Volume (26), No. (2B) , e2026567 - (27/08/2026)

Artificial Intelligence in the Service of CybersecurityTechnical, Security, and Strategic Dimensions

الذكاء الاصطناعي في خدمة الأمن السيبراني: الأبعاد التقنية والأمنية والاستراتيجية

Abdulrahman Bubishate
Faculty of Business Administration, Jinan University, Lebanese Republic
rhman_bubishate@yahoo.com

*(Corresponding author) e-mail: rhman_bubishate@yahoo.com

الملخّص

تتجلى مشكلة البحث في الحاجة إلى فهم علمي عميق للعلاقة بين الذكاء الاصطناعي والأمن السيبراني، والإجابة عن تساؤل جوهري مفاده كيف يمكن توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني، مع الحد من مخاطره وتهديداته المحتملة؟ يهدف هذا البحث إلى تحقيق مجموعة من الأهداف العلمية، من أهمها: توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، تحليل دور الذكاء الاصطناعي في تعزيز منظومات الأمن السيبراني، إبراز المخاطر والتهديدات السيبرانية المرتبطة باستخدام الذكاء الاصطناعي.
من اهم نتائج البحث هي أن الذكاء الاصطناعي أصبح عنصرًا محوريًا في منظومات الأمن السيبراني الحديثة في كشف التهديدات السيبرانية وتحليلها والاستجابة لها، عجز الأساليب التقليدية للأمن السيبراني عن مواجهة التهديدات المتقدمة، إسهام الذكاء الاصطناعي في الانتقال من الأمن التفاعلي إلى الأمن الاستباقي، كما أنه لا تقتصر تحديات توظيف الذكاء الاصطناعي على الجوانب التقنية فقط بل تمتد إلى أبعاد أخلاقية وتشريعية وتنظيمية، بالإضافة إلى أن العنصر البشري يشكّل أحد أهم نقاط الضعف في منظومات الأمن السيبراني، وتزايد ارتباط الأمن السيبراني بالأمن القومي للدول.

ABSTRACT

The research problem lies in the need for a deep scientific understanding of the relationship between artificial intelligence and cybersecurity, and in answering a fundamental question: How can artificial intelligence be employed to enhance cybersecurity, while reducing its risks and potential threats? This research aims to achieve a set of scientific objectives, the most important of which are: clarifying the conceptual framework of artificial intelligence and cybersecurity, analyzing the role of artificial intelligence in enhancing cybersecurity systems, highlighting the cyber risks and threats associated with the use of artificial intelligence.
One of the most important findings of the research is that artificial intelligence has become a pivotal element in modern cybersecurity systems in detecting, analyzing and responding to cyber threats, the inability of traditional cybersecurity methods to confront advanced threats, and the contribution of artificial intelligence in the transition from reactive to proactive security.
Moreover, the challenges of employing artificial intelligence are not limited to technical aspects only, but extend to ethical, legislative and regulatory dimensions. In addition, the human element constitutes one of the most important weaknesses in cybersecurity systems, and cybersecurity is increasingly linked to the national security of countries.

Article history:

Submission ID: 567

Submission Date: 19/01/2026

Reviewing Date: 16/02/2026

Acceptance Date: 26/02/2026

Publishing Date: 27/08/2026

DOI: 10.6520/jrs.v26i2.567

Keywords:

الكلمات المفتاحية: الهجمات السيبرانية، التعلم الآلي، أمن المعلومات ,
Keywords: Cyberattacks, Machine Learning, Information Security.

Cite as:

Bubishate, A. (2026) Artificial Intelligence in the Service of CybersecurityTechnical, Security, and Strategic Dimensions. Jersah for Research and Studies 26 (2B). https://doi.org/10.6520/jrs.v26i2.567e2026567

الذكاء الاصطناعي في خدمة الأمن السيبراني الأبعاد التقنية والأمنية والاستراتيجية

عبدالرحمن صالح عبدالرحمن بوبشيت

كلية إدارة الأعمال، جامعة الجنان، الجمهورية اللبنانية

المؤلف المراسل: عبدالرحمن صالح عبدالرحمن بوبشيت، rhman_bubishate@yahoo.co

الملخص

تتجلى مشكلة البحث في الحاجة إلى فهم كيف يمكن توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني، وتكمن الأهمية العلمية للبحث في كونه يسهم في إثراء الأدبيات العربية في مجال الذكاء الاصطناعي والأمن السيبراني وهما مجالان يعانيان من ندرة الدراسات المتخصصة التي تجمع بين الجانبين النظري والتطبيقي في إطار تحليلي متكامل، والأهمية التطبيقية من حيث تطوير استراتيجيات فعالة للأمن السيبراني المدعوم بالذكاء الاصطناعي. اعتمد هذه البحث على المنهج الوصفي، من خلال وصف الظاهرة محل الدراسة، وتحليل أبعادها. يهدف هذا البحث إلى توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، تحليل دور الذكاء الاصطناعي في تعزيز منظومات الأمن السيبراني، وإبراز المخاطر والتهديدات السيبرانية المرتبطة باستخدام الذكاء الاصطناعي. من اهم النتائج، هي أن الذكاء الاصطناعي أصبح عنصرًا محوريًا في منظومات الأمن السيبراني في كشف التهديدات السيبرانية وتحليلها والاستجابة لها، إسهام الذكاء الاصطناعي في الانتقال من الأمن التفاعلي إلى الأمن الاستباقي، وأن العنصر البشري يشكّل أحد أهم نقاط الضعف في منظومات الأمن السيبراني، وتزايد ارتباط الأمن السيبراني بالأمن القومي للدول.

الكلمات المفتاحية: الهجمات السيبرانية، التعلم الآلي، أمن المعلومات.

Artificial Intelligence in the Service of Cybersecurity Technical, Security, and Strategic Dimensions

Abdulrahman Saleh Abdulrahman Bubishate

Faculty of Business Administration, Jinan University, Lebanese Republic

Corresponding Author: Abdulrahman Saleh Abdulrahman Bubishate, rhman_bubishate@yahoo.com

Abstract

The research problem is manifested in the need to understand how artificial intelligence can be employed in enhancing cybersecurity. The scientific importance of the research lies in the fact that it contributes to enriching Arabic literature in the field of artificial intelligence and cybersecurity, two fields that suffer from a scarcity of specialized studies that combine the theoretical and applied aspects in an integrated analytical framework. The practical importance lies in the development of effective strategies for cybersecurity supported by artificial intelligence. This research adopts a descriptive approach, describing the phenomenon under study and analyzing its dimensions. It aims to clarify the conceptual framework of artificial intelligence and cybersecurity, analyze the role of AI in enhancing cybersecurity systems, and highlight the cyber risks and threats associated with the use of AI.

One of the most important results is that artificial intelligence has become a pivotal element in cybersecurity systems in detecting, analyzing and responding to cyber threats, contributing to the transition from reactive to proactive security, and that the human element constitutes one of the most important weaknesses in cybersecurity systems, and the increasing connection between cybersecurity and national security of countries.

Keywords: Cyberattacks, Machine Learning, Information Security.

المقدمة

يشهد العالم في العقود الأخيرة تحولًا رقميًا متسارعًا، رافقه اعتماد متزايد على التقنيات الذكية في مختلف مجالات الحياة، وعلى رأسها تقنيات الذكاء الاصطناعي التي أصبحت عنصرًا محوريًا في تطوير الأنظمة الرقمية وتحسين كفاءتها، وقد أسهم هذا التطور في إحداث نقلة نوعية في أساليب إدارة البيانات، واتخاذ القرار، وأتمتة العمليات، بما في ذلك المجالات الأمنية والعسكرية والاقتصادية، وفي المقابل، أدى هذا التحول الرقمي المتسارع إلى بروز تحديات أمنية غير مسبوقة، تمثلت في تصاعد التهديدات السيبرانية من حيث التعقيد والتنوع والقدرة على التخفي، مما جعل النماذج التقليدية للأمن المعلوماتي (Information Security) عاجزة عن مواجهة كثير من هذه التهديدات، ولم تعد الهجمات السيبرانية (Cyber Attacks) تقتصر على الاختراق المباشر للأنظمة، بل امتدت لتشمل الهندسة الاجتماعية، والتصيّد الاحتيالي، وانتحال الهويات الرقمية، والتلاعب بالمعلومات، وصولًا إلى تهديد الأمن القومي للدول.

في هذا السياق، برز الذكاء الاصطناعي بوصفه سلاحًا ذا حدين ، كد خبراء متخصصون في التكنولوجيا، أن الذكاء الاصطناعي يمثل سلاحاً ذا حدين، حيث يجمع بين الإمكانيات الكبيرة والمخاطر المحت ملة، ما يتطلب توجيهاً ورقابة فعالة لضمان تحقيق أهدافه والفوائد المرجوة وتقليل الآثار السلبية(1)، فمن جهة، يُستخدم كأداة فعالة لتعزيز الأمن السيبراني عبر الكشف المبكر عن التهديدات، وتحليل السلوك الشاذ، والتنبؤ بالهجمات قبل وقوعها، ومن جهة أخرى، أصبح هو نفسه هدفًا للهجمات، وأداة بيد الجهات الخبيثة لتنفيذ هجمات أكثر تطورًا وذكاءً، وانطلاقًا من هذا كله، يأتي هذا البحث ليتناول دور الذكاء الاصطناعي في خدمة الأمن السيبراني، من خلال تحليل أبعاده النظرية والتطبيقية، وبيان مخاطره وتحدياته، في إطار علمي يجمع بين البعدين الدفاعي والهجومي، وبما ينسجم مع التحولات الرقمية المعاصرة، وتوضيح مفهوم الذكاء الاصطناعي، وما هي أبرز تقنياته المستخدمة في المجال الأمني، وما هو المقصود بالأمن السيبراني، وما طبيعة التهديدات؟ وكيف يُستخدم الذكاء الاصطناعي في تعزيز قدرات الكشف والاستجابة للتهديدات السيبرانية؟ بالإضافة إلى أبرز المخاطر الأمنية المرتبطة باستخدام الذكاء الاصطناعي، لمعرفة التحديات التقنية والتنظيمية والأخلاقية التي تواجه توظيف الذكاء الاصطناعي في الأمن السيبراني.

تتمثل مشكلة البحث في التناقض الظاهر بين توظيف تقنيات الذكاء الاصطناعي في الأنظمة الرقمية، وبين المخاطر والتهديدات السيبرانية التي تستهدف هذه الأنظمة، كما أن غياب الأطر التنظيمية الموحدة، ونقص الكفاءات المتخصصة، وضعف الوعي الأمني، يزيد من هذه المشكلة. تكمن أهمية البحث في عدة جوانب منهت الأهمية العلمية حيث تنبع من كونه يسهم في إثراء الأدبيات العربية في مجال الذكاء الاصطناعي والأمن السيبراني، والأهمية التطبيقية حيث يكتسب البحث أهميته التطبيقية في تطوير استراتيجيات فعالة للأمن السيبراني المدعوم بالذكاء الاصطناعي. اعتمد هذه البحث على المنهج الوصفي، من خلال وصف الظاهرة محل الدراسة، وتحليل أبعادها المختلفة. يهدف هذا البحث إلى تحقيق مجموعة من الأهداف العلمية، من أهمها: توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، تحليل دور الذكاء الاصطناعي في تعزيز منظومات الأمن السيبراني، إبراز المخاطر والتهديدات السيبرانية المرتبطة باستخدام الذكاء الاصطناعي. تم استعراض بعض التقارير العلمية ذات الصلة والدراسات العربية والأجنبية السابقة للمناقشة حول موقع الدراسة الحالية منها. منهجية البحث اعتمدت على المنهج الوصفي، كما تمت الاستعانة بالمنهج التحليلي المقارن عند الحاجة.

من اهم نتائج البحث هي أن الذكاء الاصطناعي أصبح عنصرًا محوريًا في منظومات الأمن السيبراني الحديثة، ولم يعد دوره تكميليًا أو ثانويًا في كشف التهديدات السيبرانية وتحليلها والاستجابة لها، عجز الأساليب التقليدية للأمن السيبراني عن مواجهة التهديدات المتقدمة التي تتسم بالسرعة والتعقيد والتكيف المستمر، إسهام الذكاء الاصطناعي في الانتقال من الأمن التفاعلي إلى الأمن الاستباقي من خلال تحليل السلوكيات، التنبؤ بالهجمات، والكشف المبكر عن الحوادث الأمنية. لا تقتصر تحديات توظيف الذكاء الاصطناعي على الجوانب التقنية فقط، بل تمتد إلى أبعاد أخلاقية وتشريعية وتنظيمية، تتعلق بالخصوصية، والتحيز الخوارزمي، والمساءلة،

وحوكمة البيانات، كما أن العنصر البشري يشكّل أحد أهم نقاط الضعف في منظومات الأمن السيبراني سواء من حيث نقص الكفاءات المتخصصة أو ضعف الوعي الأمني. يتزايد ارتباط الأمن السيبراني بالأمن القومي للدول في ظل اعتماد البنى التحتية الحيوية على الأنظمة الرقمية والذكية. تناول البحث الحاجة إلى فهم علمي عميق للعلاقة بين الذكاء الاصطناعي والأمن السيبراني، والإجابة عن تساؤل جوهري مفاده: كيف يمكن توظيف الذكاء الاصطناعي في تعزيز الأمن السيبراني، مع الحد من مخاطره وتهديداته المحتملة؟

مشكلة البحث

على الرغم من الجهود المبذولة لتطوير أنظمة أمن سيبراني ذكية، إلا أن الواقع العملي يشير إلى استمرار تعرض المؤسسات الحكومية والخاصة لهجمات سيبرانية متقدمة، بعضها يعتمد على تقنيات الذكاء الاصطناعي في التخفي والتكيف وتجاوز أنظمة الحماية، لذا، تتمثل مشكلة البحث في:

1) التناقض الظاهر بين التوسع الكبير في توظيف تقنيات الذكاء الاصطناعي في الأنظمة الرقمية، وبين تصاعد المخاطر والتهديدات السيبرانية التي تستهدف هذه الأنظمة، سواء من خلال استغلال الذكاء الاصطناعي ذاته أو من خلال استهداف نماذجه وخوارزمياته.
2) غياب الأطر التنظيمية الموحدة.
3) نقص الكفاءات المتخصصة.
4) ضعف الوعي الأمني، يزيد من حدة هذه المشكلة.
5) الحاجة إلى فهم علمي عميق للعلاقة بين الذكاء الاصطناعي والأمن السيبراني.

أهمية البحث

أولًا) الأهمية العلمية: تنبع الأهمية العلمية للبحث من كونه يسهم في إثراء الأدبيات العربية في مجال الذكاء الاصطناعي والأمن السيبراني، وهو مجال ما يزال يعاني من ندرة الدراسات المتخصصة التي تجمع بين الجانبين النظري والتطبيقي في إطار تحليلي متكامل.

ثانيًا) الأهمية التطبيقية: يكتسب البحث أهميته التطبيقية من خلال ما يقدمه من رؤى يمكن أن تستفيد منها المؤسسات الحكومية والخاصة، وصناع القرار، والجهات الأكاديمية، في تطوير استراتيجيات فعالة للأمن السيبراني المدعوم بالذكاء الاصطناعي.

أهداف البحث

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف العلمية، من أهمها:

1. توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني.
2. تحليل دور الذكاء الاصطناعي في تعزيز منظومات الأمن السيبراني.
3. إبراز المخاطر والتهديدات السيبرانية المرتبطة باستخدام الذكاء الاصطناعي.
4. رصد الفجوات البحثية في الدراسات السابقة لسد فجوة بحثية في الأدبيات العربية من خلال معالجة موضوع حديث بمنهج علمي.
5. تقديم نتائج وتوصيات تسهم في تطوير السياسات الأمنية الرقمية.

الدراسات السابقة

أولا) الدراسات العربية

دراسة المهندي، آمال، (2025)(2)، بعنوان: العصر الرقمي: الأمن السيبراني في عصر الذكاء الاصطناعي، اشارت إلى أنه في العصر الحديث، أصبح الذكاء الاصطناعي جزءًا لا يتجزأ من حياتنا اليومية، حيث يُستخدم في مجالات متعددة مثل الرعاية الصحية،

النقل، والتجارة، ومع ذلك، تزداد التحديات المتعلقة بالأمن السيبراني، حيث تتطور التهديدات بشكل متسارع. بينت الدراسة أهمية الأمن السيبراني مع زيادة الاعتماد على الذكاء الاصطناعي، وانه أصبح من الضروري حماية البيانات والمعلومات الحساسة بما في ذلك حماية البيانات الشخصية، حماية الأنظمة الحيوية، وحماية الشركات، وخلصت بأن المؤسسات تحتاج إلى تبني استراتيجيات فعالة لمواجهة التهديدات، منها: التدريب والتوعية، تطبيق بروتوكولات الأمان، ومراقبة الأنظمة واكتشاف الأنشطة المشبوهة.

وأشارت دراسة الحجرف، حسن، (2024)(3)، إلى استكشاف تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني والتحديات المرتبطة بها. توصلت النتائج إلى أن الذكاء الاصطناعي يحسن كفاءة استراتيجيات الأمن السيبراني من خلال التنبؤ بالتهديدات والاستجابة السريعة، مع التأكيد على ضرورة تدريب الموارد البشرية وتطوير إطار قانوني وأخلاقي لاستخدام هذه التكنولوجيا بشكل فعال.

هدفت دراسة الهنائي، علي، (2024)(4)، بعنوان: تطبيقات الذكاء الاصطناعي في المجال الأمني، إلى التعرف على واقع تطبيقات الذكاء الاصطناعي في المجال الأمني الحالي بدول مجلس التعاون لدول الخليج العربية، والتحديات. هدفت الدراسة كذلك إلى معرفة الآفاق المستقبلية لتوظيف تقنيات الذكاء الاصطناعي في المجال الأمني. أظهرت نتائج الدراسة أن واقع تطبيقات الذكاء الاصطناعي جاء بدرجة متوسطة، وجات الآفاق المستقبلية لتوظيف تطبيقات الذكاء الاصطناعي في المجال الأمني بدول مجلس التعاون الخليجي جاءت بدرجة مرتفعة، وهذا مؤشر للجاهزية والاستعداد الذي تبذله حكومات دول المجلس لاستخدام هذه التقنيات. خرجت الدراسة ببعض التوصيات من أبرزها سن التشريعات من قوانين ولوائح تنظيمية تؤطر استخدام تطبيقات الذكاء الاصطناعي وتوظيفها في المجالات المختلفة، وإنشاء إدارات وكليات ومعاهد متخصصة بالذكاء الاصطناعي تقوم بتدريب الكوادر الأمنية على استخدام تطبيقات الذكاء الاصطناعي في المجال الأمني، بالإضافة إلى عمل دليل لتطبيقات الذكاء الاصطناعي في المجال الأمني بدول مجلس التعاون الخليجي، يضم معايير تطبيقات الذكاء الاصطناعي في المجال الأمني.

دراسة يوسف، أحمد، (2021)(5)، بينت أهمية تطبيق الذكاء الاصطناعي في تعزيز أمن المعلومات بالقطاع الخدمي، وهدفت إلى إبراز دور الذكاء الاصطناعي في تعزيز أمن المعلومات في قطاع الخدمات، في ضوء الثورة الصناعية الرابعة والتوجه نحو الرقمنة. توصلت الدراسة إلى عدد من النتائج، أهمها وجود علاقة بين علم الخدمات والذكاء الاصطناعي، حيث يساهم كلاهما في حماية المعلومات، كما تم تقديم مجموعة من التوصيات، أهمها ضرورة تعزيز أمن المعلومات في مؤسسات قطاع الخدمات على وجه الخصوص، وفي مختلف القطاعات العامة، من خلال تبني تقنية الذكاء الاصطناعي.

ثانيًا) الدراسات الأجنبية

سلّطت دراسة (Williams, R. & Caldwell, D, 2022)(6) الضوء على الذكاء الاصطناعي بوصفه عنصرًا استراتيجيًا في الأمن القومي، معتبرة أن السيطرة على تقنيات الذكاء الاصطناعي تمثل أحد محددات القوة في النظام الدولي المعاصر، لا سيما في ظل تصاعد الحروب السيبرانية.

تناولت دراسة (Brundage, M. et al, 2018)(7) الأبعاد المزدوجة للذكاء الاصطناعي، حيث بيّنت أن التقنيات نفسها التي تُستخدم في الدفاع السيبراني يمكن توظيفها في تطوير هجمات سيبرانية أكثر تعقيدًا، مثل الهجمات التكيفية وهجمات الهندسة الاجتماعية الذكية. تم استعراض مشهد التهديدات الأمنية المحتملة الناجمة عن الاستخدامات الضارة لتقنيات الذكاء الاصطناعي واقتراح طرقًا لتحسين التنبؤ بهذه التهديدات ومنعها والتخفيف من آثارها.

ناقشت دراسة (Goodfellow et al., 2016)(8) مفهوم الهجمات العدائية (Adversarial Attacks) التي تستهدف أنظمة الذكاء الاصطناعي نفسها، محذّرة من الاعتماد المطلق على النظم الذكية دون تعزيزها بضوابط أمنية متعددة المستويات.

ثالثًا: المناقشة حول موقع الدراسة الحالية من الدراسات السابقة

تتميّز هذه الدراسة بالإضافة العلمية عن الدراسات السابقة في جوانب، من أبرزها:

1. الجمع بين الأبعاد التقنية والأمنية والاستراتيجية في إطار تحليلي.
2. تقديم رؤية نقدية لاستخدام الذكاء الاصطناعي بوصفه أداة دفاعية وهجومية في آن واحد.
3. سد فجوة بحثية في الأدبيات العربية من خلال معالجة موضوع حديث بمنهج علمي.
4. التركيز على الانعكاسات الاستراتيجية لاستخدام الذكاء الاصطناعي في الأمن السيبراني على مستوى الدول والمؤسسات.

منهجية البحث

اعتمد هذه البحث على المنهج الوصفي، من خلال وصف الظاهرة محل الدراسة، وتحليل أبعادها المختلفة، والاستفادة من الدراسات السابقة والتقارير العلمية ذات الصلة، كما تمت الاستعانة بالمنهج التحليلي المقارن عند الحاجة، للمقارنة بين الاتجاهات البحثية المختلفة.

الإجراءات المنهجية للبحث

حدود البحث

الحدود المكانية: يتناول البحث موضوع الذكاء الاصطناعي والأمن السيبراني في إطار عام، مع الإشارة إلى السياقات الإقليمية والدولية ذات الصلة.

الحدود الزمانية: ان التطورات السريعة بموضوع البحث تحتم تحديد فترة زمنية محددة لتناوله، لذا، سيشمل هذا البحث التطورات البحثية والتطبيقية من نشأة الأمن السيبراني في سبعينات القرن الماضي بالتزامن مع استخدام أجهزة الحاسوب واتصالها بالإنترنت وظهور الذكاء الاصطناعي حتى نهاية عام 2024م.

الحدود الموضوعية: اقتصر البحث على الجوانب النظرية والتطبيقية المرتبطة بتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني، دون التوسع في التطبيقات الأخرى.

الجانب النظري للدراسة

أولا) الإطار النظري للذكاء الاصطناعي

1) نشأة الذكاء الاصطناعي وتطوره التاريخي: يُعد الذكاء الاصطناعي أحد أبرز مخرجات الثورة الرقمية المعاصرة، وقد ارتبط ظهوره المبكر بمحاولات الإنسان محاكاة القدرات العقلية البشرية باستخدام الآلة، ويرتبط ارتباطًا وثيقًا بعلم البيولوجيا المعرفية، الذي يدرس الأسس البيولوجية للإدراك والتفكير(9). تعود البدايات النظرية للذكاء الاصطناعي إلى منتصف القرن العشرين، حينما طُرحت تساؤلات جوهرية حول إمكانية جعل الآلات "تفكر" أو "تتعلّم"، وكان من أوائل من أسهموا في هذا المجال عالم الحاسوب البريطاني "*آلان تورنغ*"، الذي قدّم عام 1950 اختبارًا شهيرًا عُرف بـ "*اختبار تورنغ*"، لقياس قدرة الآلة على محاكاة السلوك الذكي للإنسان(10).

في عام 1956، عُقد مؤتمر "*دارتموث*" الذي يُعد نقطة الانطلاق الرسمية لمصطلح "*Artificial Intelligence*"، حيث اجتمع عدد من الباحثين الذين افترضوا إمكانية توصيف كل جانب من جوانب التعلم أو الذكاء بحيث يمكن للآلة محاكاته(11). ومنذ ذلك الحين، شهد مجال الذكاء الاصطناعي مراحل متعددة من التطور، تخللتها فترات ازدهار وأخرى من التراجع عُرفت بـ "*شتاء الذكاء الاصطناعي*"، نتيجة محدودية القدرات الحاسوبية وضعف البيانات المتاحة آنذاك، ومع مطلع القرن الحادي والعشرين، شهد الذكاء الاصطناعي طفرة غير مسبوقة(12). مدفوعة بثلاثة عوامل رئيسة: تطور القدرات الحاسوبية، توافر كميات ضخمة من البيانات، والتقدم الكبير في خوارزميات التعلم الآلي والتعلم العميق. وقد أسهم في تطوير نماذج قادرة على التكيف مع البيئات المتغيرة واكتشاف الأنماط الخفية داخل البيانات المعقدة(13)، والانتقال الذكاء الاصطناعي من الإطار النظري إلى التطبيقات العملية في مختلف القطاعات، ومنها المجال الأمني.

2) مفهوم الذكاء الاصطناعي وخصائصه: يُعرّف الذكاء الاصطناعي بأنه فرع من علوم الحاسوب يهدف إلى تصميم أنظمة وبرامج قادرة على محاكاة السلوك الذكي للبشر، مثل التعلم، والاستدلال، واتخاذ القرار، والتعرّف على الأنماط، وقد حاول الباحثون محاكاة آليات التعلم واتخاذ القرار لدى الإنسان من خلال نماذج حسابية مستوحاة من عمل الخلايا العصبية(14)، ويقوم الذكاء الاصطناعي على مجموعة من الخصائص الأساسية، من أبرزها:

1. القدرة على التعلم: من خلال تحليل البيانات واستخلاص الأنماط.
2. القدرة على التكيف: تعديل السلوك بناءً على المعطيات الجديدة.
3. الاستقلالية النسبية: اتخاذ قرارات دون تدخل بشري مباشر.
4. السرعة والكفاءة: معالجة كميات هائلة من البيانات في وقت قصير.

وتُعد هذه الخصائص من العوامل التي جعلت الذكاء الاصطناعي أداة فعالة في المجالات التي تتطلب استجابة سريعة وتحليلًا معقدًا وعلى رأسها الأمن السيبراني. أصبحت الأنظمة الذكية قادرة على تقليد سلوكيات بشرية معقدة، مثل التفاعل اللغوي والتعرف على المشاعر، الأمر الذي أثار تساؤلات أخلاقية وأمنية عميقة، خاصة عند استخدام هذه التقنيات في المجالات الحساسة(15).

3) أنواع الذكاء الاصطناعي (16): يمكن تصنيف الذكاء الاصطناعي إلى عدة أنواع وفقًا لمستوى قدراته، كما يصنف تقنياً إلى آلات تفاعلية، ذاكرة محدودة، نظرية العقل، والوعي الذاتي، ومن أبرز هذه التصنيفات:

أ. الذكاء الاصطناعي الضيق (Narrow AI)(17): هو النوع الأكثر شيوعًا حاليًا، ويُستخدم لأداء مهام محددة مثل التعرف على الصور، وتحليل النصوص، وكشف التهديدات السيبرانية. يتميّز هذا النوع بكفاءته العالية في نطاق محدد، لكنه يفتقر إلى الفهم العام، وهو نوع من أنواع الذكاء الاصطناعي، يتم فيه تصميم خوارزمية التعلم لأداء مهمة واحدة، وأي معرفة مكتسبة من أداء هذه المهمة لن يتم تطبيقها تلقائياً على مهام أخرى .تم تصميم الذكاء الاصطناعي الضيق لإكمال مهمة واحدة بنجاح دون مساعدة بشرية(18).

ب. الذكاء الاصطناعي العام (AGI: Artificial general intelligence): هو ذكاء افتراضي يُفترض أن يمتلك قدرات معرفية شبيهة بالإنسان، وقادر على أداء مهام متنوعة دون برمجة مسبقة، وهو مجال أبحاث نظرية حول الذكاء الاصطناعي يحاول إنشاء برنامج بذكاء يشبه الإنسان والقدرة على التعليم الذاتي .الهدف هو أن يكون البرنامج قادرًا على أداء المهام التي لم يتم بالضرورة تدريبه عليها أو تطويره من أجلها(19)، يتميز بحل المشكلات المعقدة في سياقات غير مألوفة، وفهم مهام متعددة لم يتم تدريبه عليها مسبقًا .

ج. الذكاء الاصطناعي الفائق (Super AI): الذكاء الاصطناعي الفائق (ASI) هو نظام ذكاء اصطناعي افتراضي يعتمد على البرمجيات، يتمتع بنطاق فكري يتجاوز الذكاء البشري .على المستوى الأساسي، يتميز هذا النوع من الذكاء بوظائف إدراكية متطورة ومهارات تفكير عالية المستوى تفوق تلك التي يمتلكها أي إنسان(20)، وهو تصور مستقبلي يتجاوز فيه الذكاء الاصطناعي القدرات البشرية في مختلف المجالات، ويثير هذا النوع جدلًا واسعًا من الناحية الأخلاقية والأمنية.

4) تقنيات الذكاء الاصطناعي:

أ) التعلم الآلي (ML: Machine Learning)(21): هو مجموعة فرعية من الذكاء الاصطناعي التي تركز على بناء أنظمة تتعلم وتتحسن مع استهلاك المزيد من البيانات. يُعد الذكاء الاصطناعي مصطلحًا أوسع يشير إلى الأنظمة أو الآلات التي تحاكي الذكاء البشري. يعتمد على خوارزميات إحصائية لتحليل البيانات الضخمة، تقديم تنبؤات، واتخاذ قرارات. يُمكن الحواسيب من التعلم من البيانات، تحديد الأنماط، وتحسين الأداء تلقائياً دون برمجة صريحة لكل خطوة، والأنواع الأربعة الأكثر شيوعًا في التعلم الآلي هي: التعلم الخاضع للإشراف.، التعلم غير الخاضع للإشراف، التعلم شبه الخاضع للإشراف، والتعلم المعزز.

وقد استُخدمت هذه الأنواع على نطاق واسع في تحليل السلوك الشبكي، وكشف الأنماط غير الطبيعية في الأمن السيبراني. غالبًا ما تتم مناقشة التعلم الآلي والذكاء الاصطناعي معًا، ويتم استخدام المصطلحات في بعض الأحيان بالتبادل، ولكنهما لا يمثلان الشيء نفسه، باختصار، كل ما هو تعلم آلي هو ذكاء اصطناعي، وليس العكس، فليس كل ذكاء اصطناعي هو تعلم آلي.

ب) التعلم العميق (Deep Learning)(22): التعلم العميق هو مجموعة فرعية من التعلم الآلي (ML) حيث تعمل خوارزميات الشبكات العصبية الاصطناعية مثل الدماغ البشري من كميات كبيرة من البيانات. يعتمد التعلم العميق على الشبكات العصبية الاصطناعية متعددة الطبقات، ويُستخدم في معالجة البيانات غير المهيكلة مثل الصور والصوت والنصوص والتعرف على الأنماط المعقدة، واتخاذ القرارات دون تدخل بشري. يُعد من أكثر التقنيات فاعلية في كشف الهجمات المتقدمة والتهديدات الخفية. يُستخدم في تطبيقات مثل السيارات ذاتية القيادة، التعرف على الوجه، وترجمة اللغات.

ج) معالجة اللغات الطبيعية (NLP)(23): هي فرع من الذكاء الاصطناعي وعلوم الحاسوب، تهدف لتمكين الآلات من فهم، تفسير، وتوليد اللغة البشرية (نصاً أو صوتاً) بطريقة طبيعية .تجمع بين اللغويات الحاسوبية، التعلم الآلي، والتعلم العميق لتحليل السياق، المعنى، والمشاعر، وتعد المحرك الأساسي للمساعدين الصوتين والترجمة الآلية. تُستخدم هذه التقنية في تحليل النصوص والمحادثات، وكشف محاولات التصيد الاحتيالي، وتحليل المحتوى الخبيث، مما يجعلها ذات أهمية خاصة في الأمن السيبراني، وهي التقنية التي تُمكّن الأنظمة من فهم وتفسير اللغات البشرية بمختلف أشكالها. تعتمد هذه التقنية على خوارزميات متقدمة لتحليل النصوص والكلمات وتحويلها إلى بيانات يمكن للأنظمة الذكية معالجتها وفهمها. تُستخدم هذه التقنية في مجموعة واسعة من التطبيقات مثل خدمة العملاء، الترجمة الآلية، وتحليل المشاعر، مما يتيح للمؤسسات تحسين تفاعلها مع العملاء بشكل فعال وسريع.

4) تطبيقات الذكاء الاصطناعي في المجال الأمني (Artificial Intelligence in the Security Field)(24): يمكن أن يساعد نظام الذكاء الاصطناعي على حماية البيانات الحساسة عبر البيئات السحابية الهجينة من خلال تحديد البيانات تلقائيًا، ومراقبة الحالات الشاذة في الوصول إلى البيانات، وتنبيه متخصصي الأمن الإلكتروني بشأن التهديدات فور حدوثها. أدى توظيف الذكاء الاصطناعي في المجال الأمني إلى تطوير أدوات أكثر كفاءة في رصد التهديدات السيبرانية والاستجابة لها. ومن أبرز هذه التطبيقات: أنظمة كشف التسلل الذكية، تحليل السلوك غير الطبيعي للشبكات، التنبؤ بالهجمات السيبرانية، أتمتة الاستجابة للحوادث الأمنية، وكشف البرمجيات الخبيثة المتقدمة، وقد أسهمت هذه التطبيقات في تقليل زمن الاستجابة للهجمات، ورفع مستوى الدقة مقارنة بالأنظمة التقليدية.

5) الذكاء الاصطناعي والأمن القومي(25): أصبح الذكاء الاصطناعي عنصرًا استراتيجيًا في منظومات الأمن القومي للدول، حيث تعتمد عليه المؤسسات العسكرية والأمنية في حماية البنية التحتية الرقمية، وتأمين الأنظمة الحساسة، ومواجهة التهديدات العابرة للحدود، كما دخل الذكاء الاصطناعي ضمن سباق دولي محموم، تسعى فيه الدول إلى تحقيق التفوق التقني، وفي المقابل، يفرض هذا الواقع تحديات قانونية وأخلاقية، تتعلق بالخصوصية، وحماية البيانات، والمسؤولية عن القرارات التي تتخذها الأنظمة الذكية، كما أصبح الذكاء الاصطناعي عنصرًا هامًا في الأمن القومي في زمن العولمة، حيث يوفر الكثير من الجهود في مجالات الأمن القومي، مثل الدفاع والأمن، من خلال تقديم احتمالات تهديدات الأمن القومي الداخلية والخارجية، وكذلك معالجة البيانات المتعلقة بالتسلح، وهذا ما دفع الكثير من الحكومات إلى رفع معدلات الاستثمارات في الذكاء الاصطناعي لخدمة الأمن القومي.

6) التحديات المرتبطة بتوظيف الذكاء الاصطناعي(26): رغم المزايا الكبيرة للذكاء الاصطناعي، إلا أن توظيفه يواجه جملة من التحديات، من أبرزها: ضعف قابلية تفسير النماذج الذكية، الاعتماد المفرط على البيانات، أخطار التحيز الخوارزمي، قابلية النماذج للهجمات العدائية، غياب الأطر التشريعية الموحدة.

ثانيا) الإطار النظري للأمن السيبراني

1) نشأة الأمن السيبراني وتطوره: ارتبط ظهور مفهوم الأمن السيبراني ارتباطًا وثيقًا بتطور استخدام الحاسوب والشبكات الرقمية، حيث بدأت الحاجة إلى حماية الأنظمة الإلكترونية منذ السبعينيات من القرن الماضي، بالتزامن مع انتشار الحواسيب المركزية وربطها بشبكات الاتصال. مع توسع استخدام الإنترنت في التسعينيات، لم تعد التهديدات مقتصرة على الأعطال التقنية، بل ظهرت أنماط جديدة من الهجمات الإلكترونية التي تستهدف البيانات والأنظمة والبنية التحتية الرقمية، وقد تطور مفهوم الأمن السيبراني من مجرد حماية تقنية للأنظمة إلى منظومة شاملة تشمل الجوانب التقنية، والتنظيمية، والبشرية، والتشريعية. مع دخول العالم مرحلة التحول الرقمي الشامل، أصبح الأمن السيبراني عنصرًا أساسيًا في استقرار المؤسسات والدول، وركيزة من ركائز الأمن القومي.

2) مفهوم الأمن السيبراني وأهدافه: يُعرَّف الأمن السيبراني بأنه مجموعة الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة الرقمية، والشبكات، والبرمجيات، والبيانات، من الهجمات الإلكترونية أو الوصول غير المصرح به أو الإتلاف أو التعطيل. يُعد الأمن السيبراني امتدادًا متطورًا لمفهوم أمن المعلومات (Information Security). تتمثل الأهداف الرئيسة للأمن السيبراني في:

أ. سرية المعلومات: منع الوصول غير المصرح به إلى البيانات.

ب. سلامة البيانات: ضمان عدم التلاعب أو التغيير غير المشروع.

ج. توافر الأنظمة: ضمان استمرارية الخدمات وعدم تعطيلها.

د. الموثوقية: تعزيز الثقة في الأنظمة الرقمية.

هـ. حماية البنية التحتية الحرجة: مثل شبكات الطاقة والاتصالات والمصارف.

3) أنواع التهديدات السيبرانية(27): تتعدد التهديدات السيبرانية وتختلف في أساليبها وأهدافها، ومن أبرزها:

أ. البرمجيات الخبيثة: تشمل الفيروسات، والديدان، وأحصنة طروادة، وبرامج الفدية، التي تهدف إلى إتلاف البيانات أو تشفيرها أو التجسس على المستخدمين.

ب. هجمات حجب الخدمة الموزعة (DDoS): وهي هجمات تهدف إلى تعطيل الأنظمة والخوادم عبر إغراقها بحركة مرور وهمية.

ج. التصيّد الاحتيالي: يعتمد على خداع المستخدمين للحصول على بيانات حساسة، ويُعد من أكثر الهجمات شيوعًا وخطورة.

د. الهندسة الاجتماعية: تركز على استغلال العامل البشري بدلًا من الثغرات التقنية.

هـ. الهجمات المتقدمة المستمرة (APT): وهي هجمات معقدة وطويلة الأمد، غالبًا ما تكون مدعومة من جهات منظمة أو دول.

نصائح للوقاية بضرورة تحديث البرامج بانتظام، استخدام برامج مكافحة فيروسات قوية، تفعيل المصادقة الثنائية، والنسخ الاحتياطي الدوري للبيانات.

4) عناصر منظومة الأمن السيبراني: تقوم منظومة الأمن السيبراني على مجموعة من العناصر المتكاملة، من أهمها:

أ. العنصر التقني: مثل جدران الحماية، وأنظمة كشف التسلل، وبرامج مكافحة البرمجيات الخبيثة.

ب. العنصر البشري: الوعي الأمني، والتدريب، والانضباط الوظيفي.

ج. العنصر التنظيمي: السياسات والإجراءات الأمنية.

د. العنصر التشريعي: القوانين واللوائح المنظمة للأمن السيبراني.

ويُعد الإخلال بأي عنصر من هذه العناصر سببًا مباشرًا في ضعف المنظومة الأمنية.

5) الأمن السيبراني وأمن المعلومات: على الرغم من التقارب بين مفهومي الأمن السيبراني وأمن المعلومات، إلا أن هناك اختلافًا جوهريًا بينهما، فأمن المعلومات (Information Security) يركز أساسًا على حماية البيانات بغض النظر عن شكلها، في حين يركز الأمن السيبراني على حماية الفضاء السيبراني بكامل مكوناته، وقد أدى التطور التقني إلى تداخل المفهومين.

6) الأمن السيبراني والأمن القومي: أصبح الأمن السيبراني أحد الأبعاد الرئيسة للأمن القومي، نظرًا لاعتماد الدول المتزايد على الأنظمة الرقمية في إدارة مرافقها الحيوية. باتت الدول تنظر إلى الفضاء السيبراني بوصفه ميدانًا جديدًا للصراع، وتسعى إلى تطوير استراتيجيات وطنية للأمن السيبراني، وتعزيز التعاون الدولي لمواجهة التهديدات العابرة للحدود.

7) التحديات التي تواجه الأمن السيبراني(28): أصبحت البيانات الرقمية والأنظمة الإلكترونية عرضة للهجمات السيبرانية، هذه الهجمات يمكن أن تؤدي إلى سرقة المعلومات وإتلاف الأنظمة، أو حتى تعطيل الخدمات الحيوية، من أبرزها: التطور السريع في أساليب الهجوم، نقص الكفاءات البشرية المتخصصة، الاعتماد المتزايد على الأنظمة الذكية، ضعف الوعي الأمني لدى المستخدمين، والتحديات القانونية والتنظيمية.

وتفرض هذه التحديات الحاجة إلى حلول مبتكرة، وعلى رأسها توظيف تقنيات الذكاء الاصطناعي.

ثالثا) الذكاء الاصطناعي في خدمة الأمن السيبراني

1) مدخل عام إلى دور الذكاء الاصطناعي في الأمن السيبراني: أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إعادة تشكيل منظومات الأمن السيبراني بصورة جذرية. يقوم دور الذكاء الاصطناعي في الأمن السيبراني على مبدأ الانتقال من الأمن التفاعلي إلى الأمن الاستباقي، حيث تُستخدم الخوارزميات الذكية للتنبؤ بالهجمات المحتملة قبل وقوعها، بدلًا من الاكتفاء بمعالجتها بعد حدوثها، وقد ساهم هذا التحول في رفع كفاءة منظومات الحماية، وتقليل زمن الاستجابة، والحد من الخسائر الناتجة عن الهجمات السيبرانية.

2) توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني(29): يُعد كلًا من الذكاء الاصطناعي والأمن السيبراني من صور التطور التكنولوجي الهائل الذي نعيشه منذ سنوات، وقد اكتسبا هذان المجالان شهرة هائلة في التكنولوجيا الحديثة، نظرًا لأدوارهما الحاسمة في تشكيل العالم الرقمي، إذ حرصت المؤسسات على الاستعانة بأدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي حتى تتمكن من اكتشاف التهديدات والاستجابة لها بشكل أسرع.

رابعا) الفرق بين الذكاء الاصطناعي والامن السيبراني: الأمن السيبراني هي العملية التي تهدف إلى حماية أنظمة وشبكات الحاسوب المتصلة بالإنترنت من الهجمات الرقمية والاختراقات، أو التدمير، أو التعطيل، أو التعطيل. الذكاء الاصطناعي هو أحد فروع علوم الكمبيوتر، مهمته هي إنشاء آلات تستطيع القيام بالمهام التي تحتاج إلى ذكاءً بشريًا مثل فهم اللغة الطبيعية والتعرف على الصور واتخاذ القرارات، يتعامل الذكاء الاصطناعي مع تجميع البيانات وتصنيفها ومعالجتها وتصفيتها وإدارتها. يتضمن الأمن السيبراني العديد من نقاط البيانات التي يمكن استخدامها للذكاء الاصطناعي.

خامسا) علاقة الذكاء الاصطناعي بالأمن السيبراني: هناك علاقة وثيقة بينهما إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب. لجأت المنظمات إلى عدة وسائل لمكافحة التهديدات، للكشف السريع عن الأنشطة الضارة ومواجهتها، وحماية الشبكات من الهجمات الإلكترونية. يعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات، وأتمتة آليات الاستجابة، مما يعزز من البنية التحتية للأمن.

سادسا) فوائد لاستخدام الذكاء الاصطناعي في الأمن السيبراني: تتمثل فوائد استخدام أدوات وأنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي بالتعامل مع الكثير من البيانات، تقليل العمليات المزدوجة، تسريع أوقات الكشف والاستجابة، محاربة الروبوتات

الضارة، تأمين المصادقة بتوفير العديد من الأدوات مثل ماسحات بصمات الأصابع والتعرف على الوجه، تحسين الدقة والكفاءة مقارنة بالحلول الأمنية التقليدية، والقدرة على التعرف على الأنماط التي لا تستطيع العين البشرية اكتشافها، وهو ما يزيد من دقة اكتشاف الأنشطة الضارة.

سابعا) استخدام الذكاء الاصطناعي في كشف التهديدات السيبرانية

أ) كشف التسلل القائم على الذكاء الاصطناعي: تُعد أنظمة كشف التسلل من أهم مجالات توظيف الذكاء الاصطناعي في الأمن السيبراني، حيث تعتمد هذه الأنظمة على تقنيات التعلم الآلي والتعلم العميق لتحليل حركة الشبكات، والكشف عن السلوك غير الطبيعي الذي قد يشير إلى وجود هجوم سيبراني.

ب) كشف البرمجيات الخبيثة: يُستخدم الذكاء الاصطناعي على نطاق واسع في تحليل البرمجيات الخبيثة، من خلال دراسة سلوك الملفات والبرامج، ويتيح هذا النهج اكتشاف البرمجيات الخبيثة غير المعروفة سابقًا، بما في ذلك البرمجيات المتخفية والبرمجيات المتعددة الأشكال.

ج) الذكاء الاصطناعي في تحليل السلوك والتنبؤ بالهجمات: يعتمد تحليل السلوك الشاذ على السلوك الطبيعي للمستخدمين والأنظمة والشبكات ومقارنته بالسلوك الفعلي، بهدف اكتشاف الانحرافات التي قد تشير إلى نشاط ضار(30)، والكشف المبكر عن الهجمات الداخلية وتسريب البيانات، إذ تقوم الخوارزميات الذكية ببناء نماذج للسلوك الطبيعي، ثم مقارنة السلوك الفعلي بهذه النماذج لاكتشاف أي انحراف قد يدل على نشاط خبيث، كما يُستخدم في التنبؤ بالهجمات السيبرانية، من خلال تحليل البيانات التاريخية، ومؤشرات التهديد، والأنماط الزمنية للهجمات، مما يمكّن المؤسسات من اتخاذ إجراءات وقائية مسبقة.

د) أتمتة الاستجابة للحوادث الأمنية (SOAR): أدى دمج الذكاء الاصطناعي مع منصات تنسيق وأتمتة الاستجابة للحوادث الأمنية إلى إحداث نقلة نوعية في إدارة الحوادث السيبرانية، إذ تتيح هذه المنصات تنفيذ استجابات تلقائية للهجمات، مثل عزل الأنظمة المصابة، أو حظر عناوين الشبكة المشبوهة، أو إيقاف العمليات الخبيثة، دون تدخل بشري مباشر. تكمن أهمية هذا التوجه في تقليل الاعتماد على العنصر البشري، وتسريع الاستجابة، وتقليل الأخطاء الناتجة عن الضغط أو نقص الخبرة.

هـ) الذكاء الاصطناعي في حماية البنية التحتية الحرجة: تُعد البنية التحتية الحرجة، مثل شبكات الطاقة والمياه والاتصالات والمصارف، من أكثر الأهداف حساسية للهجمات السيبرانية، وقد أسهم الذكاء الاصطناعي في تعزيز حماية هذه البنى، من خلال مراقبة الأنظمة الصناعية، وتحليل بيانات أجهزة الاستشعار، والكشف المبكر عن محاولات التخريب أو التلاعب، كما يُستخدم الذكاء الاصطناعي في محاكاة سيناريوهات الهجوم المحتملة، وتقييم نقاط الضعف، بما يساعد صناع القرار على تعزيز جاهزية الأنظمة الحيوية. أظهرت الدراسات أن تقليص زمن اكتشاف الهجمات يعد عاملًا حاسمًا في الحد من الأضرار، وقد ساعد الذكاء الاصطناعي في تحقيق ذلك عبر التحليل الفوري للبيانات والتنبيه المبكر(31).

و) الذكاء الاصطناعي في إدارة المخاطر السيبرانية: أتاح الذكاء الاصطناعي إمكانات متقدمة في إدارة المخاطر السيبرانية من خلال تحليل البيانات التاريخية والتنبؤ بالتهديدات المحتملة، مما أسهم في تعزيز مفهوم الأمن التنبؤي والاستباقي(32)، وتقدير احتمالية وقوعها، وتقييم آثارها المحتملة على المؤسسة، كما يدعم الذكاء الاصطناعي عملية ترتيب أولويات المخاطر، وتخصيص الموارد الأمنية بكفاءة أعلى، بما يحقق توازنًا بين التكلفة ومستوى الحماية.

ز) حدود فاعلية الذكاء الاصطناعي في الأمن السيبراني: على الرغم من المزايا الكبيرة التي يوفرها الذكاء الاصطناعي، إلا أن فاعليته في الأمن السيبراني ليست مطلقة، إذ تواجه تطبيقاته عدة قيود، من أبرزها: الاعتماد الكبير على جودة البيانات، صعوبة تفسير قرارات بعض النماذج الذكية، قابلية النماذج للهجمات العدائية، والحاجة المستمرة للتحديث والتدريب، وتؤكد هذه القيود ضرورة دمج الذكاء الاصطناعي ضمن منظومة أمنية شاملة، وعدم الاعتماد عليه بوصفه حلًا منفردًا.

ثامنا) أخطار الذكاء الاصطناعي والتهديدات السيبرانية المستقبلية والتحديات الأخلاقية والتشريعية

أ) مدخل عام إلى أخطار الذكاء الاصطناعي في المجال السيبراني: على الرغم من الدور المتنامي الذي يؤديه الذكاء الاصطناعي في تعزيز منظومات الأمن السيبراني، فإن هذا التطور ذاته أفرز مجموعة من المخاطر والتحديات التي باتت تشكّل مصدر قلق متزايد للباحثين وصناع القرار، فكما يُستخدم الذكاء الاصطناعي في الدفاع والكشف المبكر والاستجابة، فإنه يُستخدم أيضًا في تطوير أدوات هجومية أكثر ذكاءً وتعقيدًا، قادرة على تجاوز أنظمة الحماية التقليدية والذكية على حد سواء. يعود ذلك إلى الطبيعة المزدوجة للذكاء الاصطناعي، بوصفه تقنية عامة قابلة للتوظيف في اتجاهات متباينة، مما يفرض الحاجة إلى دراسة مخاطره دراسة علمية عميقة، وربطها بالأبعاد الأخلاقية والتشريعية والتنظيمية، لضمان استخدام آمن ومسؤول لهذه التقنية.

ب) الهجمات العدائية على نماذج الذكاء الاصطناعي: تُعد الهجمات العدائية (Adversarial Attacks) من أخطر التهديدات التي تواجه أنظمة الذكاء الاصطناعي، إذ تستهدف نماذج التعلم الآلي نفسها بدلًا من البنية التحتية التقليدية. تعتمد هذه الهجمات على إدخال تعديلات طفيفة على البيانات المدخلة للنموذج، تؤدي إلى تضليل النظام وإجباره على اتخاذ قرارات خاطئة، وتكمن خطورة هذه الهجمات في صعوبة اكتشافها، لا سيما عندما تُنفذ بأساليب متقدمة تستغل نقاط الضعف في بنية النموذج أو بيانات التدريب، إن بعض النماذج عالية الدقة تكون في الوقت ذاته أكثر هشاشة أمام هذا النوع من الهجمات، مما يطرح تحديات كبيرة أمام توظيف الذكاء الاصطناعي في الأنظمة الحرجة.

ج) التزييف العميق وانتحال الهوية الرقمية: من أخطر التطبيقات السلبية للذكاء الاصطناعي ما يُعرف بـ التزييف العميق (Deep Fake)، والذي يُستخدم في إنشاء صور ومقاطع فيديو وتسجيلات صوتية مزيفة يصعب تمييزها عن المحتوى الحقيقي، وقد أدى انتشار هذه التقنية إلى تصاعد أخطار انتحال الهوية الرقمية، والابتزاز الإلكتروني، ونشر المعلومات المضللة. تزداد خطورة التزييف العميق عندما يُستخدم في السياقات السياسية أو الأمنية أو الاقتصادية، حيث يمكن أن يؤدي إلى زعزعة الثقة المجتمعية، والتأثير على الرأي العام، وتهديد الاستقرار الوطني. يشكّل هذا النوع من الهجمات تحديًا كبيرًا أمام أنظمة التحقق الرقمية، ويستلزم تطوير أدوات كشف متقدمة تعتمد بدورها على الذكاء الاصطناعي.

د) استخدام الذكاء الاصطناعي في الهجمات السيبرانية المتقدمة: لم يعد الذكاء الاصطناعي مقتصرًا على الاستخدامات الدفاعية، بل أصبح أداة فعالة في تنفيذ هجمات سيبرانية متقدمة، مثل الهجمات المتكيفة التي تغيّر سلوكها تلقائيًا لتجنب الكشف، وهجمات التصيّد الاحتيالي الذكية التي تُصمَّم بناءً على تحليل سلوك الضحايا واهتماماتهم، كما يُستخدم الذكاء الاصطناعي في أتمتة الهجمات واسعة النطاق، وزيادة سرعتها ودقتها، وتقليل الحاجة إلى تدخل بشري مباشر، مما يجعل من الصعب تتبع مصدر الهجوم أو التنبؤ به.

هـ) المخاطر الأخلاقية المرتبطة بالذكاء الاصطناعي: يثير توظيف الذكاء الاصطناعي في المجال السيبراني جملة من الإشكالات الأخلاقية، من أبرزها مسألة الخصوصية، وجمع البيانات، واستخدامها دون علم أو موافقة أصحابها، كما تبرز مشكلة التحيز الخوارزمي، حيث قد تعكس النماذج الذكية تحيزات موجودة في بيانات التدريب، مما يؤدي إلى قرارات غير عادلة أو تمييزية. تطرح هذه القضايا تساؤلات جوهرية حول مسؤولية القرارات التي تتخذها الأنظمة الذكية، وحدود الاعتماد عليها، ودور الإنسان في الإشراف والمساءلة، وهو ما يستدعي تبني مبادئ أخلاقية واضحة تحكم تصميم واستخدام الذكاء الاصطناعي. يسهم الذكاء الاصطناعي في دعم اتخاذ القرار الأمني من خلال تقديم تحليلات وتوصيات مبنية على بيانات دقيقة، مع التأكيد على بقاء القرار النهائي بيد العنصر البشري نظرًا لأبعاده الأخلاقية والاستراتيجية.

و) التحديات التشريعية والتنظيمية: غالبًا ما تتأخر القوانين عن ملاحقة الابتكارات التقنية، ويؤدي هذا التأخر إلى وجود فراغ قانوني يُستغل في تنفيذ أنشطة سيبرانية ضارة دون مساءلة واضحة، كما تختلف التشريعات من دولة إلى أخرى، مما يصعّب التعاون الدولي في

مواجهة التهديدات السيبرانية العابرة للحدود، ومن هنا، تبرز الحاجة إلى أطر تشريعية مرنة، وتعاون دولي فعّال، يوازن بين تشجيع الابتكار وحماية الأمن والحقوق الفردية.

ز) التهديدات السيبرانية المستقبلية في ظل تطور الذكاء الاصطناعي: تشير التوقعات المستقبلية إلى أن التهديدات السيبرانية ستزداد تعقيدًا مع تطور تقنيات الذكاء الاصطناعي، لا سيما مع ظهور نماذج أكثر استقلالية وقدرة على التعلم الذاتي، وقد يشهد المستقبل هجمات تعتمد على أنظمة ذكية قادرة على التنسيق فيما بينها، واتخاذ قرارات هجومية دون تدخل بشري مباشر، كما يُتوقع أن تتداخل التهديدات السيبرانية مع مجالات أخرى، مثل الأمن الاقتصادي والإعلامي والسياسي، مما يستدعي مقاربات شاملة تتجاوز الحلول التقنية البحتة.

تاسعا) حالات استخدام شائعة للذكاء الاصطناعي في مجال الأمن السيبراني(33)

أمثلة عليها لتعزيز الأمن السيبراني باستخدام الذكاء الاصطناعي للتخفيف من المخاطر السيبرانية:

1) إدارة الثغرات الأمنية: مثال من قطاع الصناعة حيث يمكن لشركة تطوير البرمجيات استخدام الذكاء الاصطناعي لتحديد الثغرات الأمنية المحددة في برمجياتها التي يُرجح أن يستغلها المهاجمون، وذلك استنادًا إلى بيانات هجمات واقعية، ويمكن للذكاء الاصطناعي معالجة هذه المشكلات فورًا وفقًا لحوكمة الذكاء الاصطناعي المعمول بها وأفضل الممارسات.
2) إدارة التعرض: مثال من قطاع الطاقة قد تستخدم إحدى شركات الطاقة ميزات الذكاء الاصطناعي في منصة إدارة المخاطر الخاصة بها لاكتشاف حالات سوء التكوين المترابطة التي قد تؤدي من شبكة تكنولوجيا المعلومات إلى أنظمة التشغيل الحيوية، وبناءً على هذه المعلومات، يمكنها بعد ذلك التوصية بإجراءات تجزئة آلية أو تفعيلها حسب الحاجة.
3) الكشف عن التهديدات عبر البريد الإلكتروني: يمكن لمؤسسة مالية استخدام الذكاء الاصطناعي في بوابة البريد الإلكتروني الخاصة بها لحظر رسائل البريد الإلكتروني المعقدة التي تبدو وكأنها من الرئيس التنفيذي أو غيره من المسؤولين التنفيذيين لحماية بيانات العملاء الحساسة، كذلك تبسيط العمليات المالية واتخاذ القرارات وأتمتة العمليات المعقدة من خلال تحليل كميات كبيرة من البيانات في الوقت الحقيقي والقدرة على تقديم إدارة مالية شخصية وتحليل التاريخ المالي للعميل، واكتشاف أنماط الإنفاق، والتوصية بإجراءات لتحسين الصحة المالية وأتمتة تحويلات الأموال لمنع رسوم السحب على المكشوف، وتحسين المدخرات بناءً على أسعار الفائدة، واكتشاف المخاطر المحتملة قبل أن تؤثر على الاستقرار المالي، مما يساعد المؤسسات المالية على تعزيز الكفاءة التشغيلية، وتقليل التكاليف، وتقديم رؤى مالية أفضل لكل من الشركات والأفراد.
4) الكشف عن نقاط الاتصال والاستجابة لها: مثال من قطاع الرعاية الصحية، قد يستخدم مزود خدمات الرعاية الصحية حلول الكشف عن نقاط الاتصال والاستجابة لها المدعومة بالذكاء الاصطناعي لاكتشاف ومنع مهاجمي برامج الفدية من تشفير بيانات المرضى وتسريبها واستعادة النظام إلى حالته الأصلية، كإزالة الملفات/المحتوى الضار كجزء من المراحل الأولى لهجوم برامج الفدية.
5) أتمتة دعم تكنولوجيا المعلومات وإدارة الخدمات: تتمثل إحدى المزايا الرئيسية في الخدمة الذاتية المستقلة، حيث يمكن للموظفين الحصول على مساعدة فورية في تكنولوجيا المعلومات دون الانتظار لتدخل بشري مثل إعادة تعيين كلمات المرور، وتثبيت البرمجيات، وتوفير الوصول، بينما تتكامل أيضًا مع أنظمة المؤسسات المختلفة لتشخيص وحل المشكلات التقنية الأكثر تعقيدًا(34).
6) تعزيز عمليات الموارد البشرية ودعم الموظفين: تطبيق واحد يقوم بتبسيط عملية التوظيف من خلال فحص السير الذاتية تلقائيًا، وتحديد أفضل المرشحين، وجدولة المقابلات، هذا يقلل من عبء العمل اليدوي على محترفي الموارد البشرية ويسرع من عملية التوظيف، والإجابة على الأسئلة المتعلقة بالموارد البشرية، ومساعدة الموظفين في استفسارات المزايا، والمساعدة في عمليات الانضمام وتخطيط القوى العاملة وتطوير المواهب.

7) كشف التهديدات والاستجابة في الوقت الحقيقي: يحسن الذكاء الاصطناعي الأمن السيبراني من خلال التعرف على التهديدات والتخفيف منها بشكل تلقائي في الوقت الحقيقي. تراقب هذه الأنظمة حركة الشبكة باستمرار، وتحلل سلوك المستخدم، وتكتشف الشذوذ الذي قد يشير إلى نشاط خبيث من خلال الاستفادة من نماذج التعلم الآلي، يمكن للذكاء الاصطناعي التمييز بين العمليات الطبيعية والتهديدات المحتملة.

الخاتمة

خلص هذا البحث إلى أن الذكاء الاصطناعي أصبح أحد أهم الأدوات الاستراتيجية في مواجهة التهديدات السيبرانية المعاصرة، لما يتمتع به من قدرات متقدمة في التحليل والتنبؤ والاستجابة، غير أن هذا الدور المتنامي لا يخلو من مخاطر وتحديات، تجعل من الضروري التعامل مع الذكاء الاصطناعي بمنظور متوازن يجمع بين الاستفادة من إمكاناته، والتحكم في مخاطره. بيّن البحث أن تحقيق أمن سيبراني فعّال في عصر الذكاء الاصطناعي يتطلب تكاملًا بين التكنولوجيا، والتشريع، والأخلاق، وبناء القدرات البشرية، والتعاون الدولي، من هنا، فإن الاستثمار في الذكاء الاصطناعي يجب أن يقترن دائمًا بسياسات حوكمة رشيدة، ورؤية استراتيجية شاملة، تضمن أمن الفضاء السيبراني واستدامته.

النتائج

1. أصبح الذكاء الاصطناعي عنصرًا محوريًا في منظومات الأمن السيبراني الحديثة، ولم يعد دوره تكميليًا أو ثانويًا، بل بات من الأدوات الأساسية في كشف التهديدات السيبرانية وتحليلها والاستجابة لها.
2. تعجز الأساليب التقليدية للأمن السيبراني عن مواجهة التهديدات المتقدمة التي تتسم بالسرعة والتعقيد والتكيف المستمر، وهو ما يفسر الاتجاه المتزايد نحو تبني تقنيات التعلم الآلي والتعلم العميق في المجال الأمني.
3. يسهم الذكاء الاصطناعي في الانتقال من الأمن التفاعلي إلى الأمن الاستباقي، من خلال تحليل السلوكيات، والتنبؤ بالهجمات، والكشف المبكر عن الأنماط غير الطبيعية قبل تحولها إلى حوادث أمنية جسيمة.
4. يمثل الذكاء الاصطناعي سلاحًا ذا حدين، إذ يُستخدم في الوقت ذاته من قبل الجهات الدفاعية لتعزيز الحماية، ومن قبل الجهات الخبيثة لتطوير هجمات سيبرانية أكثر ذكاءً وتعقيدًا، مثل الهجمات العدائية والتزييف العميق.
5. تُعد نماذج الذكاء الاصطناعي نفسها أهدافًا محتملة للهجمات السيبرانية، وهو ما يفرض ضرورة التعامل مع أمن الذكاء الاصطناعي بوصفه جزءًا لا يتجزأ من منظومة الأمن السيبراني الشاملة.
6. لا تقتصر تحديات توظيف الذكاء الاصطناعي على الجوانب التقنية فقط، بل تمتد إلى أبعاد أخلاقية وتشريعية وتنظيمية، تتعلق بالخصوصية، والتحيز الخوارزمي، والمساءلة، وحوكمة البيانات.
7. يشكّل العنصر البشري أحد أهم نقاط الضعف في منظومات الأمن السيبراني، سواء من حيث نقص الكفاءات المتخصصة أو ضعف الوعي الأمني، مما يؤكد أن التكنولوجيا وحدها لا تكفي لتحقيق الحماية الشاملة.
8. يتزايد ارتباط الأمن السيبراني بالأمن القومي للدول، في ظل اعتماد البنى التحتية الحيوية على الأنظمة الرقمية والذكية، مما يجعل أي خلل سيبراني تهديدًا مباشرًا للاستقرار الوطني.

التوصيات

1. ضرورة الجمع بين الأبعاد التقنية والأمنية والاستراتيجية في إطار تحليلي لتقديم رؤية نقدية لاستخدام الذكاء الاصطناعي بوصفه أداة دفاعية وهجومية في آن واحد.
2. الحاجة لمزيد من الأبحاث والدراسات العلمية لسد فجوة بحثية في الأدبيات العربية من خلال معالجة موضوع حديث بمنهج علمي.

3. التركيز على الانعكاسات الاستراتيجية لاستخدام الذكاء الاصطناعي في الأمن السيبراني على مستوى الدول والمؤسسات.
4. تعزيز تبني تقنيات الذكاء الاصطناعي في منظومات الأمن السيبراني، مع مراعاة دمجها ضمن أطر أمنية شاملة وعدم الاعتماد عليها بوصفها حلولًا منفردة.
5. الاهتمام بأمن نماذج الذكاء الاصطناعي نفسها، من خلال تبني ممارسات التصميم الآمن، واختبار المتانة ضد الهجمات العدائية، وتحديث النماذج بصورة دورية.
6. تطوير الأطر التشريعية والتنظيمية التي تحكم استخدام الذكاء الاصطناعي في المجال السيبراني، بما يوازن بين تشجيع الابتكار وحماية الأمن والحقوق الفردية.
7. تعزيز دور الجامعات ومؤسسات التعليم العالي في إعداد كوادر متخصصة تجمع بين المعرفة التقنية في الذكاء الاصطناعي والأمن السيبراني، والوعي الأخلاقي والقانوني.
8. إدراج برامج تدريبية وتوعوية مستمرة للعاملين في المؤسسات الحكومية والخاصة، لرفع مستوى الوعي الأمني والحد من المخاطر الناتجة عن العامل البشري.
9. تشجيع البحث العلمي في مجال أمن الذكاء الاصطناعي، ولا سيما الدراسات التطبيقية التي تعالج الهجمات العدائية، وقابلية تفسير النماذج، وإدارة المخاطر.
10. تعزيز التعاون الإقليمي والدولي في مجال الأمن السيبراني، نظرًا للطبيعة العابرة للحدود للتهديدات الرقمية، وتبادل الخبرات وأفضل الممارسات.
11. تبني مبادئ أخلاقية واضحة لاستخدام الذكاء الاصطناعي، تضمن الشفافية، والمساءلة، وحماية الخصوصية، وتحد من التحيز الخوارزمي.
12. دراسة تطبيقات الذكاء الاصطناعي في حماية البنية التحتية الحرجة بصورة معمقة.
13. تحليل الأطر القانونية المقارنة لتنظيم الذكاء الاصطناعي والأمن السيبراني.
14. دراسة الأثر الاجتماعي والسياسي للتزييف العميق والمعلومات المضللة المدعومة بالذكاء الاصطناعي.

المصادر والمراجع

أولًا) الهوامش

1. https://www.bing.com.
2. المهندي، آمال، "العصر الرقمي.. الأمن السيبراني في عصر الذكاء الاصطناعي"، الراية الشامل، قطر، 2025.
3. الحجرف، حسن، "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤية نظرية"، مجلة الدراسات الجامعية للبحوث الشاملة، ISSN:2707-7675، 2024.
4. الهنائي، علي، "تطبيقات الذكاء الاصطناعي في المجال الأمني"، دراسة مُطبقة على دول مجلس التعاون لدول الخليج العربية، كلية الحقوق، جامعة مدينة السادات، مصر، المجلد 10، العدد 4، ديسمبر 2024، الصفحة 2633-2558، 2024.
5. يوسف، أحمد، "أهمية تطبيق الذكاء الاصطناعي في تعزيز أمن المعلومات بالقطاع الخدمي علم الخدمة مدخلا"، الملتقى العلمي الوطني الرابع حول: الاتجاهات العالمية الحديثة في مجال تسويق الخدمات – النماذج والممارسات- بتقنية التحاضر عن بعد - جامعة حسيبة بن بوعلي الشلف، الجزائر، 2021.

6. Caldwell, D & ،.Williams, R. *"Artificial intelligence and national security ,Journal of Cyber Policy".* 2022. 18–1 ،(1)7.
7. Brundage, M. et al.*," The Malicious Use of Artificial Intelligence".* Oxford, 2018.
8. Goodfellow, I. et al. "*Deep Learning",* MIT Press. http://www.deeplearningbook.org. 2016.
9. Russell, S., Norvig, P. "*Artificial Intelligence: A Modern Approach*", Pearson. 2021.
10. Mc Carthy, J, " *What Is Artificial Intelligence?"* Stanford University, 2007. http://www-formal.stanford.edu/jmc/.
11. Crevier, D. AI: " *The Tumultuous History of the Search for Artificial Intelligence*". 1993. https://www.amazon.com/"*Ai-Tumultuous-History-Artificial-Intelligence*"/ds/0465029973.
12. Kaplan, J., "*Artificial Intelligence: What Everyone Needs to Know*", Oxford University Press. Oxford University.
13. Mitchell, T. "*Machine Learning*", McGraw-Hill Science/Engineering/Math. 1997.
14. Bishop, Christopher, "*Pattern Recognition and Machine Learning*", Springer. http://research.microsoft.com/cmbishop.
15. Anderson, J., "*Cognitive Psychology, and Its Implications*". Ninth Edition.
16. أنواع الذكاء الاصطناعي، https://www.google.com/search.
17. الذكاء الاصطناعي الضيق - https://mittrarabia.com/technodad.
18. Churchland, P. Neurophilosophy. The MIT Press. ISBN: 9780262530859. 1989.
19. https://aws.amazon.com/ar/what-is/artificial-general-intelligence/
20. https://www.ibm.com/qa-ar/think/topics/artificial-superintelligence
21. https://www.oracle.com/middleeast-ar/artificial-intelligence/machine-learning/what-is-machine-learning
22. ما المقصود بالتعلم العميق؟ - شرح "التعلم العميق "بالذكاء الاصطناعي- AWS.amazon.com/ar/what-is/deep-learning/.
23. https://www.rmg-sa.com.
24. https://www.instagram.com/reel/DTgS-LXkxN9/
25. https://www.europarabct.com.
26. journals.ekb.eg.

27.أنواع تهديدات الأمن السيبراني -.://bakkah.com/ar/knowledge-center/
28.التحديات التي تواجه الأمن السيبراني https://www.bing.com.
29.توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، -https://bakkah.com/ar/knowledge center/ - آخر تحديث Jan 2025.
30.Buczak, A., Guven, E., "*A Survey of Data Mining and Machine Learning.*"
31.Chandola, V., "*Anomaly Detection: A Survey*".
32.Ahmed, M. et al., "*Network Anomaly Detection*".
33. 10حالات استخدام شائعة للذكاء الاصطناعي في مجال الأمن السيبراني وأمثلة عليها -https://es-la.tenable.com/cybersecurity-guide/learn/10-common-ai-cybersecurity-use-cases-and-examples، آخر تحديث 28 يناير 2026.
34.الذكاء الاصطناعي الفعال: كيف يعمل و7 حالات استخدام حقيقية https://www.exabeam.com/ar/explainers/ai-cyber-security/agentic-ai-how-it-works-and-7-real-world-use-cases.

ثانياً) المراجع بالعربية

- أمينة ختو: "بيئة المؤسسة وأثرها على الاداء الوظيفي"، مذكرة مكملة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة عبدالحميد بن باديس، مستغانم، 2015-2019.
- أنواع الذكاء الاصطناعي، https://www.google.com/search.
- توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، https://bakkah.com/ar/knowledge-center/ - آخر تحديث Jan 2025.
- حجازي، عبدالفتاح بيومي، "مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي": دارسة لقانونية متعمقة في القانون المعلوماتي، الاسكندرية، دار الفكر الجامعي، 2020.
- الحجرف، حسن، "دور الذكاء الاصطناعي في تعزيز الأمن السيبراني": رؤية نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، ISSN:2707-7675، 2024.
- خرسان، باسم، (2021)، "الأمن السيبراني في العراق": القراءة في مؤشر الأمن السيبراني العالمي، بغداد، مركز البيان للدراسات والتخطيط.
- الداعمي، غالب، "صناعة الرأي العام من عصر الطباعة إلى فضاء الانترنت – تقاليد موروثة وسلطة مطلقة"، دار أمجد للنشر والتوزيع، الاردن، 2019م.
- الرشيدي، طارق، "أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على مصادر الاسهم وأحجام التداول": دراسة مقارنة في لقطاع تكنولوجيا المعلومات، مجلة المحاسبة والمراجعة، العدد الثاني، 2019.
- الرنتيسي، احمد والعوائد، علي، "تحديات توظيف تطبيقات الذكاء الاصطناعي في دمج الاشخاص ذوي الإعاقة البصرية في محافظة ظفار"، مجلة الخدمة الاجتماعية، العدد 85، الإصدار 5، ص 145 – 177، عمان، 2025.
- شحرة، أبو بكر، "بناء القدرات في الأمن السيبراني"، المجلة العربية، الأمن السيبراني حروب الأرقام الصماء، ع ،495 الرياض، السعودية، 2015، ص 9.

- الشوا، مُحَمَّد، "الاثبات الجنائي في ظل نظام العولمة والتقنيات الحديثة"، دراسة تطبيقية على الاتحاد الأوروبي، التشريع الفرنسي، القاهرة، دار النهضة العربية، 2015.
- صفاء، تغريد، ومهدي، لبنى، "أثر السيبرانية في تطور القوة"، مجلة حمورابي للدراسات، مركز حمورابي للبحوث والدراسات الاستراتيجية، ع-33 ،34 السنة ،5 بغداد، 2020.
- عبد الحميد، عبد الله، "الأمن السيبراني: المفاهيم والتحديات المعاصرة"، القاهرة: دار الفكر العربي، 2021.
- عبد المعبود، عزة وحسن، طه، "أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة"، المجلة المصرية لعلوم المعلومات، مج 7، ع 1، بنى سويف، 2020.
- علي، مُحَمَّد، "الذكاء الاصطناعي وتطبيقاته في العصر الرقمي"، دار المسيرة، عمّان، 2020.
- غازي، خالد، "صناعة الكذب، كيف نفهم الإعلام البديل"، وكالة الصحافة العربية، الجيزة، 2022.
- القحطاني، عواطف، "متطلبات تعزيز الأمن الفكري لدى الطالبة الجامعية من منظور طريقة العمل مع الجماعات"، جامعة نايل للعلوم، 2019.
- كرار، عباس، "الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران"، *مجلة حمورابي للدراسات*، مج. 10، ع. 40، 2021، ص 195-223.
- مُحَمَّد، أميرة، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي"، مجلة البحوث الفقهية والقانونية بدمنهور، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص 355.
- مُحَمَّد، بسمة، "الحروب السيبرانية وأثرها في التنظيم الدولي"، كلية الآداب والعلوم، مجلة العلوم والدارسات الإنسانية، بنغازي، ليبيا، 2015.
- محمود، أحمد، "أثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة"، الأمن السيبراني في الشرق الأوسط، دارسة حالة من 2020 - ،2030 بحث منشور في المؤتمر الدولي مستقبل منطقة الشرق الأوسط – روية مصر، جامعة عين شمس، مركز الشرق الأوسط للدارسات المستقبلية، القاهرة، مجلة الدراسات القانونية والاقتصادية – دورية علمية محكمة - ISSN: 2356 9492(9999، 2020.
- المري، راشد، "الجرائم الإلكترونية، في ظل الفكر الجنائي المعاصر": دراسة مقارنة، القاهرة، دار النهضة العربية، 2015.
- المهندي، آمال، "العصر الرقمي.. الأمن السيبراني في عصر الذكاء الاصطناعي"، الراية الشامل، قطر، 2025.
- موسى، فريال، "تحديات الأمن السيبراني وكيفية مواجهتها"، العدد 463، 2024.
https://www.lebarmy.gov.lb/ar/content/.
- النيروز، على، "جرائم نظم المعلومات"، الاردن، دار السناء للنشر، 2017، ص 114.
- الهنائي، علي، تطبيقات الذكاء الاصطناعي في المجال الأمني (دراسة مُطبقة على دول مجلس التعاون لدول الخليج العربية)، كلية الحقوق، جامعة مدينة السادات، مصر، المجلد 10، العدد 4، ديسمبر 2024، الصفحة 2633-2558، 2024.
- يعقوب، ابتهال وآخرون، "مؤشر مقترح الإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق الأوراق المالية على وفق المتطلبات الدولية": دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد 1، 2022.
- يوسف، أحمد، أهمية تطبيق "الذكاء الاصطناعي في تعزيز أمن المعلومات بالقطاع الخدمي علم الخدمة مدخلا"، الملتقى العلمي الوطني الرابع حول: "الاتجاهات العالمية الحديثة في مجال تسويق الخدمات – النماذج والممارسات- بتقنية التحضر عن بعد". جامعة حسيبة بن بوعلي الشلف، الجزائر، 2021.

ثالثاً) المراجع الأجنبية

References

- A survey on deep learning for cybersecurity: *Progress, challenges, and opportunities*. *Computer Networks*.108740 ،207 ، https://doi.org/10.1016/j. comment108740. 2022.
- American Scientific Research Journal for Engineering, Zhejiang Normal University – China. Technology, and Sciences. Vol. 31.
- Bishop, Christopher, *Pattern Recognition and Machine Learning*, Springer. http://research.microsoft.com/cmbishop.
- Blattman, Christopher. *Building Women's Economic and Social*. 2013.
- Buczak, A. L & ،.Guven, E. A *Survey of Data Mining and Machine Learning*. 2022.
- Caldwell, D & ،.Williams, R. *Artificial intelligence and national security .Journal of Cyber Policy*, .18–1 ،(1)7. 2022.
- Canadian Institute for Cybersecurity. CIC-IDS 2017Dataset". University of New Brunswick. 2017.
- Crevier, D. *AI: The Tumultuous History of the Search for Artificial Intelligence*. https://www.amazon.com/*Ai-Tumultuous-History-Artificial-Intelligence*/dp/0465029973. 1993.
- Farahnakian, F ،.Heikkonen, J & .Plosila, J. "Deep auto-encoder based approach for intrusion detection system." In *Proceedings of the International Conference on Advanced Communication Technology (ICACT).* 2018 .
- Floridi, L., *Ethics of Artificial Intelligence*, Oxford University Press. https://global.oup.com/academic/product/the-ethics-of-artificial-intelligence-9780198883098.
- Gamage, T. T. Samarabandu, J & ،.Sidhu, I.. "*Deep learning methods in network intrusion detection.*" *Journal of Network and Computer Applications.*102733 ،168https://doi.org/10.1016/j. jnca.2020.102733. 2020.
- Gartner, *AI in Cyber Risk Management*.
- Goodfellow, I ،Shlens, J & Szegedy, C. "*Explaining and harnessing adversarial examples*", *arXiv preprint* ،arXiv:6572 .1412. 2014.
- Goodfellow, I. et al. Deep Learning, MIT Press. http://www.deeplearningbook.org. 2016.
- IBM, *Security Orchestration and Automation.*
- Kaplan, J., "*Artificial Intelligence: What Everyone Needs to Know",* Oxford University Press. Oxford University.
- Kshetri, N., *Cybersecurity and Cyberwar*.
- Kurakin, A ،.Goodfellow, I & ،.Bengio, S. "*Adversarial examples in the physical world*", *arXiv preprint* ،arXiv:1607.02533. 2016.
- McCarthy, J, "*What Is Artificial Intelligence?"* Stanford University, http://www-formal.stanford.edu/jmc/. 2007.
- *Methods for Cyber Security Intrusion Detection*.
- Mirsky, Y., Doitshman ،T., Elovici, Y & ،.Shabtai, A، Kitsune: An ensemble of autoencoders for online network intrusion detection. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. 2018.
- Mitchell, T. *Machine Learning*, McGraw-Hill Science/Engineering/Math.
- MITRE Corporation.(2022) . MITRE ATLAS: "*Adversarial Threat Landscape for AI Systems*." MITRE. 1997.
- National Institute of Standards and Technology (NIST). "*Artificial Intelligence Risk Management Framework (AI RMF 1.0)*." U.S. Department of Commerce. 2023.
- NIST, Keller. *Cybersecurity Framework* helping organizations to better understand and improve their management of cybersecurity risk. 2013.

- Nunnally, J.C. and Bernstein, I.H. The Assessment of Reliability. Psychometric Theory, 3, 248-292. 1994.
- Nye, J., *Cyber Power*, Harvard University.
- Russell, S., Norvig, P. *Artificial Intelligence: A Modern Approach*, Pearson. 2021.
- SANS Institute. "*AI and its growing role in cybersecurity*". SANS Institute. 2024.
- Shaukat, K., et al. "*A survey on machine learning techniques for cybersecurity in the last decade." IEEE Access*.222354–222310 ،8 ، https://doi.org/10.1109/ACCESS.2020.3046215. 2020.
- Sommer, R., Paxson, V., *Outside the Closed World*.
- Stallings, W., *Network Security Essentials*.
- Tavallaee, M ،.Bagheri, E., Lu, W & Ghorbani, A. A. "*A detailed analysis of the KDD CUP 99 data set*". In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009.
- Whitman, M., Mattord, H., "*Principles of Information Security".* Fourth Edition. ISBN-13: 978-1-111-13821-9. Boston, USA.
- World Economic Forum. "*Global Cybersecurity Outlook*." WEF. 2023.

رابعاً) المواقع الإلكترونية

- 10حالات استخدام شائعة للذكاء الاصطناعي في مجال الأمن السيبراني وأمثلة عليها -https://es-la.tenable.com/cybersecurity-guide/learn/10-common-ai-cybersecurity-use-cases-and-examples، آخر تحديث 28 يناير 2026.
- Ahmed, M. et al., "*Network Anomaly Detection".*
- Buczak, A., Guven, E., "*A Survey of Data Mining and Machine Learning."*
- Chandola, V., "*Anomaly Detection: A Survey".*
- Churchland, P. Neurophilosophy. The MIT Press. ISBN: 9780262530859. 1989.
- Gartner, *AI in Cyber Risk Management*.
- https://2mnm3lomaty.blogspot.com/p/information-security.html.
- https://ar.wikipedia.org/wiki/
- https://aws.amazon.com/ar/what-is/artificial-general-intelligence/
- https://jdl.journals.ekb.eg/article_395429.html
- https://www.bing.com.
- https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html.
- https://www.cisco.com/site/us/en/solutions/security/zero-trust/index.html.
- https://www.europarabct.com.
- https://www.for9a.com/specialities/AA-Cyber-Security.
- https://www.ibm.com/qa-ar/think/topics/artificial-superintelligence
- https://www.instagram.com/reel/DTgS-LXkxN9/
- https://www.oracle.com/middleeast-ar/artificial-intelligence/machine-learning/what-is-machine-learning
- https://www.rmg-sa.com.
- journals.ekb.eg.
- MITRE ATLAS Official Website.
- NIST AI RMF Publications Portal.
- SANS Cybersecurity Research Library.
- أنواع الذكاء الاصطناعي، https://www.google.com/search.
- أنواع تهديدات الأمن السيبراني - https://bakkah.com/ar/knowledge-center/.

- التحديات التي تواجه الأمن السيبراني https://www.bing.com.
- توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، https://bakkah.com/ar/knowledge-center/ - آخر تحديث Jan 2025.
- الذكاء الاصطناعي الضيق - https://mittrarabia.com/technodad.
- الذكاء الاصطناعي الفعال: كيف يعمل و7 حالات استخدام حقيقية https://www.exabeam.com/ar/explainers/ai-cyber-security/agentic-ai-how-it-works-and-7-real-world-use-cases.
- ما المقصود بالتعلم العميق؟ - شرح "التعلم العميق" بالذكاء الاصطناعي-AWS.amazon.com/ar/what-is/deep - learning/.

خامساً) المجلات والدوريات

- بوقرين عبد الحليم، قانون مكافحة جرائم تقنية المعلومات الكويتي: دارسة مقارنة، الكويت، مجلة كلية القانون الكويتية العالمية، جامعة عمار ثليجي الاغواط – الجزائر، 2017، العدد 20.
- الجنفاوي، خالد، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية لآداب والدراسات الإنسانية،2021، مج 5، العدد 19.
- حسين، حمدي، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي، برلين، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي، 2015، المجلد 2، العدد 5.
- شرمالي، فتيحة، الجهود الدولية لمكافحة الجريمة المنظمة العابرة للحدود، مذكر ة لنيل شهادة الماستر في القانون الخاص، كلية الحقوق والعلوم السياسية، لقسم القانون الخاص، مجلة الدراسات القانونية والاقتصادية، دورية علمية محكمة (- ISSN: 2356 9999)9492، 2015.
- الطيار، حسين، الأمن السيبراني في منظور مقاصد الشارع :دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائل، مجلة جامعة الطائل للعلوم الإنسانية، 2020، المجلد 6، العدد 21.
- عطايا، إبراهيم، الجريمة الإلكترونية وسبل مواجهتها في التشريع الاسلامي والانظمة الدولية، دراسة تحليلية تطبيقية، طنطا، مجلة كلية الشريعة والقانون، 2015، المجلد ،30 العدد 2، ص 373.
- العنزي، زينب، الجريمة الإلكترونية في ميزان الفقه والقانون، العراق، مجلة الدراسات الاسلامية والبحوث الأكاديمية، 2023، العدد 99،.
- المري، راشد، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، مجلة الشريعة والقانون بدمنهور، 2023، العدد 40.