Employing Artificial Intelligence in Cybersecurity and its Effectiveness in Combating Cybercrime and Predicting Future Cybercrimes

Mohammad A. Qerbaa[(1)*] **Salim A. Al-Qaisi**[(2)]

(1) Researcher, Mu'tah University, Karak - Jordan.
(2) Professor, Department of Sociology, Faculty of Social Sciences, Mutah University, Karak - Jordan.

Received: 11/3/2026
Accepted: 23/4/2026
Published: 30/6/2026

*** *Corresponding Author:***
qerbaa2020@gmail.com

DOI:https://doi.org/10.59759/art.v5i2.2003

Abstract

This study aimed to analyze the utilization of artificial intelligence (AI) in the field of cybersecurity and its effectiveness in combating cybercrime and predicting future cybercrimes. The descriptive-analytical method was employed. A questionnaire consisting of 20 items was developed and its validity and reliability were verified before being distributed to a purposive sample of 60 employees from the Cybercrime Unit of the Public Security Directorate and the National Cybersecurity Center. The results indicated a high level of AI's impact on combating cybercrime. They also revealed a positive correlation between the level of AI utilization in the Cybercrime Unit and the National Cybersecurity Center and its effectiveness in fighting cybercrime. Furthermore, the findings showed that employing AI techniques significantly contributed to predicting future cybercrimes, demonstrating a positive effect of AI implementation in cybersecurity on cybercrime forecasting. Based on these results, it is recommended to adopt a comprehensive national institutional strategy to enhance AI deployment in cybersecurity operations. This strategy should focus on continuously updating digital infrastructure, developing intelligent systems, integrating AI into daily operational processes, and establishing clear regulatory frameworks to ensure the safe and ethical use of these technologies within security institutions.

Keywords: Artificial Intelligence, Cybersecurity, Cybercrime, Prediction, Cybercrimes.

توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانيه المستقبلية

محمد أحمد قرباع[1] سليم أحمد القيسي[2]

(1) باحث، جامعة مؤتة، الكرك- الأردن.

(2) أستاذ، قسم علم الاجتماع، كلية العلوم الاجتماعية، جامعة مؤتة، الكرك – الأردن.

ملخص

هدفت هذه الدراسة إلى تحليل توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية، تم استخدام المنهج الوصفي التحليلي. تم تطوير استبيان يتضمن 20 فقرة وتم التحقق من صدقه وثباته قبل توزيعه على عينة قصدية بلغت (60) عاملاً من العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني، وكانت أبرز نتائج الدراسة ان هناك تأثير للذكاء الاصطناعي على مكافحة الجريمة الإلكترونية وبدرجة مرتفعة، ووجود علاقة ارتباطية طردية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الالكترونيه والمركز الوطني للامن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية، كما أبرزت نتائج الدراسة أن توظيف الذكاء الاصطناعي أسهم في التنبو بالجرائم السيبرانيه المستقبليه وبدرجة مرتفعة، ووجود أثر ايجابي لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني على التنبؤ بالجرائم السيبرانية المستقبلية، وبناءً على هذه النتائج، توصي الدراسة بتبني استراتيجية وطنية مؤسسية شاملة لتعزيز توظيف الذكاء الاصطناعي في العمل الأمني السيبراني، تقوم على التحديث المستمر للبنية التحتية الرقمية، وتطوير الأنظمة الذكية، ودمج الذكاء الاصطناعي في العمليات التشغيلية اليومية، مع وضع أطر تنظيمية واضحة تضمن الاستخدام الأمن والأخلاقي لهذه التقنيات داخل المؤسسات الأمنية.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، الجريمة الإلكترونية، التنبؤ، الجرائم السيبرانية.

المقدمة.

شهد العالم خلال العقدين الأخيرين طفرة تكنولوجية متسارعة أحدثت تغييرات جذرية في بنية المجتمعات وأنماط التفاعل الإنساني، حيث بات الاعتماد على الفضاء الرقمي واسعًا في مجالات الاقتصاد، والتعليم، والصحة، والاتصالات، والخدمات الحكومية. وقد رافق هذا التحول الرقمي العالمي تزايد ملحوظ في معدلات الجرائم الإلكترونية، سواء من حيث حجمها أو مستوى تعقيدها أو الأدوات المستخدمة في تنفيذها. فقد تطورت الجريمة الإلكترونية من مجرد اختراقات بسيطة

تستهدف الأنظمة المحدودة إلى جرائم منظمة تعتمد على شبكات دولية، وبنى تحتية تقنية متقدمة، وأساليب احتيال معقدة تتجاوز الحدود الجغرافية، مما جعلها من أبرز التحديات الأمنية على مستوى العالم (علاي ،2023).

ومنذ دخول الذكاء الاصطناعي إلى مجالات الحياة كافة، برز دوره في إعادة تشكيل طبيعة الجرائم الإلكترونية بشكل واضح. كما ظهرت أنماط جديدة من الجرائم تعتمد على الذكاء الاصطناعي مثل تزوير الهوية باستخدام التزييف العميق، وهجمات الاصطياد الاحتيالي المدعومة بخوارزميات توليد اللغة، وهجمات الاختراق الذاتي التطورية، والبرمجيات الخبيثة القادرة على التعلم والتكيّف مع أنظمة الحماية. كون هذه الجرائم السيبرانية المستحدثة تتميز بأنها عابرة للحدود، سريعة التطور، يصعب اكتشافها أحيانًا، وتتطلب أدوات متقدمة للوقاية منها أو مكافحتهاوهذا التطور المتسارع منح المجرمين قدرة أكبر على إخفاء هوياتهم، وتجاوز أنظمة الأمن التقليدية، وتنفيذ هجمات واسعة النطاق تستهدف أفرادًا ومؤسسات وقطاعات حيوية (استراتيجية المركز الوطني للامن السيبراني الأردني، 2025).

في المقابل، سُخِّر الذكاء الاصطناعي أيضًا في تعزيز الأمن السيبراني عالميًا عبر أنظمة قادرة على تحليل السلوك الشبكي، ورصد الأنماط غير الطبيعية، والتنبؤ بالهجمات قبل وقوعها، مما جعل الصراع بين المهاجمين ومُطوري أنظمة الدفاع السيبراني أكثر تعقيدًا وديناميكية. وبالتالي أصبح الذكاء الاصطناعي عنصرًا مزدوج التأثير، فهو أداة للوقاية والحماية بقدر ما قد يُستغل في الهجوم والاختراق.

حيث يسعى علم الجريمة إلى دراسة مدى ثأثير هذه الأنماط الجديدة على المجتمع الذي بدوره كان قادراً على التطور والتغير والتكيف وفقاً لمرور الزمن بناءً على المتغيرات البيئية والثقافية والتحولات التكنولوجية المتزايدة التي أوصلتنا إلى الذكاء الاصطناعي والذي يعد تحولاً نوعياً يضفي ظاهرة جديدة للمجتمع في التفاعلات الاجتماعية (جندل، 2022).

لقد أحدثت هذه الجرائم تحديات قانونية وأمنية جديدة، إذ غالبًا ما تسبق تطوراتها التشريعات القائمة، وتضع سلطات إنفاذ القانون أمام صعوبات كبيرة في إثباتها أو تتبع مرتكبيها، خاصة في ظل طبيعتها الرقمية واللامادية، واعتمادها على هوية مخفية وأدوات متطورة.

كما يُسهم الاتصال الرقمي بشكل كبير في توسّع نطاق الجريمة الإلكترونية، حيث أدى الانتشار الواسع للإنترنت ووسائل التواصل الاجتماعي إلى تسهيل ارتكاب الجرائم العابرة للحدود،

وإخفاء الأدلة الرقمية أو محوها بسرعة، مما يزيد من تعقيد عملية التحقيق الجنائي. كما أن البيئة الرقمية أتاحت للمجرمين فرصًا أكبر لاستهداف الأفراد والمؤسسات من خلال وسائل متعددة مثل الاختراق والاحتيال الإلكتروني، الأمر الذي يتطلب تطوير آليات حديثة لمكافحة هذه الجرائم وتعزيز قدرات الأجهزة الأمنية. وفي هذا السياق، تشير الدراسات الحديثة إلى أن الجريمة الإلكترونية تتميز بطابعها العالمي وصعوبة تتبعها نظرًا لاعتمادها على تقنيات الاتصال الرقمي المتقدمة وسرعة انتقال البيانات عبر الشبكات.

وعلى المستوى الإقليمي والعربي، لم تكن الدول بمنأى عن هذا التحول، إذ سجلت العديد من التقارير ارتفاعًا في معدلات الجريمة الإلكترونية، خصوصًا مع الانتشار المتزايد للخدمات الرقمية والتحول إلى الحكومات الإلكترونية. ويُعد الأردن من الدول التي خطت خطوات متقدمة في مجال التحول الرقمي على مستوى الخدمات الحكومية والمالية والتعليمية، الأمر الذي انعكس تلقائيًا على زيادة المخاطر الإلكترونية التي تستهدف البنى الرقمية الوطنية. وتشير تقارير الأمن السيبراني الأردنية إلى تزايد ملحوظ في محاولات الاختراق، والاحتيال الإلكتروني، وهجمات الهندسة الاجتماعية، ومحاولات استغلال البيانات، خصوصًا مع توسّع استخدام الذكاء الاصطناعي عالميًا.

وفي ضوء ما يشهده الأردن من توسّع متسارع في تبنّي التقنيات الرقمية وتقديم الخدمات الحكومية والمالية والتعليمية عبر منصات إلكترونية متقدمة، يبرز بوضوح تأثير الذكاء الاصطناعي على طبيعة وأنماط الجريمة الإلكترونية داخل المجتمع الأردني الذي يمثل مجتمع الدراسة في هذه الأطروحة. فقد أدى التحول الرقمي المحلي إلى ظهور جرائم إلكترونية أكثر تعقيدًا، تتضمن استخدام تقنيات الذكاء الاصطناعي في التمويه، وصناعة هجمات احتيالية دقيقة، ومحاولة تجاوز أنظمة الحماية التقليدية بوسائل متطورة (استراتيجية المركز الوطني للأمن السيبراني الأردني، 2025).

وفي المقابل، تسعى الجهات الأمنية الأردنية—وخاصة وحدة مكافحة الجرائم الإلكترونية—إلى توظيف تطبيقات الذكاء الاصطناعي لتعزيز قدراتها في الكشف المبكر عن الهجمات، وتحليل الأنماط السلوكية المشبوهة، والاستجابة بسرعة وفعالية للتهديدات الرقمية. ونتيجة لهذا التفاعل بين الاستخدامات الإجرامية والدفاعية للذكاء الاصطناعي، باتت البيئة الرقمية الأردنية تواجه تحديات نوعية تتطلب فهماً معمقاً لطبيعة هذه التطبيقات، وتأثيرها المباشر على المجتمع الأردني وقطاعاته الحيوية.

ومن هنا تأتي هذه الدراسة التي تسعى إلى تحليل توظيف الذكاء الاصطناعي في مجال

الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية من منظور العاملين في وحدة الجرائم الإلكترونية.

مشكلة الدراسة وأسئلتها

شهد المجتمع الأردني تطورًا هائلًا في تقنيات الذكاء الاصطناعي، وأصبح من الممكن توظيف هذه التقنيات بشكل متزايد في مجال الأمن السيبراني بهدف تعزيز الحماية الرقمية، وكشف الهجمات الإلكترونية، والتنبؤ بها قبل وقوعها، وبرز الذكاء الاصطناعي في التأثير على طبيعة وأنماط الجريمة الإلكترونية في المجتمع الأردني، سواء من حيث أساليب الهجوم أو من حيث آليات الدفاع والوقاية. فالذكاء الاصطناعي أصبح عاملاً رئيسًا يعيد تشكيل المشهد الأمني والجرمي، ويمثل تحديًا إستراتيجيًا للأجهزة الأمنية ووحدات الجرائم الإلكترونية في الأردن، التي تواجه اليوم جرائم أكثر تطورًا، وأدواتٍ أكثر تعقيدًا، وخصوصًا يمتلكون مهارات رقمية تتجاوز القدرات التقليدية وعند توظيف الذكاء الاصطناعي في مجال الأمن السيبراني لم يخلُ من إشكالات جوهرية، لعل أبرزها أنه – وبنفس القدر – يُستغل من قبل المجرمين السيبرانيين لتطوير أساليب أكثر تعقيدًا وذكاءً في تنفيذ الجريمة، مما يخلق سباقًا تقنيًا بين الجهات الأمنية والمجرمين.

وتكمن مشكلة الدراسة في التناقض القائم بين الدور الإيجابي في توظيف الذكاء الاصطناعي في دعم الأمن السيبراني، وبين احتمالات استخدامه كسلاح مضاد في يد مجرمي الفضاء الرقمي، مما يؤدي إلى ظهور أنماط مستحدثة من الجريمة يصعب اكتشافها أو إثباتها، ويُحدث تحديات قانونية وأمنية غير مسبوقة.كما تُطرح تساؤلات حول مدى فعالية هذه التوظيفات ، ومدى جاهزية المؤسسات الأمنية للتعامل معها، فضلًا عن الأطر الأخلاقية والتشريعية المنظمة لهذا الاستخدام، مما يجعل من الضروري دراسة هذا التوظيف بشكل علمي منهجي للكشف عن آثاره على تطور الجريمة السيبرانية ومكافحتها.

وعلى الرغم من التطور المتسارع في تقنيات الذكاء الاصطناعي، وتزايد الاعتماد على الأنظمة الرقمية في مختلف القطاعات، إلا أن الجرائم الإلكترونية والتهديدات السيبرانية تشهد تنامياً مستمراً من حيث التعقيد والأساليب المستخدمة. كما أن العديد من المؤسسات لا تزال تعتمد على أساليب تقليدية في الحماية والاستجابة، تقوم على رد الفعل بعد وقوع الهجوم بدلاً من التنبؤ به ومنعه مسبقاً.

وتكمن المشكلة البحثية في عدم وضوح مستوى توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية، إضافة إلى محدودية الدراسات التي تناولت أثر هذا التوظيف في القدرة على التنبؤ بالجرائم السيبرانية المستقبلية في البيئة محل الدراسة.

أسئلة الدراسة

- هل توجد علاقة ذات دلالة احصائية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية؟
- هل يسهم توظيف الذكاء الاصطناعي اسهاما ذا دلاله احصائية في التنبو بالجرائم السيبرانيه المستقبليه؟

أهمية الدراسة

أولاً: الأهمية النظرية

تنبع أهمية هذه الدراسة من كونها تسهم في إثراء الأدبيات العلمية التي تربط بين متغيري الذكاء الاصطناعي والأمن السيبراني، من خلال تقديم إطار تحليلي يوضح طبيعة العلاقة بين توظيف الذكاء الاصطناعي وفاعلية مكافحة الجريمة الإلكترونية. كما تدعم الاتجاهات البحثية الحديثة التي تركز على النماذج التنبؤية في إدارة المخاطر السيبرانية، وتسهم في سد فجوة معرفية في الدراسات العربية في هذا المجال.

ثانياً: الأهمية التطبيقية

تتمثل الأهمية التطبيقية للدراسة في تقديم نتائج علمية يمكن أن يستفيد منها صانعو القرار ومديرو أنظمة المعلومات في المؤسسات الحكومية والخاصة، بما يعزز من قدرتهم على تبني حلول قائمة على الذكاء الاصطناعي لرفع مستوى الجاهزية السيبرانية. كما تسهم نتائج الدراسة في دعم تطوير السياسات والاستراتيجيات الوطنية المتعلقة بمكافحة الجريمة الإلكترونية، وتوجيه برامج التدريب وبناء القدرات نحو الاستخدام الفاعل للتقنيات الذكية في المجال الأمني.

أهداف الدراسة

تهدف هذه الدراسة إلى:

- التعرف على العلاقة بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية.
- قياس مدى إسهام توظيف الذكاء الاصطناعي بشكل ذي دلالة إحصائية في التنبؤ بالجرائم السيبرانية المستقبلية.

التعريفات النظرية والاجرائية لمفاهيم الدراسة

الذكاء الاصطناعي: هو فرع من علوم الحاسوب يهدف إلى تطوير أنظمة وبرامج قادرة على محاكاة الذكاء البشري، من خلال التعلم، التفكير، التحليل، واتخاذ القرارات. يعتمد الذكاء الاصطناعي على الخوارزميات المتقدمة والتعلم الآلي والشبكات العصبية الاصطناعية لمعالجة البيانات واتخاذ الإجراءات بناءً عليها.

الجريمة: فعل أو امتناع عن فعل يخالف القانون، ويعاقب عليه بموجب القوانين والتشريعات المعمول بها في المجتمع.

الأمن السيبراني: هو مجموعة من الإجراءات والتقنيات المصممة لحماية الأنظمة الرقمية، والشبكات، والبيانات من الهجمات الإلكترونية أو الوصول غير المشروع. ويمثل الإطار الذي تُستخدم فيه تقنيات الذكاء الاصطناعي لأغراض الحماية والكشف.

جرائم الأمن السيبراني (الجريمة الإلكترونية): هي أي نشاط إجرامي يتم تنفيذه عبر الفضاء الإلكتروني، باستخدام أجهزة الحاسوب أو الشبكات أو الإنترنت، بهدف إلحاق الضرر بالأفراد أو المؤسسات أو الحكومات. تشمل هذه الجرائم اختراق الأنظمة، سرقة البيانات، الاحتيال الإلكتروني، التجسس، ونشر البرمجيات الضارة.

توظيف الذكاء الاصطناعي: يشير إلى استخدام وتطبيق تقنيات الذكاء الاصطناعي في البيئات الأمنية الرقمية، سواء في كشف الجرائم، التنبؤ بها، تحليل الأدلة الرقمية، أو رصد الهجمات السيبرانية.

حدود الدراسة

تتحدد الدراسة الحالية فيما يأتي:

- **الحدود الموضوعية:** " توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية.
- **الحدود البشرية:** "استجابات أفراد الدراسة من العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني على فقرات الاستبانة".
- **الحدود المكانية:** تم تطبيق الدراسة في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني في المملكة الأردنية الهاشمية.
- **الحدود الزمانية:** تم تطبيق الدراسة ضمن الفصل الدراسي الأول 2025 – 2026 م.

الدراسات السابقة

تمت مراجعة الدراسات السابقة ذات العلاقة بموضوع الدراسة بغرض تحليل النتائج وربطها بالدراسة الحالية، وتقديم الاقتراحات والتوصيات بناءً على الاتفاق أو الاختلاف مع تلك الدراسات السابقة:

أولاً: الدراسات العربية

هدفت دراسة الرواشدة، صباح عادل عارف (2025) إلى التعرف إلى دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في مديرية الأمن العام الأردنية/ وحدة الجرائم الإلكترونية .تمثل مجتمع الدارسة في المديرية موظفي وحدة الجرائم الإلكترونية في مديرية الأمن العام الأردنية. وتم استخدام أسلوب المقابلة والعينة القصدية لغايات تمثيل مجتمع الدراسة، وبلغت عينة الدراسة (132) واعتمدت الدراسة المنهج الوصفي التحليلي لتحقيق أهدافها. تم استخدام الإستبانة لجمع البيانات، وأظهرت نتائج تحليل إجابات أفراد العينة أن هناك دوراً للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية.

هدفت دراسة محمد قاسم ، مراد محمد غالب (2024) إلى معرفة دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وكيف ساهمت السلطات الرقمية وتقنيات التنبؤ بالجرائم في منع وتقليل الجرائم الإلكترونية وما هو دور بعض التشريعات العربية في تنظيم مكافحة الجريمة الإلكترونية والآلية المتبعة لمواجهتها ولتحقيق أهداف الدراسة استخدم المنهج الوصفي التحليلي لمعرفة آلية استخدام الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية، والمنهج المقارن من

خلال المقارنة بين الأنظمة القانونية ودورها في مكافحة الجريمة الإلكترونية . أبرزت الدراسة نتائج أن الذكاء الاصطناعي أصبح حاجزًا فعّالًا ضد الجرائم الإلكترونية في الدول المتقدمة ويسهم بشكل كبير في تقليل الجرائم من خلال التنبؤ بجري الشخصيات الإجرامية وتواجه التشريعات العربية تحديات في استيعاب التطور التقني؛ حيث تنقسم بين تعديل القوانين القديمة أو وضع تشريعات جديدة.

هدفت دراسة عزيز، محمد الخزامي (2023) الى تمثيل دور الذكاء الاصطناعي في مجالات العلوم الاجتماعية والإنسانية، وكما هدفت ايضا الى التعرف على التعاريف المختلفة للذكاء الاصطناعي ومراحل تطوره والتعرف على مراحل تطور الذكاء الاصطناعي وعلاقته التبادلية مع العلوم الاجتماعية والإنسانية وعرض بعض التطبيقات للذكاء الاصطناعي في مجال العلوم الاجتماعية والانسانية. اتبعت الدراسة المنهج الوصفي النظري، من خلال مراجعة الأدبيات المتخصصة والنماذج التطبيقية المتاحة حول التكامل بين الذكاء الاصطناعي والمجالات الاجتماعية والإنسانية. وتوصلت الدراسة للنتائج أن الذكاء الاصطناعي وسّع حدود المعرفة إلى مستويات غير مسبوقة، داعمًا التنوع والعمق في العلوم الاجتماعية والإنسانية. وبات بالإمكان دمج البيانات التكنولوجية مع التحليلات الثقافية والسلوكية، مما خلق مساحات بحثية جديدة. وتقنيات الذكاء الاصطناعي حسّنت من كفاءة إنتاج البحث ودقته، إضافة إلى تسريع العمليات المعرفية.

هدفت دراسة اشتية والكفارنة (2022) إلى توضيح الدور الذي يمكن أن يلعبه الذكاء الاصطناعي في التنبؤ بالجرائم، وتحليل البيانات الأمنية، والكشف عن الأنماط السلوكية المسبقة التي تساعد على منع وقوع الجرائم. كما ركزت على إمكانية دمج تقنيات الذكاء الاصطناعي ضمن الاستراتيجيات الأمنية في فلسطين. وتم استخدم المنهج الوصفي التحليلي بالإضافة إلى الجانب التطبيقي من خلال تحليل بعض البيانات الأمنية وربطها بتقنيات الذكاء الاصطناعي. توصلت الدراسة إلى أن الذكاء الاصطناعي يمثل أداة فاعلة في خفض معدلات الجريمة إذا ما تم توظيفه بشكل صحيح، حيث يُسهم في رصد وتحليل الأنماط السلوكية الإجرامية والكشف المبكر عن التهديدات وتعزيز قدرة الأجهزة الأمنية على الاستجابة السريعة. بينما الدراسة الحالية تركز على الأمن السيبراني والجرائم الإلكترونية.

هدفت دراسة عبد الرازق (2021) إلى التعرف على تأثير استخدام الذكاء الاصطناعي على ارتكاب الجرائم المعلوماتية، وذلك نظرًا لاستحداث عدد من الجرائم الفنية المستمدة من التقنية المعلوماتية. فبعض المجرمين اتجهوا لاستخدام الوسائل التقنية المستحدثة لتنفيذ جرائمهم، فكانت

محل اهتمام رجال القانون والمختصين من أجل إيجاد الحلول المناسبة لقمعها ومكافحتها. لذلك سارعت الكثير من الدول المتقدمة والدول العربية، للتصدي لتلك الظاهرة، وذلك بتشريع وسن القوانين التي تمنع من ارتكاب مثل تلك الجرائم. واعتمدت الدراسة على المنهج الوصفي التحليلي بالإضافة إلى الاستعانة بالمنهج المقارن، واشتملت الدراسة على ثلاثة مباحث وبينت ماهية الذكاء الاصطناعي والجريمة الإلكترونية، وطبيعتها القانونية، وخصائصها، والتعرف على صور الجرائم المعلوماتية وعلاقتها بمجال الذكاء الاصطناعي، والتعرف على موقف التشريع السعودي والمصري بشأن مكافحة جرائم تقنية المعلومات، ومن أبرز النتائج أن الذكاء الاصطناعي يلعب دورًا مهمًا في زيادة الجرائم الإلكترونية وانتشارها.

هدفت دراسة الحجرف (2021) إلى استكشاف الكيفية التي يمكن أن يعزز بها الذكاء الاصطناعي من قدرات الأمن السيبراني، وذلك من خلال معالجة الهجمات الإلكترونية والتنبؤ بالثغرات الأمنية ودعم اتخاذ القرار الأمني. وتم استخدام المنهج الوصفي النظري من خلال تحليل الدراسات السابقة والنماذج العالمية التي دمجت الذكاء الاصطناعي بالأمن السيبراني. وأظهر البحث نتائج أن الذكاء الاصطناعي يُعد من الأدوات الجوهرية في مواجهة التحديات السيبرانية المعاصرة. وكما أبرزت الدراسة دور خوارزميات التعلم الآلي في اكتشاف الهجمات الإلكترونية بشكل أسرع وأكثر دقة مقارنة بالأنظمة التقليدية. وأكدت النتائج أن أنظمة الذكاء الاصطناعي قادرة على التعلم المستمر من الهجمات الجديدة والتكيف معها

ثانياً: الدراسات الاجنبية

شهدت العقود الأخيرة اهتماماً متزايداً من الباحثين الأجانب بدراسة العلاقة بين الذكاء الاصطناعي والأمن السيبراني، خصوصاً فيما يتعلق بالكشف عن الجرائم الإلكترونية والتنبؤ بها والحد من آثارها.

هدفت دراسة El-Kady (2025) إلى تحليل الدور الذي تلعبه تقنيات الذكاء الاصطناعي وتعلم الآلة في تعزيز كفاءة التحقيق الجنائي الرقمي، خاصة في مواجهة الجرائم المرتبطة بالدارك ويب والعملات الرقمية، حيث اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال استعراض الأدبيات والتطبيقات التقنية الحديثة. وابرز نتائج الدراسة كانت أن الذكاء الاصطناعي يمثل أداة محورية في كشف الأنماط الإجرامية المعقدة وتحليل البيانات الضخمة، كما يسهم في تتبع المعاملات الرقمية وتسريع عملية جمع الأدلة وتحليلها، رغم وجود تحديات تقنية وقانونية، مما

يؤكد ضرورة تطوير أدوات التحقيق وأساليب العمل الأمني لمواكبة التطورات في هذا المجال.

هدفت دراسة (Csongor & Tóth, 2024) إلى تحليل الهجمات العدائية المدعومة بالذكاء الاصطناعي في مجال الأمن السيبراني من منظور شامل يجمع بين الأبعاد التقنية والقانونية والأخلاقية، مع التركيز على الإشكاليات المرتبطة بالمسؤولية القانونية والحوكمة في ظل استخدام الأنظمة الذكية في العمليات الهجومية والدفاعية. واعتمدت الدراسة على المنهج التحليلي المقارن من خلال مراجعة الأدبيات المتخصصة وتحليل الإطارين القانوني والتقني لاستخدامات الذكاء الاصطناعي في الأمن السيبراني. وتوصلت إلى أن التطور المتسارع في تقنيات الذكاء الاصطناعي يخلق تحديات قانونية وأخلاقية معقدة، أبرزها غموض المسؤولية عند وقوع الأضرار الناتجة عن الأنظمة الذكية، وضرورة تطوير أطر تنظيمية وتشريعية متكاملة تضمن الاستخدام الأمن والمسؤول لهذه التقنيات، بما يعزز من فعالية الأمن السيبراني ويحد من المخاطر المرتبطة بالهجمات الذكية.

هدفت دراسة (Djenna et al., 2023) إلى تطوير نموذج متقدم يعتمد على تقنيات الذكاء الاصطناعي والتعلم العميق لتعزيز قدرات الأمن السيبراني في الكشف المبكر عن الهجمات الإلكترونية، وبشكل خاص هجمات البوت نت (Botnet)، وذلك ضمن سياق الجرائم الإلكترونية المعقدة. واعتمدت الدراسة على المنهج التجريبي التحليلي من خلال تصميم نموذج تعاوني يجمع بين الشبكات العصبية الالتفافية (CNN) ونماذج الذاكرة طويلة وقصيرة المدى (LSTM) لتحليل البيانات الشبكية واكتشاف الأنماط غير الطبيعية. وتوصلت الدراسة إلى أن النموذج المقترح حقق دقة عالية في الكشف عن الهجمات تجاوزت 98.7% مع انخفاض كبير في معدل الإيجابيات الخاطئة، مما يعكس فعالية الذكاء الاصطناعي في تحسين أنظمة كشف التهديدات وتعزيز التحقيق الجنائي الرقمي، إضافة إلى قدرته على رصد الأنماط الخفية والمتغيرة في الجرائم الإلكترونية بشكل أكثر سرعة وفعالية.

هدفت دراسة (Pum, 2022) إلى تحليل التحولات التي أحدثها استخدام الذكاء الاصطناعي في مجال الجرائم الإلكترونية، مع التركيز على الجرائم السيبرانية المدعومة بالتقنيات الذكية، وتحديد التحديات التي تفرضها هذه التحولات على السياسات العامة والأطر القانونية والأمنية. واعتمدت الدراسة على المنهج التحليلي النظري من خلال مراجعة الأدبيات المتخصصة وتحليل تطور أنماط الجرائم الإلكترونية في ظل استخدام تقنيات الذكاء الاصطناعي. وتوصلت إلى أن

دمج الذكاء الاصطناعي في تنفيذ الهجمات السيبرانية أسهم في ظهور أنماط جديدة من الجرائم المنظمة أكثر تعقيدًا واتساعًا، تعتمد على التعلم الآلي والتحليل التنبؤي لزيادة فعالية الهجمات، كما أبرزت الدراسة وجود فجوة واضحة في التشريعات الحالية وعدم كفايتها لمواجهة هذه التطورات، مما يستدعي تطوير أطر تنظيمية وقانونية دولية أكثر شمولية للحد من المخاطر المتزايدة وحماية البنى التحتية الرقمية.

هدفت دراسة (Zhang et al., 2022) إلى بحث دور الذكاء الاصطناعي التفسيري (Explainable AI – XAI) في تعزيز فعالية أنظمة الأمن السيبراني من خلال تحسين مستوى الشفافية وقابلية تفسير القرارات الصادرة عن النماذج الذكية، خاصة في سياق الكشف عن التهديدات والهجمات الإلكترونية. واعتمدت الدراسة على المنهج التحليلي المقارن من خلال مراجعة نماذج الذكاء الاصطناعي المستخدمة في الأمن السيبراني وتحليل مدى قابليتها للتفسير والثقة في نتائجها. وتوصلت الدراسة إلى أن اعتماد النماذج التقليدية ذات طبيعة "الصندوق الأسود" يحد من فهم آلية اتخاذ القرار ويؤثر على مستوى الثقة لدى الجهات الأمنية، في حين أن دمج تقنيات الذكاء الاصطناعي التفسيري يسهم في تعزيز الشفافية وتحسين قدرة المختصين على فهم وتحليل النتائج، مما يؤدي إلى رفع كفاءة الاستجابة للتهديدات السيبرانية وزيادة فعالية أنظمة الأمن الرقمي.

هدفت دراسة (Takermura, 2021) إلى تحليل تأثير تقنيات التنبؤ الجرمي (Predictive Policing) في مجال الأمن الجنائي، مع التركيز على مدى دقة وموثوقية استخدام الأنظمة الذكية في التنبؤ بالجرائم المستقبلية، إضافة إلى دراسة الإشكاليات الأخلاقية والقانونية المرتبطة بتوظيف هذه التقنيات. واعتمدت الدراسة على المنهج التحليلي النقدي من خلال مراجعة الأدبيات العلمية المتعلقة بالتنبؤ الجرمي وتحليل التطبيقات العملية لأنظمة الذكاء الاصطناعي في العمل الأمني. وتوصلت الدراسة إلى أن هذه الأنظمة، رغم فعاليتها في دعم اتخاذ القرار الأمني، إلا أنها قد تعاني من مشكلات تتعلق بالانحياز الناتج عن البيانات التاريخية المستخدمة في التدريب، مما يؤدي إلى إعادة إنتاج أنماط اجتماعية غير عادلة، كما أشارت إلى أن غياب الشفافية في خوارزميات العمل يخلق ما يُعرف بـ"الصندوق الأسود"، الأمر الذي يحد من قدرة الجهات الرقابية والقضائية على تقييم مخرجات هذه الأنظمة، ويستدعي تطوير أطر تنظيمية تضمن الاستخدام العادل والشفاف لهذه التقنيات في المجال الأمني.

التعقيب على الدراسات السابقة

اهم ما يميز هذه الدراسة الحالية بالمقارنة مع الدراسات السابقة هو البعد الميداني والتطبيقي كونه واضحًا، من خلال اجراء الاستبانة واستطلاع آراء العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني ، مما يجعل نتائجها أكثر ارتباطًا بالواقع العملي، ويعزز فهم تأثير الذكاء الاصطناعي على مكافحة الجرائم الرقمية والتنبؤ بها في السياق المحلي. إضافة إلى تبنيها منظورًا تكامليًا يربط بين توظيف الذكاء الاصطناعي وفاعلية مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم المستقبلية، وهو ما يمنحها قيمة علمية وعملية تسهم في دعم الجهود الأمنية وتطوير السياسات الوقائية في المجال السيبراني. أظهرت نتائج الدراسة الحالية توافقًا واضحًا مع عدد من الدراسات السابقة العربية والأجنبية في عدة جوانب، ومن أبرزها: **التوافق الاول:** فاعلية الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية ، اتفقت نتائج الدراسة الحالية مع ما توصلت إليه دراسات مثل (محمد قاسم ومراد محمد، 2024) و(عبد الرازق، 2021) و (El–Kady , 2025) ، و (Djenna et al., 2023) حيث أكدت جميعها أن الذكاء الاصطناعي يسهم بشكل فعّال في كشف الجرائم الإلكترونية وتحليلها من خلال معالجة كميات كبيرة من البيانات الأمنية بسرعة ودقة. **التوافق الثاني:** الدور التنبؤي للذكاء الاصطناعي، توافقت نتائج الدراسة مع دراسات (اشتية والكفارنة، 2022) و(الرواشدة، 2025) و (Takermura, 2021) التي أشارت إلى أن تقنيات الذكاء الاصطناعي قادرة على التنبؤ بالأنماط الإجرامية المستقبلية، وهو ما أكدته آراء أفراد العينة في الدراسة الحالية. **التوافق الثالث:** أهمية التحول نحو الأمن السيبراني اتفقت الدراسة مع (الحجرف، 2021)(Csongor & Tóth ,2024) في أن توظيف الذكاء الاصطناعي يعزز من الانتقال من الأساليب التقليدية (الاستجابة بعد وقوع الجريمة) إلى الأساليب الوقائية الاستباقية. التوافق الخامس: الحاجة إلى تطوير الكوادر والتشريعات، أكدت نتائج الدراسة الحالية – كما في دراسات (عزيز والخزامي، 2023) (Pum , 2022) – على ضرورة تأهيل الكوادر البشرية وتحديث التشريعات لمواكبة التطور التكنولوجي في مجال الذكاء الاصطناعي والأمن السيبراني. رغم هذا الاتفاق، أظهرت الدراسة الحالية بعض الاختلافات المهمة عن الدراسات السابقة، ومن أبرزها: الاختلاف الول: التركيز على الواقع الميداني مقابل الطابع النظري، اختلفت الدراسة الحالية عن العديد من الدراسات السابقة التي ركزت على الجانب النظري، حيث اعتمدت هذه الدراسة على آراء العاملين في الأجهزة الأمنية، مما أظهر صورة أكثر واقعية، وكشف عن بعض التحديات

التطبيقية التي لم تتناولها الدراسات السابقة بشكل كافٍ. الاختلاف الثاني: إبراز التحديات العملية في تطبيق الذكاء الاصطناعي حيث بينت نتائج الدراسة وجود معوقات تطبيقية مثل: نقص التدريب المتخصص، محدودية الموارد التقنية، التحديات القانونية وهذه الجوانب لم تحظَ بنفس العمق في بعض الدراسات السابقة التي ركزت على الإيجابيات أكثر من التحديات. الاختلاف الثالث: درجة فاعلية الذكاء الاصطناعي، بينما ذهبت بعض الدراسات إلى التأكيد على فاعلية عالية جدًا للذكاء الاصطناعي، أظهرت الدراسة الحالية أن الفاعلية مرتفعة ولكنها مشروطة بعوامل مثل: كفاءة الكوادر، توفر البنية التحتية، مستوى التنسيق المؤسسي الاختلاف الرابع : التركيز على السياق الأردني، تميزت الدراسة الحالية بتركيزها على البيئة الأمنية الأردنية، وهو ما أدى إلى نتائج قد تختلف نسبيًا عن دراسات أجريت في بيئات تكنولوجية أكثر تقدمًا، خاصة من حيث الإمكانات والموارد. يمكن تفسير هذا الاتفاق والاختلاف بعدة عوامل، من أهمها: اختلاف البيئة التطبيقية بين الدراسات (محلية vs دولية)، اختلاف المنهج المستخدم (نظري مقابل ميداني)، تطور التكنولوجيا بين وقت إجراء الدراسات المختلفة، اختلاف عينات الدراسة (خبراء، أكاديميون، عاملون ميدانيون).

المنهجية والتصميم

يتضمن هذا الجزء التعريف بمنهجية الدراسة ومجتمعها وعينتها وكذلك أداة الدراسة وأسلوب تصميمها والمؤشرات والمعايير العلمية والعملية للتحقق من صدق وثبات أداة الدراسة وكما يتضمن شرحاً وعرضاً تفصيلياً للمعالجات الاحصائية التي استخدمت من اجل الوصول إلى النتائج وتحليلها.

منهجية الدراسة

تم اعتماد المنهج الوصفي التحليلي، والذي يهدف هذا المنهج إلى وصف الظواهر المتعلقة بتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني بشكل دقيق وتأثيره على الجريمة، وتحليل توظيفاته المختلفة على الجريمة السيبرانية، وذلك للتعرف توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية.

مجتمع وعينة الدراسة

تكون مجتمع الدراسة من العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني وعددهم (130) فردا. وتم اختيار عينة الدراسة

بالطريقة القصدية وعددها (60) عاملاً من العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني وتم اختيار العينة كون طبيعة موضوع الدراسة يتطلب اختيار أفراد يمتلكون معرفة وخبرة مباشرة وعميقة في هذا المجال، وهو ما ينطبق على العاملين في كل من وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني. كما أن اختيار هذه العينة يضمن الحصول على بيانات دقيقة وذات مصداقية عالية، كونهم الأكثر احتكاكًا بالواقع العملي للذكاء الاصطناعي في المجال الأمني، والأكثر قدرة على تقييم مدى فاعليتها في كشف الجرائم والتنبؤ بها.

إضافة إلى ذلك، فإن طبيعة العمل في هذه المؤسسات الأمنية تجعل من الصعب الوصول إلى جميع الأفراد بطريقة عشوائية، مما يعزز من ملاءمة استخدام العينة القصدية باعتبارها الأنسب للدراسات النوعية أو الدراسات ذات الطابع الأمني المتخصص. كما أن هذا الاختيار يحقق هدف الدراسة المتمثل في الربط بين الجانب التقني والجانب الأمني التطبيقي، من خلال الاعتماد على خبرات ميدانية مباشرة تسهم في تقديم تقييم واقعي لفعالية الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية. واعتمدت عينة الدراسة على المتغيرات الديموغرافية من حيث " الجنس، العمر، عدد سنوات الخبرة الفعلية داخل مكان العمل، المؤهل التعليمي، ومكان العمل"واستنادا على ذلك تم وصف عينة الدراسة كالآتي:

الجدول (1): وصف عينة الدراسة وفق المتغيرات الديموغرافية لأفراد الدراسة

المتغير	الفئة	العدد	النسبة المئوية
الجنس	ذكر	33	55.0
	أنثى	27	45.0
العمر	من 20 سنة–29 سنة	9	15.0
	من 30سنة–39 سنة	33	55.0
	من 40 سنة–49 سنة	18	30.0
	50 سنة فأكثر	0	0.0
عدد سنوات الخبرة	أقل من 5 سنوات	21	35.0
	من 5–10سنوات	24	40.0
	من 11–15 سنة	6	10.0

المتغير	الفئة	العدد	النسبة المئوية
	أكثر من 15 سنة	9	15.0
المؤهل التعليمي	دبلوم	7	11.7
	بكالوريوس	42	70.0
	دراسات عليا	11	18.3
مكان العمل	وحدة الجرائم الإلكترونية	30	50.0
	المركز الوطني للأمن السيبراني	30	50.0
المجموع		60	100.0

يتبين لنا من الجدول (1) ما يلي:

1. بلغ عدد أفراد العينة من الذكور (33) بنسبة مئوية (55.0%)، بينما بلغ عدد الاناث (27) وبنسبة مئوية (45.0%).
2. بلغت أعلى نسبة مئوية لتوزيع أفراد العينة تبعاً لمتغير العمر (55.0%) لفئة العمر (من 30 سنة–39 سنة)، بينما بلغت أدنى نسبة مئوية (15.0%) لفئة العمر (من 20 سنة – 29 سنة).
3. بلغت أعلى نسبة مئوية لتوزيع أفراد العينة تبعاً لمتغير سنوات الخبرة (40%) لسنوات الخبرة (من 5 –10 سنوات)، بينما بلغت أدنى نسبة مئوية (10.0%) لسنوات الخبرة (من 11–15 سنة).
4. بلغت أعلى نسبة مئوية لتوزيع أفراد العينة تبعاً لمتغير المؤهل العلمي (70.0%) للمؤهل (بكالوريوس)، بينما بلغت أدنى نسبة مئوية (11.7%) للمؤهل (دبلوم).
5. بلغ عدد الذين يعملون في وحدة الجرائم الإلكترونية (30) وبنسبة مئوية (50.0%)، بينما بلغ عدد الذين يعملون في المركز الوطني للأمن السيبراني (30) وبنسبة مئوية (50.0%).

أداة الدراسة

تطلبت طبيعة الدراسة تطوير استبانة لجمع البيانات اللازمة لتحقيق أهداف الدراسة، وقد روعي في تطوير الاستبانة الدقة وإتباع القواعد والأسس المنهجية اللازمة لتحديد المحاور وصياغة الفقرات، وكذلك مراعاة الأساليب العلمية التي تمكن من توفير عناصر الاتساق والتكامل بين محاور الأداة، وقد تم تطوير أداة الدراسة، بعد إجراء المسح المكتبي والاطلاع على العديد من

الدراسات السابقة وذات الصلة بموضوعها مثل دراسة (قاسم وغالب، (2023) ، ودراسة (الرواشدة، 2025).

وقد تم إعداد أداة الدراسة "الاستبانة" بعد إجراء الخطوات المنهجية التالية:

أ. تنفيذ استطلاع أولي من خلال عرض الاستبانة بصورتها الأولية على عينة من مجتمع الدراسة مكونة من (15) من العاملين في وحدة الجرائم الإلكترونية التابعة لمديرية الأمن العام والعاملين في المركز الوطني للأمن السيبراني، تم من خلال هذا الاستطلاع الاستفادة من الآراء والاقتراحات المساعدة لتحديد محاور أداة الدراسة، وصياغة الفقرات في صيغتها الأولية.

ب. بعد إجراء التعديلات المقدمة من قبل العينة الاستطلاعية الأولية على أداة الدراسة تم عرضها على لجنة من أعضاء هيئة التدريس من أصحاب لاختصاص من أعضاء هيئة التدريس، وذلك بهدف التحقق من الصدق الظاهري للأداة، وقد بينت نتائج التحكيم قبول جميع فقرات ومحاور أداة الدراسة التي حازت على درجة اتفاق 80% من المحكمين وسوف يتم توضيح هذه المحاور تالياً.

ج. الاختبار التجريبي للاستبيان في ضوء الخطوتين السابقتين تم إعداد أداة الدراسة في صورتها شبه النهائية، والتي تم تطبيقها على عينة استطلاعية من مجتمع الدراسة تضم (15) عاملين، وذلك بهدف التحقق من الاتساق الداخلي للفقرات وثبات أداة الدراسة، ومدى إمكانية تطبيقها على عينة الدراسة الرئيسة للدراسة وتعميم النتائج.

تضمنت أداة الدراسة في صورتها النهائية الأجزاء والمحاور الرئيسة التالية:

الأول: متغيرات الدراسة المستقلة المتعلقة بخصائص عينة الدراسة، والتي تضم متغيرات الجنس، والعمر، وعدد سنوات الخبرة الفعلية داخل مكان العمل، والمؤهل التعليمي، ومكان العمل.

الثاني: ويشمل على (20) فقرة لقياس توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وتأثيره على الجريمة من وجهة نظر العاملين في وحدة الجرائم الإلكترونية والعاملين في المركز الوطني للأمن السيبراني وينقسم إلى محورين كالأتي:

المحور الأول: وتضمن على (10) فقرات ويهدف إلى قياس تأثير الذكاء الاصطناعي على مكافحة الجريمة الإلكترونية.

المحور الثاني: وتضمن على (10) فقرات ويهدف إلى قياس الذكاء الاصطناعي والتنبؤ بالجرائم

الإلكترونية المستقبلية.

صدق وثبات أداة الدراسة

أولاً: الصدق الظاهري

للتأكد من الصدق الظاهري لأداء الدراسة تم عرض أداة الدراسة بشكلها الأولي على (7) محكميين من الأساتذة أعضاء هيئة التدريس من أقسام كليات العلوم الاجتماعية والعلوم التربوية من جامعة مؤتة وجامعة اليرموك والجامعة الأردنية ، وذلك بهدف تحكيم الاستبانة وتقصي آرائهم حول مدى تحقيق محاورها لأهداف الدراسة، ومدى كفاية عدد الفقرات، وحاجة الفقرات للتعديل أو الإضافة أو الحذف، ومدى وضوح الصياغة اللغوية للفقرات، وقد قام السادة أعضاء لجنة المحكمين بوضع ملاحظاتهم من حيث مدى ملائمة ووضوح الفقرات، وتعديل بعض الفقرات وصياغتها باللغوية بطريقة أوضح.

وبناء على آراء لجنة التحكيم وملاحظاتها، تم تعديل فقرات أداة الدراسة التي أجمع 80% من أعضاء لجنة التحكيم على ضرورة تعديلها، والانتهاء إلى صياغة الاستبيان بشكله النهائي.

ثانيًا: الصدق البنائي:

لاستخراج دلالات صدق البناء لأداة الدراسة، تم استخراج معاملات الارتباط بين كل فقرة وارتباطها بالمحور الذي تنتمي إليه وبين الفقرة والاداة ككل، بحيث يتوافر شرطان رئيسيان لتلك المعاملات؛ هما: ان لا يقل معامل الارتباط المصحح عن (0.30)، ووجود دلالة احصائية لتلك المعاملات. والجدول (2) يبين قيم تلك المعاملات.

جدول (2): معاملات الارتباط بين الفقرة والدرجة الكلية والمحور التي تنتمي إليه

رقم الفقرة	معامل الارتباط المحور(1)*	معامل الارتباط مع الأداة*	رقم الفقرة	معامل الارتباط المحور(2)*	معامل الارتباط مع الأداة*
1	.805	.775	1	.793	.716
2	.759	.424	2	.770	.689
3	.814	.389	3	.874	.687
4	.849	.782	4	.805	.744

رقم الفقرة	معامل الارتباط المحور(1)*	معامل الارتباط مع الأداة*	رقم الفقرة	معامل الارتباط المحور(2)*	معامل الارتباط مع الأداة*
5	.779	.409	5	.817	.520
6	.845	.779	6	.704	.656
7	.782	.616	7	.651	.698
8	.838	.743	8	.620	.761
9	.841	.742	9	.818	.720
10	.827	.693	10	.886	.762

- دالة إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$).

يتبين لنا من الجدول (2) أن جميع قيم معاملات الارتباط بين الفقرة والمجال الذي تنتمي له وبين الفقرة والأداة ككل، هي قيم مقبولة وكافية لإجراء الدراسة.

ثبات أداة الدراسة:

من أجل التأكد من صحة وثبات المقياس المستخدم في إجراء الدراسة تم استخراج معامل الثبات كرونباخ ألفا، وذلك لمعرفة معامل ثبات الاتساق الداخلي لكل محور لمقياس الدراسة، ولمعرفة تلك القيم الجدول (3) يوضح ذلك:

جدول (3): معاملات الاتساق الداخلي (كرونباخ ألفا) لمحاور مقياس الدراسة

المحور	معامل كرونباخ ألفا
المحور الأول	0.843
المحور الثاني	0.857
المقياس ككل	0.902

يتبين لنا من الجدول (3) أن قيم معامل الثبات لمحاور الدراسة تراوحت بين (0.843–0.857)، وكما بلغت قيمته للمقياس ككل (0.902) هي قيم مرتفعة ومقبولة وكافيه لإجراء الدراسة.

أساليب المعالجة الإحصائية

عالجت الدراسة البيانات الميدانية، باستخدام البرنامج الإحصائي للعلوم الاجتماعية SPSS، واستخدام أساليب الإحصاء الوصفي والاستدلالي، والتي تضمنت:

1- مقياس الإحصاء الوصفي (Descriptive Statistic Measures) وذلك لوصف خصائص عينة الدراسة، اعتماداً على التكرارات والنسب المئوية، ومن أجل الإجابة عن أسئلة الدراسة، ومعرفة الأهمية النسبية لأبعاد الدراسة باستخدام المتوسطات الحسابية، والانحرافات المعيارية.

2- معامل الارتباط بيرسون لإجراء اختبار العلاقات الارتباطية بين متغيرات الدراسة.

واعتمدت الدراسة تصنيف إجابات فقرات محاور الدراسة وفقا لمقياس ليكرت الخماسي (Likert) وحدد بخمس إجابات حسب أوزانها رقميا، ولتفسير المتوسطات الحسابية لإستجابات أفراد عينة الدراسة على كل فقرة من فقرات محاور مقياس الدراسة؛ تم استخدام المعيار الإحصائي الآتي والمبين في الجدول (4):

الجدول (4): المعيار الإحصائي لتفسير المتوسطات الحسابية لإستجابات أفراد عينة الدراسة على كل فقرة من فقرات المحاور

المتوسط الحسابي	درجة الاستجابة
من 1.00 –2.33	منخفضة
من 2.34 –3.66	متوسطة
من 3.67 – 5.00	مرتفعة

حيث تم حساب طول الفئة من خلال قسمة $\frac{\text{قيمة أكبر} - \text{قيمة أصغر}}{\text{الفئات عدد}} = \frac{5-1}{3} = 1.33$

عرض النتائج ومناقشتها والتوصيات

يتضمن هذا الجزء عرض لنتائج الدراسة التي تهدف إلى معرفة توظيف الذكاء الاصطناعي في مجال الأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية والتنبؤ بالجرائم السيبرانية المستقبلية، وتم عرض تلك النتائج وفقاً لأسئلة الدراسة، وفيما يلي عرض لذلك:

في البداية تم حساب المتوسطات الحسابية والانحرافات المعياريةلإستجابات أفراد العينة لكل

محور من محاور الدراسة، كما تم حساب المتوسطات الحسابية والانحرافات المعيارية لكل فقرة من فقرات تلك المحاور، الجداول التالية توضح ذلك:

أولا: النتائج المتعلقة بالسؤال الاول: هل توجد علاقة ذات دلالة احصائية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية؟

جدول (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات المحور (الأول) مرتبة تنازلياً حسب المتوسطات الحسابية

الرتبة	رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة
1	2	يساعد الذكاء الاصطناعي في رفع معدلات الكشف عن هويات المجرمين	4.450	.675	مرتفعة
2	9	استخدام الاسم المستعار للمجرم يزيد من صعوبة الكشف عن الجرمية ومرتكبها	4.400	.741	مرتفعة
3	3	يسهم استخدام الذكاء الاصطناعي لدينا في القدرة على كشف جرائم الابتزاز الإلكتروني وخفض حالات الاحتيال المالي الالكتروني	4.150	.799	مرتفعة
4	7	الذكاء الاصطناعي يسهم في طرق جمع الأدلة الرقمية	4.100	.896	مرتفعة
5	4	يتسم الذكاء الاصطناعي في فعالية التصدي للهجمات الفيروسية	4.000	1.008	مرتفعة
6	1	الذكاء الاصطناعي يعمل على تعقب مرتكبي الجرائم الإلكترونية والتحقيق معهم	3.950	.675	مرتفعة
6	8	الذكاء الاصطناعي يسهم في تحسين سرعة استجابة وحدة الجرائم الإلكترونية للبلاغات والجرائم	3.950	.746	مرتفعة
8	6	استخدام الذكاء الاصطناعي يؤدي إلى التقليل من معدل وقوع ضحايا الجرائم الإلكترونية	3.850	1.325	مرتفعة
9	5	يتميز الذكاء الاصطناعي بأن له القدرة على التصدي ومواجهة الجرائم العابرة للحدود	3.700	1.013	مرتفعة
10	10	الذكاء الاصطناعي هو أداة حاسمة في مكافحة الجريمة الإلكترونية	3.600	.978	متوسطة
		المحور الأول ككل	4.015	.574	مرتفعة

يظهر من جدول(6) أن تأثير الذكاء الاصطناعي على مكافحة الجريمة الإلكترونية جاء بدرجة مرتفعة، فقد تراوحت المتوسطات الحسابية لإستجابات أفراد العينة على فقرات المحور بين(3.60-4.45) بدرجات موافقة مرتفعة ومتوسطة، حيث كان أعلاها للفقرة رقم (2) والتي تنص على " يساعد الذكاء الاصطناعي في رفع معدلات الكشف عن هويات المجرمين" ، ثم يليها المتوسط الحسابي (4.40) للفقرة رقم (9) والتي تنص على "استخدام الاسم المستعار للمجرم يزيد من صعوبة الكشف عن الجرمية ومرتكبها."، ثم يليها المتوسط الحسابي (4.15) للفقرة رقم (2) والتي تنص على "يسهم استخدام الذكاء الاصطناعي لدينا في القدرة على كشف جرائم الابتزاز الإلكتروني وخفض حالات الاحتيال المالي الالكتروني "، بينما بلغ أدناها للفقرة رقم (10) والتي تنص على " الذكاء الاصطناعي هو أداة حاسمة في مكافحة الجريمة الإلكترونية " ، وبلغ المتوسط الحسابي للمحور ككل (4.015) وبدرجة موافقة مرتفعة.

وللإجابة عن هذا السؤال تم استخراج قيمة معامل الارتباط بيرسون (Pearson Correlation) بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الالكترونيه والمركز الوطني للامن السيبراني وبين فاعلية في مكافحة الجريمة الالكترونيه ، جدول (7) يوضح ذلك:

جدول (7): نتائج استخراج قيم معامل الارتباط بيرسون بين مستوى توظيف الذكاء الاصطناعي وبين الفاعلية في مكافحة الجريمة الإلكترونية

		الفاعلية في مكافحة الجريمة الإلكترونية
مستوى توظيف الذكاء الاصطناعي	معامل الارتباط بيرسون	**.427
	الدلالة الاحصائية	.000

** ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.01$)

يظهر من خلال الجدول السابق رقم (7) أن قيمة معامل الارتباط بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني وبين فاعلية في مكافحة الجريمة الالكترونيه بلغت (0.427) وهي قيمة ذات دلالة احصائية عند مستوى الدلالة ($\alpha \leq 0.01$)، مما يدل على وجود علاقة ارتباطية طردية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الالكترونيه والمركز الوطني للامن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية.

ثانيًا: النتائج المتعلقة بالسؤال الثاني: هل يسهم توظيف الذكاء الاصطناعي اسهاما ذا دلالـه احصائية في التنبو بالجرائم السيبرانيه المستقبليه؟

جدول (9): المتوسطات الحسابية والانحرافات المعيارية لفقرات المحور (الثاني) مرتبة تنازلياً حسب المتوسطات الحسابية

الرتبة	رقم الفقرة	الفقرة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة
1	9	التنبؤ بالجرائم الإلكترونية بواسطة الذكاء الاصطناعي يسهم في تطوير استراتيجيات وقائية أفضل	4.350	.659	مرتفعة
2	8	التنبؤات بالجرائم الإلكترونية باستخدام الذكاء الاصطناعي تقلل من حجم الخسائر المحتملة	4.000	.781	مرتفعة
3	10	الذكاء الاصطناعي أداة أساسية في توقع التهديدات السيبرانية طويلة المدى	3.950	.594	مرتفعة
4	5	الجرائم السيبرانية تتطور على غرار تطور الذكاء الاصطناعي في المستقبل	3.900	1.053	مرتفعة
5	2	الذكاء الاصطناعي يسهم في الكشف المبكرعن النشاطات المشبوهة عبر الإنترنت	3.800	.514	مرتفعة
5	6	الذكاء الاصطناعي له القدرةَ في التنبؤ بأنماط جديدة من الجرائم السيبرانية	3.800	.935	مرتفعة
7	7	الذكاء الاصطناعي يساعد في تحديد المناطق الجغرافية أو الدول الأكثر تعرضاً للهجمات السيبرانية	3.750	.704	مرتفعة
8	1	الذكاء الاصطناعي له القدرة على التنبؤ بالجرائم الإلكترونية قبل وقوعها	3.700	.462	مرتفعة
9	3	الذكاء الاصطناعي يستطيع رصد التهديدات الناشئة قبل أن تتحول إلى هجمات فعلية وتحديد توقيتها	3.500	.597	متوسطة
10	4	استخدام الذكاء الاصطناعي يحقق مستوى مرتفعًا من الدقة في التنبؤ بالجرائم الإلكترونية	3.450	.675	متوسطة
		المحور الثاني ككل	3.820	.500	مرتفعة

يظهر من جدول (9) أن الذكاء الاصطناعي والتنبؤ بالجرائم الإلكترونية المستقبلية جاء بدرجة

مرتفعة، فقد تراوحت المتوسطات الحسابية لإستجابات أفراد العينة على فقرات المحور بين(3.45-4.35) بدرجات موافقة مرتفعة ومتوسطة، حيث كان أعلاها للفقرة رقم (9) والتي تنص على " التنبؤ بالجرائم الإلكترونية بواسطة الذكاء الاصطناعي يسهم في تطوير استراتيجيات وقائية أفضل" ، ثم يليها المتوسط الحسابي (4.00) للفقرة رقم (8) والتي تنص على "التنبؤات بالجرائم الإلكترونية باستخدام الذكاء الاصطناعي تقلل من حجم الخسائر المحتملة."، ثم يليها المتوسط الحسابي (3.95) للفقرة رقم (10) والتي تنص على "الذكاء الاصطناعي أداة أساسية في توقع التهديدات السيبرانية طويلة المدى "، بينما بلغ أدناها للفقرة رقم (4) والتي تنص على " استخدام تطبيقات الذكاء الاصطناعي يحقق مستوى مرتفعًا من الدقة في التنبؤ بالجرائم الإلكترونية " ، وبلغ المتوسط الحسابي للمحور ككل (3.82) وبدرجة موافقة مرتفعة.

وللإجابة عن هذا السؤال تم تطبيق اختبار تحليل الانحدار البسيط (simple linear regression) على التنبؤ بالجرائم السيبرانية المستقبلية تبعاً لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني، الجدول التالي يوضح ذلك:

جدول (10): نتائج تطبيق اختبار تحليل الانحدار البسيط على التنبؤ بالجرائم السيبرانية المستقبلية تبعاً لتوظيف الذكاء الاصطناعي

R الارتباط	التباين المفسر	قيمة ف	دلالة ف الاحصائية	قيمة β	قيمة t	دلالة الإحصائية
0.567	0.310	27.482	*0.00	0.82	5.242	*0.00

* ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$)

من خلال الجدول السابق نستنتج وجود ارتباط موجب بين توظيف الذكاء الاصطناعي في مجال الأمن السيبراني والتنبؤ بالجرائم السيبرانية المستقبلية حيث بلغ معامل الارتباط (0.567)، كما أظهرت نتائج تطبيق اختبار تحليل الانحدار البسيط على وجود أثر ذو دلالة إحصائية لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني، حيث بلغت قيمة (ف) (27.482) بدلالة إحصائية أقل من ($\alpha \leq 0.05$)، وهذا ما أكده اختبار (ت). كذلك فقد أظهرت النتائج أن التباين المفسر قد بلغ (0.310) وهذا يدل على أن نسبة تأثير توظيف الذكاء الاصطناعي في مجال الأمن السيبراني على التباين في التنبؤ بالجرائم السيبرانية المستقبلية قد بلغت (31.0%)، كما

بلغت قيمة بيتا (0.82). ومما يعني وجود أثر ايجابي لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني على التنبؤ بالجرائم السيبرانية المستقبلية.

مناقشة النتائج

يتضمن هذا الجزء من الدراسة خلاصة النتائج والاستنتاجات والحقائق التي تم التوصل لها من خلال تحليل بيانات الدراسة والإجابة عن أسئلتها وبالشكل الأتي:

أولًا: أظهرت نتائج الدراسة المتعلقة بالإجابة عن السؤال الأول أن تأثير الذكاء الاصطناعي على مكافحة الجريمة الإلكترونية جاء بدرجة مرتفعة، حيث بلغ المتوسط الحسابي الكلي للمحور (4.015)، وهو ما يعكس قناعة قوية لدى أفراد العينة بالدور المحوري الذي تؤديه تقنيات الذكاء الاصطناعي في تعزيز القدرات الوطنية لمواجهة الجرائم الإلكترونية. ويُعد هذا المؤشر دلالة واضحة على التحول من النموذج الأمني التقليدي إلى نموذج أمني ذكي قائم على التحليل الخوارزمي، والبيانات الضخمة، والتعلم الآلي، والتنبؤ بالمخاطر الرقمية.ويُلاحظ أن أعلى متوسط حسابي جاء للفقرة المتعلقة بمساهمة الذكاء الاصطناعي في رفع معدلات الكشف عن هويات المجرمين، وهو ما يعكس فاعلية تقنيات الذكاء الاصطناعي في تحليل الأنماط الرقمية، وربط البيانات متعددة المصادر، وتتبع البصمات الرقمية (Digital footprints)، وتحليل السلوك السيبراني، وهي أدوات لم تكن متاحة بالكفاءة نفسها في النظم التقليدية. وهذا يشير إلى انتقال جوهري في طبيعة التحقيقات الإلكترونية من النمط التفاعلي إلى النمط الاستباقي التنبؤي (Predictive & Preventive Policing). كما يبرز ارتفاع متوسط فقرة استخدام الأسماء المستعارة وزيادة صعوبة الكشف عن المجرم بوصفه مؤشرًا على وعي مهني متقدم بطبيعة البيئة السيبرانية، حيث تتسم الجرائم الإلكترونية بخصائص الإخفاء الرقمي، وتعدد الهويات، والتشفير، وإخفاء المصدر، وهو ما يجعل الجريمة السيبرانية أكثر تعقيدًا من الجريمة التقليدية. ويعكس هذا الإدراك أهمية الذكاء الاصطناعي كأداة تحليل متقدمة قادرة على تجاوز مظاهر الإخفاء الظاهري عبر تحليل الأنماط السلوكية الرقمية بدل الاكتفاء بالهوية الظاهرة.

أما الفقرة المتعلقة بدور الذكاء الاصطناعي في كشف جرائم الابتزاز الإلكتروني وخفض حالات الاحتيال المالي الإلكتروني، فتمثل بعدًا تطبيقيًا بالغ الأهمية؛ إذ تشير إلى أن الذكاء الاصطناعي لا يقتصر على الجانب التحليلي فقط، بل يمتد إلى المجال الوقائي والحماية

الاستباقية، من خلال تحليل الأنماط غير الطبيعية في المعاملات الرقمية،وكشف محاولات الاحتيال المبكر، والتنبؤ بسلوكيات الابتزاز الرقمي، وبناء نماذج إنذار مبكر (Early Warning Systems).وهذا يؤكد أن الذكاء الاصطناعي أصبح جزءًا من منظومة الأمن الوقائي الرقمي وليس فقط أداة لاحقة لكشف الجريمة بعد وقوعها.

وفي المقابل، فإن انخفاض متوسط الفقرة التي تنص على أن الذكاء الاصطناعي هو أداة حاسمة في مكافحة الجريمة الإلكترونية مقارنة ببقية الفقرات، رغم بقائه ضمن مستوى الموافقة، يمكن تفسيره علميًا بعدة اعتبارات: منها إدراك أفراد العينة أن الذكاء الاصطناعي ليس أداة مستقلة بذاتها، بل يعمل ضمن منظومة متكاملة تشمل العنصر البشري، والتشريعات، والبنية التنظيمية، والتعاون الدولي.والوعي بوجود حدود تقنية وأخلاقية وتشغيلية لاستخدام الذكاء الاصطناعي، مثل مشكلات الخصوصية، ودقة الخوارزميات، والانحياز الخوارزمي، وأمن البيانات.والإيمان بأن مكافحة الجريمة الإلكترونية عملية منهجية مركبة لا يمكن اختزالها في أداة تقنية واحدة مهما بلغت كفاءتها.وعليه، تعكس النتائج تصورًا ناضجًا ومتوازنًا لدى أفراد العينة، يقوم على أن الذكاء الاصطناعي يمثل عنصرًا مركزيًا في منظومة مكافحة الجريمة الإلكترونية، لكنه ليس بديلاً عن باقي مكونات النظام الأمني السيبراني، بل جزءًا تكامليًا ضمن بنية متعددة الأبعاد.

وبناءً على ذلك، يمكن القول إن نتائج هذا المحور تعكس تحولًا بنيويًا في فلسفة مكافحة الجريمة الإلكترونية، من نموذج رد الفعل (Reactive Model) إلى نموذج الاستباق الذكي (Proactive Intelligent Model)، حيث لم تعد المواجهة الأمنية قائمة على الاستجابة بعد وقوع الجريمة فقط، بل على التنبؤ والوقاية والتحليل المستمر للمخاطر الرقمية.

كما أظهرت نتائج الدراسة وجود علاقة ارتباطية طردية ذات دلالة إحصائية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني وبين فاعلية مكافحة الجريمة الإلكترونية، حيث بلغ معامل الارتباط ($r = 0.427$)، وهي قيمة دالة إحصائيًا عند مستوى الدلالة ($\alpha \leq 0.01$). ويشير هذا الارتباط الموجب متوسط القوة إلى أنه كلما ارتفع مستوى توظيف الذكاء الاصطناعي، ارتفعت فاعلية مكافحة الجريمة الإلكترونية، وهو ما يعكس علاقة تكاملية وظيفية بين البعد التقني (الذكاء الاصطناعي) والبعد الأمني (مكافحة الجريمة السيبرانية).وتُفسَّر هذه النتيجة علميًا في ضوء التحول البنيوي في أنماط العمل الأمني السيبراني، حيث لم يعد الذكاء الاصطناعي مجرد أداة دعم تقني، بل أصبح عنصرًا مؤثرًا في

إعادة تشكيل منظومة العمل الأمني نفسها، من خلال: تعزيز قدرات الكشف المبكر عن الجرائم الإلكترونية، وتحسين سرعة الاستجابة للحوادث السيبرانية،ورفع دقة التحليل الجنائي الرقمي، ودعم اتخاذ القرار الأمني المبني على البيانات (Data–driven decision making)،

كما تعكس هذه العلاقة الارتباطية وجود علاقة سببية محتملة غير مباشرة (غير حتمية إحصائيًا) بين مستوى التوظيف التقني للذكاء الاصطناعي وبين فعالية الأداء الأمني السيبراني، حيث يعمل الذكاء الاصطناعي بوصفه عامل تمكين (Enabler) ضمن منظومة متعددة المتغيرات تشمل الموارد البشرية، والإطار التشريعي، والبنية التنظيمية، والتعاون المؤسسي، والبنية التحتية الرقمية.ويكتسب معامل الارتباط المتوسط (0.427) دلالة علمية مهمة؛ إذ يشير إلى أن الذكاء الاصطناعي يمثل عاملًا مؤثرًا جوهريًا، لكنه ليس العامل الوحيد في فاعلية مكافحة الجريمة الإلكترونية، وهو ما يعكس طبيعة الظاهرة المركبة للجريمة السيبرانية التي تتأثر بعدة متغيرات متداخلة، من أبرزها كفاءة الكوادر البشرية المتخصصة،وجودة التشريعات الرقمية،ومستوى التنسيق المؤسسي، وجاهزية البنية التحتية السيبرانية.

يمكن تفسير هذه النتيجة في إطار نموذج المنظومة الأمنية الذكية المتكاملة (Integrated Smart Security System)، الذي يفترض أن فاعلية مكافحة الجريمة الإلكترونية ناتجة عن تفاعل تكاملي بين التكنولوجيا الذكية والعوامل البشرية والتنظيمية والتشريعية، وليس نتيجة عامل تقني منفرد.

كما تعكس هذه العلاقة الارتباطية الانتقال من نموذج الأمن التفاعلي (Reactive Security Model) إلى نموذج الأمن الاستباقي الذكي (Proactive Intelligent Security Model)، حيث يسهم الذكاء الاصطناعي في بناء أنظمة إنذار مبكر، ونماذج تنبؤية، وتحليل سلوكي رقمي متقدم، ما يؤدي إلى رفع مستوى الفاعلية الشاملة في مواجهة الجريمة الإلكترونية.

وبناءً على ذلك، يمكن الاستنتاج إن العلاقة الارتباطية المكتشفة لا تعكس فقط ارتباطًا إحصائيًا، بل تعكس علاقة بنيوية وظيفية بين الذكاء الاصطناعي وفاعلية مكافحة الجريمة الإلكترونية، تؤسس لرؤية استراتيجية مفادها أن الذكاء الاصطناعي لم يعد خيارًا تقنيًا، بل أصبح أحد محددات القوة الأمنية السيبرانية في الدول الحديثة.

وتتفق هذه النتيجة مع نتائج دراسة قاسم وغالب (2024) والتي اظهرت نتائجها أن الذكاء الاصطناعي أصبح حاجزًا فعّالًا ضد الجرائم الإلكترونية في الدول المتقدمة ويسهم بشكل كبير في تقليل الجرائم من خلال التنبؤ بجري الشخصيات الإجرامية ومع دراسة الرواشدة (2025) والتي

أظهرت نتائجها أن هناك دوراً للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية. ومع دراسةعبد الرازق المحسن (2021) والتي اظهرت نتائجها أن تطبيقات الذكاء الاصطناعي أصبحت أداة أساسية في مواجهة الجرائم الإلكترونية حيث أثبتت فعاليتها في تحليل الأنماط السلوكية للمجرمين السيبرانيين، واكتشاف الهجمات قبل وقوعها. ومع دراسة اشتية و الكفارنة، (2022) إلى أن الذكاء الاصطناعي يمثل أداة فاعلة في خفض معدلات الجريمة إذا ما تم توظيفه بشكل صحيح.

ويتوافق مع دراسة (Dilek et al., 2015) والتي أظهرت من قدرة الأنظمة المستندة إلى الخوارزميات الحيوية على التعلم المستمر والتكيف مع أنماط الهجوم المتغيرة، مما يجعلها أداة فعّالة في المواجهة الاستباقية.

ثانيًا: أظهرت نتائج الدراسة أن دور الذكاء الاصطناعي في التنبؤ بالجرائم الإلكترونية المستقبلية جاء بدرجة مرتفعة، حيث بلغ المتوسط الحسابي الكلي للمحور (3.82)، وتراوحت المتوسطات الحسابية لفقراته بين (3.45–4.35) بدرجات موافقة مرتفعة ومتوسطة، وهو ما يعكس قناعة واضحة لدى أفراد العينة بأهمية الذكاء الاصطناعي كأداة استراتيجية في بناء منظومات إنذار مبكر للأمن السيبراني، والانتقال من منطق الاستجابة بعد وقوع الجريمة إلى منطق التنبؤ والاستباق الوقائي.وقد جاءت أعلى المتوسطات الحسابية للفقرة التي تنص على أن التنبؤ بالجرائم الإلكترونية بواسطة الذكاء الاصطناعي يسهم في تطوير استراتيجيات وقائية أفضل، وهو ما يدل على إدراك مؤسسي متقدم لأهمية الذكاء الاصطناعي في دعم التخطيط الأمني الاستراتيجي، حيث لا يقتصر دوره على التحليل الآني للتهديدات، بل يمتد إلى بناء نماذج تنبؤية طويلة المدى قادرة على استشراف أنماط الجريمة المستقبلية، وتوجيه السياسات الأمنية، وتطوير البرامج الوقائية المبنية على البيانات.كما يعكس ارتفاع متوسط الفقرة المتعلقة بتقليل حجم الخسائر المحتملة من خلال التنبؤات الذكية وعيًا بأهمية البعد الاقتصادي للأمن السيبراني، حيث يسهم الذكاء الاصطناعي في تقليص كلفة الهجمات السيبرانية من خلال الكشف المبكر، والاستجابة السريعة، ومنع تفاقم الأضرار، وهو ما يحوّل الأمن السيبراني من تكلفة تشغيلية إلى استثمار وقائي استراتيجي في استدامة الأنظمة الرقمية.

ويؤكد ارتفاع متوسط فقرة اعتبار الذكاء الاصطناعي أداة أساسية في توقع التهديدات السيبرانية طويلة المدى أن الذكاء الاصطناعي أصبح جزءًا من البنية التخطيطية للأمن السيبراني، وليس مجرد أداة تشغيلية، حيث يسهم في بناء سيناريوهات مستقبلية، وتحليل الاتجاهات الرقمية،

واستشراف المخاطر الناشئة، وهو ما يعكس انتقال المؤسسات الأمنية إلى نموذج الأمن الاستشرافي الذكي (Smart Foresight Security).في المقابل، فإن انخفاض متوسط الفقرة المتعلقة بتحقيق مستوى مرتفع من الدقة في التنبؤ بالجرائم الإلكترونية باستخدام الذكاء الاصطناعي، رغم بقائه ضمن مستوى الموافقة، يعكس وعيًا واقعيًا بحدود النماذج التنبؤية، والتحديات المرتبطة بجودة البيانات، والتحيز الخوارزمي، وتعقيد السلوك الإجرامي الرقمي، وعدم قابلية الظواهر الاجتماعية–التقنية للتنبؤ الدقيق الكامل، وهو ما يدل على تصور متوازن لدى أفراد العينة لا يبالغ في قدرات الذكاء الاصطناعي التنبؤية، بل يدرك حدودها المنهجية والعلمية.

وتُفسَّر هذه النتائج في إطار التحول من نموذج الأمن التفاعلي إلى نموذج الأمن الاستباقي القائم على البيانات (Data-driven Proactive Security)، حيث يمثل الذكاء الاصطناعي أداة مركزية في بناء أنظمة الإنذار المبكر، والتحليل التنبؤي، والتخطيط الوقائي، دون أن يلغي دور العنصر البشري أو الأطر التنظيمية والتشريعية، بل يعمل في تكامل معها.

وتشير نتائج الدراسة إلى وجود ارتباط موجب دال إحصائيًا بين مستوى توظيف الذكاء الاصطناعي في مجال الأمن السيبراني والقدرة على التنبؤ بالجرائم السيبرانية المستقبلية، حيث بلغ معامل الارتباط (0.567)، وهي قيمة تعكس علاقة ارتباطية متوسطة إلى قوية، بما يدل على أن ازدياد مستوى توظيف الذكاء الاصطناعي يقترن بارتفاع القدرة المؤسسية على التنبؤ بالتهديدات والجرائم السيبرانية المستقبلية. وتعكس هذه النتيجة إدراكًا واضحًا للطبيعة الاستراتيجية للذكاء الاصطناعي بوصفه أداة مركزية في بناء أنظمة الاستشراف الأمني والإنذار المبكر في الفضاء السيبراني.وقد أكدت نتائج تحليل الانحدار البسيط هذه العلاقة من خلال إظهار وجود أثر ذي دلالة إحصائية لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني على التنبؤ بالجرائم السيبرانية المستقبلية، حيث بلغت قيمة (27.482) (F) بدلالة إحصائية أقل من مستوى الدلالة ($\alpha \leq 0.05$)، وهو ما يشير إلى أن هذا الأثر ليس عشوائيًا بل يعكس علاقة حقيقية ذات دلالة علمية، كما عزز ذلك اختبار (t) الذي أكد دلالة هذا التأثير إحصائيًا. وتُظهر هذه النتائج أن الذكاء الاصطناعي يؤدي دورًا فاعلًا في الانتقال من نموذج الأمن التفاعلي إلى نموذج الأمن الاستباقي القائم على التحليل التنبؤي والبيانات الضخمة.كما أوضحت النتائج أن نسبة التباين المفسر (R^2) بلغت (0.310)، بما يعني أن توظيف الذكاء الاصطناعي في مجال الأمن السيبراني يفسر ما نسبته (31.0%) من التباين في القدرة على التنبؤ بالجرائم السيبرانية

المستقبلية، وهي نسبة تفسيرية مرتفعة نسبيًا في الدراسات ذات الطبيعة المركبة، وتدل على أن الذكاء الاصطناعي يمثل عاملًا مؤثرًا رئيسًا في بناء القدرات التنبؤية، مع الإقرار بوجود عوامل أخرى مساندة مثل كفاءة الموارد البشرية، وجودة البيانات، والبنية التشريعية، والتكامل المؤسسي، والتعاون الدولي.وتؤكد قيمة معامل بيتا ($\beta = 0.82$) القوة التفسيرية العالية لهذا الأثر، حيث تشير إلى وجود تأثير إيجابي مباشر قوي لتوظيف الذكاء الاصطناعي في مجال الأمن السيبراني على التنبؤ بالجرائم السيبرانية المستقبلية، وهو ما يعكس الدور الجوهري للذكاء الاصطناعي في بناء النماذج التنبؤية، وتحليل الاتجاهات الرقمية، واستشراف أنماط السلوك الإجرامي السيبراني، وبناء أنظمة إنذار مبكر قائمة على التعلم الآلي والتحليل الخوارزمي المتقدم.وتُفسَّر هذه النتائج في إطار التحول نحو نموذج الأمن السيبراني الاستشرافي الذكي (Smart Predictive Cybersecurity Model)، الذي يقوم على توظيف الذكاء الاصطناعي في تحليل البيانات الضخمة، وربط الأنماط السلوكية، وبناء سيناريوهات مستقبلية، وتوقع المخاطر قبل تحققها، بما يسهم في تعزيز القدرة الوقائية للمؤسسات الأمنية، وتقليل الخسائر المحتملة، ورفع كفاءة التخطيط الاستراتيجي طويل المدى.وبناءً على ذلك، يمكن الاستنتاج إن نتائج هذا التحليل لا تعكس مجرد علاقة إحصائية، بل تكشف عن علاقة بنيوية استراتيجية بين الذكاء الاصطناعي والقدرات التنبؤية في الأمن السيبراني، حيث أصبح الذكاء الاصطناعي عنصرًا مؤسسًا في بناء منظومات التوقع والاستشراف، وليس مجرد أداة تقنية مساندة. وهو ما يفرض ضرورة تبني استراتيجيات وطنية تقوم على الاستثمار المستدام في الذكاء الاصطناعي التنبؤي، وبناء القدرات البشرية المتخصصة، وتطوير التشريعات الرقمية، وتعزيز التكامل المؤسسي، بما يضمن بناء منظومة أمن سيبراني استباقية قادرة على مواجهة التهديدات المستقبلية قبل تحققها.

وتتفق هذه النتيجة مع دراسةعبد الرازق المحسن (2021) والتي اظهرت نتائجها أن تطبيقات الذكاء الاصطناعي أصبحت أداة أساسية في مواجهة الجرائم الإلكترونية حيث أثبتت فعاليتها في تحليل الأنماط السلوكية للمجرمين السيبرانيين، واكتشاف الهجمات قبل وقوعها. ومع دراسة اشتية والكفارنة، (2022) إلى أن الذكاء الاصطناعي يمثل أداة فاعلة في خفض معدلات الجريمة إذا ما تم توظيفه بشكل صحيح، حيث يُسهم فيرصد وتحليل الأنماط السلوكية الإجرامية والكشف المبكر عن التهديدات وتعزيز قدرة الأجهزة الأمنية على الاستجابة السريعة

وتتفق مع دراسة Zhang et al. (2022) والتي أظهرت دور الذكاء الاصطناعي التفسيري

XAI فـي تعزيـز الشـفافية والثقـة لـدى الجهـات الأمنيـة، وتسـهيل فهـم أنمـاط الهجمـات السـيبرانية المعقدة والاستجابة لها بشكل أسرع وأكثر دقة، كما تتفق هذه النتائج مع ما أشارت إليه دراسة Djenna et al. (2023)، حيث أظهر النموذج العملي المطبق أن تقنيات التعلم العميق والشبكات العصبية الالتفافية قادرة على كشف الهجمات الإلكترونية بدقة عالية، مما يعزز قدرة الأجهزة الأمنية على استباق التهديدات.

خلاصة الدراسة

اظهرت نتائج الدراسة الحالية ان تأثير الذكاء الاصطناعي على مكافحة الجريمة الإلكترونية جـاء بدرجـة مرتفعـة ، حيـث كـان أعلاهـا للفقـرة رقـم (2) والتـي تـنص علـى " يسـاعد الـذكاء الاصطناعي في رفع معدلات الكشف عن هويات المجرمين" ، "، بينما بلغ أدناها للفقرة رقم (10) والتي تنص على " الذكاء الاصطناعي هو أداة حاسمة في مكافحة الجريمة الإلكترونية " ، وبلغ المتوسط الحسابي للمحور ككل (4.015) وبدرجة موافقة مرتفعة ووجود علاقة ارتباطية طردية بين مستوى توظيف الذكاء الاصطناعي في وحدة الجرائم الالكترونيه والمركز الوطني للامن السيبراني وبين فاعلية في مكافحة الجريمة الإلكترونية .كما بينت النتائج أن دور الذكاء الاصطناعي في التنبؤ بالجرائم الإلكترونية المستقبلية جاء بدرجة مرتفعة.

التوصيات

من النتائج التي توصلت اليها الدراسة، تم صياغة مجموعة من التوصيات كالاتي:

- تبني استراتيجية وطنية مؤسسية شاملة لتعزيز توظيف الذكاء الاصطناعي في العمل الأمني السيبراني، تقوم على التحديث المستمر للبنية التحتية الرقمية. وتعزى هذه التوصية الى الفقرة التي اشارت أن هنالك انخفاض في الكشف عن جرائم الاحتال المالي والابتزاز الإلكترونية كون اكتشاف مثل هذا الجرائم يمثل صعوبة لدى العاملين في وحدة الجرائم الإلكترونية والعاملين في المركز الوطني السيبراني كون هذه الفقرة تمثل بعدًا تطبيقيًا بالغ الأهمية؛ لكونها تشير إلى أن الذكاء الاصطناعي لا يقتصر على الجانب التحليلي فقط، بل يمتد إلى المجال الوقائي والحماية الاستباقية.
- توسيع نطاق استخدام تقنيات الذكاء الاصطناعي في منظومات الكشف المبكر والتحليل الجنائي

الرقمي والوقاية السيبرانية، وتكاملها مع قواعد البيانات الوطنية والدولية، بما يعزز فاعلية الاستجابة الأمنية، ويرفع كفاءة الكشف، ويحد من معدلات الجرائم الإلكترونية على المستويين الوقائي والعلاجي. تشير هذه التوصية الى فقرة ان الذكاء الاصطناعي يستطيع رصد التهديدات الناشئة قبل أن تتحول إلى هجمات فعلية وتحديد توقيتها حيث أن هنالك متوسط حسابي متوسط بحيث يصعب على العاملين في وحدة الجرائم الإلكترونية والعاملين في المركز الوطني الأمن السيبراني تحديد توقيتها.

- تطوير أنظمة دفاع سيبراني ذكية مضادة (AI vs AI Systems)، تقوم على الذكاء الاصطناعي الدفاعي، وتحليل السلوك الإجرامي الرقمي، وبناء نماذج استجابة تكيفية، لمواجهة التطور المستمر في أساليب الجريمة الإلكترونية المدعومة بالذكاء الاصطناعي.
- إنشاء منظومات وطنية للإنذار المبكر السيبراني تعتمد على الذكاء الاصطناعي التنبؤي، وتحليل البيانات الضخمة، وبناء نماذج استشرافية، لدعم التخطيط الأمني الاستراتيجي طويل المدى، وتعزيز الانتقال من الأمن التفاعلي إلى الأمن الاستباقي. وتعزى هذه التوصية في انخفاض متوسط الفقرة المتعلقة بتحقيق مستوى مرتفع من الدقة في التنبؤ بالجرائم الإلكترونية باستخدام الذكاء الاصطناعي، يتمثل بوجود تحدي بجودة البيانات، والتحيز الخوارزمي، وتعقيد السلوك الإجرامي الرقمي، وعدم قابلية الظواهر الاجتماعية–التقنية للتنبؤ الدقيق الكامل، وهو ما يدل على تصور متوازن لدى أفراد العينة لا يبالغ في قدرات الذكاء الاصطناعي التنبؤية، بل يدرك حدودها المنهجية والعلمية.

المراجع:

أولا: المراجع العربية

- استراتيجية المركز الوطني للأمن السيبراني الأردني، 2025 منشورة عبر الإنترنت.
- اشتية، محمد والكفارنة، شادي. (2022). الذكاء الاصطناعي ودوره في الحد من الجرائم: دراسة تحليلية تطبيقية، مجلة جامعة العين للأعمال والقانون، 2(8)، 28 – 59.
- جندل، جاسم محمد (2022)، الجرائم الإلكترونية، دار المعتز للنشر والتوزيع، عمان – الأردن.
- الحجرف، حسن نايف. (2021). دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، 5(32)، 14071-14091.

- الخزامي، محمد. (2023). دور الذكاء الاصطناعي في العلوم الاجتماعية والإنسانية. المجلة العربية للعلوم الاجتماعية والإنسانية، جامعة الجلالة
- الرواشدة، صباح عادل عارف، (2020)، دور أنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية دراسة ميدانية، المجلة الأردنية في ادارة الأعمال، الاردن.
- عبد الرازق، رانا مصبح. (2021). تأثير الذكاء الاصطناعي على الجريمة الإلكترونية، المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية، 22(1)، 430–437.
- علاوي، عمار راشد، ن عبد المجيد، محمد نور الدين، (2021)، استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها، مجلة الشارقة للعلوم القانونية، الأمارات
- الفريحات، عماد حسين محمد .(2023) .الجهود العربية والإفريقية لمواجهة الجرائم الإلكترونية في الفترة 2010–2023 .مجلة ابن خلدون للدراسات والأبحاث، 3.(5).190–219.
- قاسم، مراد محمد غالب محمد. (2023). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة مقارنة. مجلة جامعة تعز للدراسات الاجتماعية والإنسانية.

ثانيًا: المراجع الأجنبيّة

- Brundage, Miles, et al (2015). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.
- Csongor, H., & Tóth, D. (2024). Artificial Intelligence in Cybersecurity: Examining Liability, Crime Dynamics, and Preventive Strategies. EU and comparative law issues and challenges series (ECLIC), 8, 730-747.
- Dilek, Selma, Hüseyin Çakır, and Mustafa Aydın. (2015)"Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review.".
- Djenna, A., Barka, E., Benchikh, A., & Khadir, K. (2023). Unmasking cybercrime with artificial-intelligence-driven cybersecurity analytics. Sensors, 23(14), 6302.
- El-Kady, R. (2025). Unveiling the Illegal Uses of Cryptocurrencies in Dark Web and Advanced AI and Machine Learning Techniques in Cryptocurrency Forensics. In Concept, Theories, and Management of Cryptocurrencies (pp. 363-394). IGI Global Scientific Publishing.
- Pum, M. (2022). The rise of AI-powered cybercrime: Implications for digital

security and policy. University of Chicago. Retrieved from: https://www.researchgate.net/publication/390748096_The_Rise_of_AI-Powered_Cybercrime_Implications_for_Digital_Security_and_Policy

- Takemura, N. (2021). AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after' Singularity' and Prospects of Informational Civilization. International Journal for Crime, Justice and Social Democracy, 10(3), 1-16.
- Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEe Access, 10, 93104-93139.