الوقت الفعلي، وتحديد الشذوذ والأنماط التي تشير إلى التهديدات المحتملة بشكل أسرع بكثير من المحللين البشريين. يمكن أن يؤدي هذا إلى تدابير وقائية أسرع وأكثر فعالية، مما يقلل من تأثير الهجمات الإلكترونية.
2. **التحليلات التنبؤية:** يمكن للذكاء الاصطناعي التعلم من الهجمات السابقة وتحديد نقاط الضعف في الأنظمة قبل استغلالها. ويمكن أن يساعد هذا النهج الاستباقي في منع الهجمات قبل وقوعها.

3. **إضفاء الطابع الديمقراطي على الأمن:** يمكن للأدوات التي تعمل بالذكاء الاصطناعي أن تجعل قدرات الأمن المتطورة في متناول المنظمات والأفراد الأصغر حجمًا الذين قد لا يملكون الموارد اللازمة لحلول الأمن التقليدية. في المقابل نجد أن الذكاء الاصطناعي يخلق العديد من التحديات للأمن السيبراني:

 1. **القدرة على التفسير والشفافية:** يمكن أن تكون خوارزميات الذكاء الاصطناعي معقدة وغير شفافة، مما يجعل من الصعب فهم كيفية اتخاذها لقراراتها. يمكن أن يؤثر هذا الافتقار إلى القدرة على التفسير مخاوف بشأن التحيز والمساءلة وإساءة الاستخدام المحتملة.
 2. **خصوصية البيانات:** يعتمد الذكاء الاصطناعي على كميات كبيرة من البيانات، مما قد يثير مخاوف تتعلق بالخصوصية. يجب على المنظمات ضمان جمع البيانات واستخدامها بشكل مسؤول، والامتثال للوائح ذات الصلة.
 3. **التحديات المتطورة:** يمكن أن يكون الذكاء الاصطناعي فعالاً ضد التهديدات المعروفة، لكن مجرمي الإنترنت يكتفون بتكتيكاتهم باستمرار. يعد الحفاظ على خوارزميات الذكاء الاصطناعي محدثة وقادرة على اكتشاف التهديدات الجديدة تحديًا مستمرًا.
 4. **فجوة المهارات:** يتطلب تنفيذ وإدارة حلول أمان الذكاء الاصطناعي مهارات متخصصة قد تكون نادرة. يعد سد الفجوة بين الأمن السيبراني وخبرة الذكاء الاصطناعي أمرًا بالغ الأهمية للتبني الناجح.
 5. **التكلفة والتعقيد:** يمكن أن تكون حلول الذكاء الاصطناعي مكلفة ومعقدة التنفيذ. يعد العثور على حلول فعالة من حيث التكلفة وسهلة الاستخدام أمرًا ضروريًا للتبني على نطاق واسع (Aldhamer, 2023, pp. 16,17).

يعتبر الاتجاه نحو تعزيز القدرات الأمنية للدول عاملاً حاسماً في تحقيق الأمن الشامل، وخاصة في ظل التحديات المتزايدة التي تطرأ على مستوى العالم في العصر الرقمي. في السنوات الأخيرة، أصبح من الواضح أن تهديدات الأمن السيبراني تتزايد بشكل سريع ومعقد، بما في ذلك الهجمات الإلكترونية المتقدمة، والتجسس الرقمي، والقرصنة على البنى التحتية الحيوية، مما يهدد استقرار الدول في العديد من المجالات. هذا التزايد في المخاطر يدفع الدول إلى تعزيز قدراتها الأمنية بشكل شامل، مع التركيز على حماية المعلومات الرقمية والأنظمة الحساسة.

5. الخاتمة:

إن الذكاء الاصطناعي والأمن السيبراني مترابطان ومكملان بعضهما البعض؛ مما يجعل العمل على هذين المجالين أمراً حتمياً لا مفر منه. فالحروب الهجينة أصبحت جزءاً من التهديدات اللاتماثلية حيث تستخدم المسيرات والطائرات بدون طيار مما يقلل التكلفة مقارنة بالحروب التقليدية. لا بد من ضرورة الاستثمار في هذا المجال حتى يمكن مواكبة التهديدات المستقبلية.

الذكاء الاصطناعي يلعب اليوم دوراً محورياً في هذه المعركة من خلال قدراته في تحسين استراتيجيات الأمن السيبراني وتطوير حلول لمكافحة التهديدات الرقمية. فعلى سبيل المثال، يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات بسرعة فائقة، مما يساعد في اكتشاف الأنماط السلوكية المشبوهة والتصدي للهجمات في مراحل مبكرة. كما يمكن استخدامه لتطوير أنظمة دفاع ذكية تتمتع بالقدرة على التكيف مع الأساليب الهجومية المتغيرة، مما يجعلها أكثر فعالية في التصدي للهجمات المستمرة والمعقدة.

تعتبر هذه التحولات في مجال التكنولوجيا الأمنية جزءاً من الاستراتيجيات الوطنية الحديثة، حيث تتبنى الدول تقنيات الذكاء الاصطناعي بشكل موسع لبناء قدرات سيبرانية رادعة. لا تقتصر هذه القدرات على الأبعاد العسكرية فقط، بل تشمل أيضاً القطاعين الاقتصادي والاجتماعي، حيث أن أية هجمات سيبرانية قد تؤثر على الأنظمة المالية أو شبكات الطاقة أو القطاع الصحي. بالتالي، فإن تعزيز القدرات الأمنية باستخدام الذكاء الاصطناعي يعد بمثابة حجر الزاوية لحماية الدول من التحديات المعقدة في العالم الرقمي.

علاوة على ذلك، فإن تعزيز القدرات الأمنية بهذه الطريقة يتطلب من الدول استثمار الموارد في التعليم والتدريب وتطوير الكوادر البشرية المتخصصة في هذه المجالات. فتكنولوجيا الذكاء الاصطناعي تقدم حلولاً متطورة، لكن الأمر يتطلب فرقاً من المحترفين المدربين بشكل جيد لاستخدام هذه الأدوات في التصدي للتهديدات الأمنية المتطورة.

وفي الأخير يتوجب على الدول والمنظمات الاستثمار بشكل أكبر في الذكاء الاصطناعي وتطوير استراتيجيات أمنية متكاملة تواكب التحديات المتزايدة في الفضاء السيبراني. إن الذكاء الاصطناعي ليس مجرد أداة مساعدة، بل أصبح عنصراً أساسياً لتحقيق الأمن السيبراني المستدام، والذي يعد أحد الركائز الأساسية للحفاظ على الاستقرار الرقمي في المستقبل.

6. قائمة المراجع:

1. إدريس عطية. (2019). تطبيقات الهندسة الامنية في سياسة الجزائر الافريقية. الجزائر: دار الامة.
2. المركز السعودي للأمن السيبراني. (2021، 2610). تطبيقات الذكاء الاصطناعي للأمن السيبراني. تم الاسترداد من المركز السعودي للأمن السيبراني: https://cert.gov.sa/ar/awareness/ai_applications_in_cybersecurity/
3. ايهاب خليفة. (2024). الخوارزميات القاتلة للعلاقات الدولية في عصر الذكاء الاصطناعي. القاهرة: العربي للنشر والتوزيع.
4. بكه. (501، 2025). الذكاء الاصطناعي والامن السيبراني. تم الاسترداد من بكة: <https://bakkah.com/ar/knowledge-center>
5. ذياب بن عمر. (2024). تطبيقات الذكاء الاصطناعي في البحوث العلمية الفرص والتحديات منصة سكوبوت نموذجاً. تأليف يوف بن يزة، البحث العلمي في عصر الذكاء الاصطناعي (صفحة 154). باتنة: مخبر الامن الانساني.
6. زياد كيلاي. (2024). الابعاد النظرية والتاريخية للذكاء الاصطناعي. تأليف دلال محمود، تكنولوجيا الذكاء الاصطناعي وتحولات القوة العالمية (الصفحات 12-25). القاهرة: المركز المصري للفكر والدراسات الاستراتيجية.
7. سميرة، ب. (2017، 07). الامن السيبراني في الجزائر. المجلة الجزائرية للأمن الإنساني (04).
8. شادي عبد الوهاب منصور. (2019). حروب الجيل الخامس. القاهرة: العربي للنشر والتوزيع.
9. عادل عبد الصادق. (2024). الابعاد الامنية والعسكرية لتطبيقات الذكاء الاصطناعي بين الفرص والتحديات. تأليف دلال محمود، تكنولوجيا الذكاء الاصطناعي وتحولات القوة العالمية (الصفحات 77-119). القاهرة: المركز المصري للفكر والدراسات الاستراتيجية.
10. عبد الله الهاشمي. (2023). الامن ومواجهة التهديدات الكبرى. ابوظبي: مركز تريندز للبحوث والاستشارات.
11. علي احمد عباس. (2021). التعددية القطبية من منظور القوى الكبرى في عصر الذكاء الاصطناعي. دمشق: الهيئة العامة السورية للكتاب.
12. علي زياد العلمي، وحيد علي حسين. (2023). تكتيكات الحروب الحديثة. القاهرة: العربي للنشر والتوزيع.
13. علي عباس مراد. (2016). الامن والامن القومي مقارنة نظرية. بيروت: دار الروافد الثقافية.
14. عمار ياسر البابلي. (2020). الفضاء الالكتروني التحديات الامنية المعاصرة. القاهرة: معهد البحوث والدراسات العربية.

15. عمار ياسر زهير البابلي. (سبتمبر، 2023). الارهاب والخوارزميات دور الذكاء الاصطناعي في مواجهة العنف والتطرف الرقمي. دراسات استراتيجية ومستقبلية.
16. عمر محمد علي محمد. (2021). حروب الجيل الرابع. القاهرة: الهيئة المصرية العامة للكتاب.
17. فتح الله شيخ. (2023). الذكاء الاصطناعي. القاهرة: الهيئة العامة لقصور الثقافة.
18. فراس جمال شاكر. (2023). الحروب المعلوماتية في المجال الامني والعسكري. القاهرة: العربي للنشر والتوزيع.
19. محمد الجندي. (2023). الامن السيبراني من حروب المعلوماتية الى الجرائم السيبرانية. القاهرة: دار المعارف.
20. مرعي علي الرحيمي. (2023). الحرب السيبرانية. القاهرة: دار الفجر للنشر.
21. منصور عبد الحكيم. (2022). الحرب السيبرانية. القاهرة: دار الفاروق للنشر.
22. هبة الله أحمد. (2011). الارهاب الدولي. الاسكندرية: منشأة المعارف.
23. بمى أحمد شوقي عمران. (2023). الذكاء الاصطناعي والنظام الدولي الاشكاليات والتحديات. القاهرة: معهد البحوث والدراسات العربية.

English References:

1. Aldhamer, M. (2023). The Impact of Artificial Intelligence on the Future of Cybersecurity. Multi-knowledge Electronic Comprehensive Journal for Education and Science Publication (MECSJ), (71), 2616-9185
2. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10), 13-21.
3. Dilek Fraisl, The Potential Of Artificial Intelligence For The Sdgs And Official Statistics, Paris 21, Working Paper Draft For Comments, April 2024.
4. Russell & Norvig, (2023). Artificial Intelligence: Definition and Background. Ed (Sheikh, H., Prins, C., Schrijvers, E) In: Mission AI. Research for Policy. Springer, Cham, p 20. HYPERLINK "https://doi.org/10.1007/978-3-031-21448-6_2" \h https://doi.org/10.1007/978-3-031-21448-6_2
5. Schiliro, F. (2023). Towards a contemporary definition of cybersecurity. arXiv preprint arXiv:2302.02274
6. Steve Wilson. (April 2023) Cybersecurity and Artificial Intelligence: Threats and Opportunities, Contrast Security.