E-ISSN: 2706-9931
P-ISSN: 1994-473X

Al-Adab Journal Vol. 68, No. 3, (September) 2026

Applications of Artificial Intelligence and Their Role in Combating Cyber Crimes: A Theoretical Review of UAE Security Institutions

Fatima Mohammed Bin Sandal (Corresponded Author) [1]
Wafa Barhoumi Hamdi [2]
[1] MA student – Department of Sociology – University of Sharjah, College of Art's, Humanities & Social Science U23101277@sharjah.ac.ae https://orcid.org/0009-0003-9220-8940
[2] Assistant Professor – Department of sociology – University of Sharjah, College of Art's, Humanities & social Science whamdi@sharjah.ac.ae

DOI: https://doi.org/10.31973/4mxyhp08

Publication Dates

(Received 2025-06-11) (Revised 2025-06-22) (Accepted 2025-07-07) (Published 2026-09-15)

Abstract:

The research aims to identify the fundamental conceptual theories and principles that explain the interaction of artificial intelligence with the field of combating cybercrime, analyze and describe the operating mechanisms of AI applications in detecting and preventing cyber-attacks as mentioned in the scientific literature, analyze the theoretical and practical transformation in cybersecurity defense strategies by integrating AI into UAE security institutions, and identify the technical challenges of implementing AI in cybersecurity. To achieve the study's objectives, methodological analytical literature review was employed, and the researcher found that there are theories that explain the role of AI in interpreting crime, but these theories are limited. Additionally, the AI applications used in the UAE are effective in detecting and preventing cybercrimes, such as the use of predictive policing and cloud computing. Furthermore, AI applications have transformed the approach from reactive to proactive, utilizing tools such as machine learning for pattern analysis, continuous network monitoring, and dynamic adaptation to new threats.

***The authors has signed the consent form and ethical approval**

Keywords: Artificial intelligence, cybercrimes, challenges, security institutions.

Al-Adab Journal Vol. 68, No. 3, (September 2026)
E-ISSN: 2706-9931 P-ISSN: 1994-473X

تطبيقات الذكاء الاصطناعي ودورها في مكافحة الجرائم السيبرانية: مراجعة نظرية في المؤسسات الامنية الاماراتية

فاطمة محمد بن صندل (المؤلف المراسل)
جامعة الشارقة، كلية الآداب والعلوم الإنسانية والاجتماعية، قسم علم الاجتماع، دولة الإمارات العربية المتحدة

أ.م.د. وفاء برهومي حمدي
جامعة الشارقة، كلية الآداب والعلوم الإنسانية والاجتماعية، قسم علم الاجتماع، دولة الإمارات العربية المتحدة

تواريخ المنشور

الإستلام	النسخة النهائية	الموافقة	النشر الالكتروني
(٢٠٢٥/٦/١١)	(٢٠٢٥/٦/٢٢)	(٢٠٢٥/٧/٧)	(٢٠٢٦/٩/١٥)

(مُلَخَّصُ البَحث)

يهدف البحث إلى تحديد النظريات والمبادئ المفاهيمية الأساسية التي تُفسر تفاعل الذكاء الاصطناعي مع مجال مكافحة الجرائم السيبرانية، وتحليل ووصف آليات عمل تطبيقات الذكاء الاصطناعي في كشف الهجمات السيبرانية ومنعها كما وردت في الأدبيات العلمية، وتحليل التحول النظري والعملي في استراتيجيات الدفاع السيبراني بدمج الذكاء الاصطناعي في المؤسسات الأمنية الإماراتية، والتعرف على التحديات التقنية لتطبيق الذكاء الاصطناعي في الأمن السيبراني.

ولتحقيق أهداف الدراسة اتبعت المنهج الاستعراضي النظري التحليلي، وتوصلت الباحثة إلى أن هناك نظريات تفسر دور الذكاء الاصطناعي في تفسير الجريمة ولكن هذه النظريات محدودة، كما أن تطبيقات الذكاء الاصطناعي المستعملة في دولة الإمارات تعمل على كشف الجرائم الإلكترونية ومنعها كاستعمال الشرطة التنبؤية والحوسبة السحابية، كما أن تطبيقات الذكاء الاصطناعي قد أحدثت تحولا عبر التحول من النمط التفاعلي إلى الاستباقي، وأدوات مثل: التعلم الآلي لتحليل الأنماط، والمراقبة المستمرة للشبكات، والتكيف الديناميكي مع التهديدات الجديدة.

الكلمات المفتاحية: الذكاء الاصطناعي ،الجرائم السيبرانية ،التحديات ،المؤسسات الأمنية.

*** وقع المؤلفون على نموذج الموافقة والموافقة الأخلاقية الخاصة بالمساهمة البشرية في البحث**

مقدمة:

مع التطورات المتسارعة في مجال التقنيات الرقمية ونظم المعلومات في عصر الثورة الصناعية الرابعة، والانفتاح الواسع على ثقافات الدول، ظهرت أنماط جديدة من التحديات الأمنية كان أهمها: الجريمة الإلكترونية. فقد أصبح الفضاء الرقمي بيئة خصبة لارتكاب أنواع متعددة من الجرائم التي لا تعترف بالحدود الجغرافية، ولا تقتصر على نطاق دولة معينة، بل قد تتشعب آثارها وتتسع رقعتها لتشمل دولًا عد.

تُعد الجرائم الإلكترونية من القضايا المعقدة التي يصعب اكتشافها والحد منها؛ لقدرة مرتكبيها على إخفاء الأدلة وتتبع آثارهم. وقد أصبحت هذه الجرائم واقعًا ملموسًا في دولة الإمارات العربية المتحدة، التي شهدت في السنوات الأخيرة زيادة ملحوظة في معدلاتها، تزامنًا مع تسارع التحول الرقمي في مختلف القطاعات.

وفي ظل هذه التحديات، ظهرت أهمية التوظيف الذكي للتقنيات الحديثة وفي مقدمتها الذكاء الاصطناعي، الذي أصبح جزءًا لا يتجزأ من أنظمة الحياة اليومية، بدءًا من الهواتف الذكية وأجهزة الحاسوب، وصولًا إلى الأنظمة الأمنية والمراقبة. وقد أثبت الذكاء الاصطناعي قدرته على تحليل البيانات الضخمة، والتعلم من الأنماط السابقة، واتخاذ قرارات سريعة تساعد في التنبؤ بالجرائم والتصدي لها بفاعلية.

ونظرًا لما توليه دولة الإمارات من اهتمام بالغ في تعزيز أمنها السيبراني، فقد تبنت استراتيجيات متقدمة تقوم على تطوير البنية التحتية الرقمية، ودعم البحث العلمي، واستثمار قدرات الذكاء الاصطناعي في المجالات الأمنية. كما أنشأت مؤسسات متخصصة تُعنى بمواكبة التطورات المستقبلية، مما يعكس وعي الدولة بأهمية الاستعداد لمواجهة الجرائم الإلكترونية بأدوات المستقبل.

من هذا المنطلق، تسعى هذه الدراسة إلى تسليط الضوء على دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية في دولة الإمارات العربية المتحدة، عبر استعراض أهم التقنيات المستعملة، وتحليل مدى فاعليتها، وبيان التحديات والفرص المستقبلية في هذا المجال الحيوي.

مصطلحات الدراسة

- الذكاء الاصطناعي: هو علم وهندسة صنع آلات ذكية (الظاهري، ٢٠١٧: ٣)، ويعرفه (دهشان، ٢٠٢٠: ١١٠) بأنه

محاولة جعل الكمبيوتر أو الآلة التي تعمل بالبرمجة مثل الإنسان سواء في تفكيره أو تصرفاته أو حله لمشكلاته، وممارسته لنواحي الحياة اليومية كافة، وذلك عن طريق دراسات تُجرى على الإنسان، وتستخلص منها نتائج تساعد في تفسير سلوك الإنسان وبرمجة ذلك لتطبيقه على الآلة.

وتعرفه الباحثة إجرائيا بأنه: محاولة جعل جهاز الحاسوب كالإنسان في تفكيره، وتصرفاته، وممارسته لنواحي الحياة كافة.

- الجريمة الإلكترونية: هو كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية (الحجار، ٢٠٢١: ١٣٦)

وتعرفها الباحثة إجرائيا بأنها: كل الأفعال المخالفة لقوانين دولة الإمارات العربية وأنظمتها والتي ترتكب بواسطة جهاز الحاسوب وشبكات الإنترنت.

عناصر الدراسة

مشكلة الدراسة

على الرغم من التطور التكنولوجي المتسارع لتطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني عالميا، تظهر فجوة معرفية واضحة في الأدبيات الأكاديمية حول:

- الأسس النظرية التي تفسر آليات عمل هذه التطبيقات في سياق المؤسسات الأمنية الإماراتية.
- الفجوات والمحددات المفاهيمية التي تحول من دون بناء نموذج نظري موحد لاستشراف نقاط القوة والضعف قبل التطبيق الميداني.

ويتفرع من السؤال الرئيس الأسئلة الفرعية الآتية:

أسئلة الدراسة

١. ما النظريات والمبادئ المفاهيمية الأساسية التي تفسر دور الذكاء الاصطناعي في مكافحة الجرائم السيبرانية؟
٢. كيف تصف الأدبيات العلمية آليات عمل تطبيقات الذكاء الاصطناعي في كشف ومنع الهجمات السيبرانية؟
٣. كيف يُحدث الذكاء الاصطناعي تحولًا في استراتيجيات الدفاع السيبراني التقليدية، وما الأدوات الرئيسة التي يعتمدها في هذا التحول؟
٤. ما أهم التحديات التقنية التي تواجه تطبيق الذكاء الاصطناعي في مجال الأمن السيبراني بحسب الأدبيات العلمية؟

أهمية الدراسة

- تحديد الثغرات النظرية في أدبيات الذكاء الاصطناعي والأمن السيبراني، مما يوجه الباحثين نحو موضوعات جديدة تحتاج استقصاءً.
- كشف التحديات التي تواجه المؤسسات الأمنية المحلية.
- المساهمة في حماية البنى التحتية الحيادية والبيانات الحساسة في دولة ذات توجه تقني متسارع مثل: الإمارات.

أهداف الدراسة

- تحديد النظريات والمبادئ المفاهيمية الأساسية التي تُفسر تفاعل الذكاء الاصطناعي مع مجال مكافحة الجرائم السيبرانية.
- تحليل آليات عمل تطبيقات الذكاء الاصطناعي ووصفها في كشف الهجمات السيبرانية ومنعها كما وردت في الأدبيات العلمية.
- تحليل التحول النظري والعملي في استراتيجيات الدفاع السيبراني بدمج الذكاء الاصطناعي في المؤسسات الأمنية الإماراتية.
- التعرف على التحديات التقنية لتطبيق الذكاء الاصطناعي في الأمن السيبراني

منهج الدراسة:

في هذه الدراسة، تم اعتماد المنهج التحليلي النظري كما تم جمع تحليل الدراسات السابقة من عام ٢٠١٨ وحتى عام ٢٠٢٤

الإطار النظري

تعريف الجرائم الإلكترونية:

عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة المنعقد في فينا سنة ٢٠٠٠م الجريمة الإلكترونية بأنها جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية (الحجار، ٢٠٢١:١٣٦).

ولم يتطرق المشرع الإماراتي إلى تعريف محدد للجريمة المستحدثة أو الجريمة الإلكترونية، وإنما قام بتعريف بعض أشكال الجرائم الإلكترونية.

ويعرف المشرع الإماراتي المحتوى غير القانوني بأنه: المحتوى الذي يكون إحدى الجرائم المعاقب عليها قانوناً أو يكون من شأن نشره أو تداوله أو إعادة تداوله داخل الدولة الإضرار بأمن الدولة أو سيادتها أو أياً من مصالحها أو الصحة العامة أو ضمان السلم العام أو بالعلاقات الودية للدولة مع الدول الأخرى أو التأثير في نتائج انتخابات أعضاء

المجلس الوطني الاتحادي أو المجالس الاستشارية بإمارات الدولة أو التحريض على مشاعر العداء أو الكراهية بين مجموعة مختلفة من الأشخاص أو انخفاض ثقة العامة في أداء أي واجب أو مهمة أو في ممارسة أي صلاحية من إحدى سلطات الدولة أو أي من مؤسساتها (قانون الجرائم الإماراتي ٢٠٢١: ٣٦٤)

ويعرف المشرع الإماراتي البيانات الزائفة بأنها: الشائعات والبيانات الكاذبة أو المضللة سواء كلياً أو جزئياً وسواء بحد ذاتها أو في إطار السياق الذي ظهرت فيه (قانون الجرائم الإماراتي ٢٠٢١: ٣٦٤)

ويعرف المشرع الإماراتي الاختراق بأنه الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها (قانون الجرائم الإلكترونية الإماراتي ٢٠٢١: ٣٦٤).

ويعرف المشرع الإماراتي الاعتراض بأنه: مشاهدة أو مراقبة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو التحايل أو تغيير المحتوى أو إساءة الاستعمال أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ومن دون وجه حق (قانون الجرائم الإلكترونية الإماراتي ٢٠٢١: ٣٦٤).

ويعرف المشرع الإماراتي الهجمات الإلكترونية بأنها: كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات أو وظائف أي منها، سواء أكان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها (قانون الجرائم الإلكترونية الإماراتي ٢٠٢١: ٣٦٤).

ويعرف المشرع الإماراتي مواد إباحية للأطفال بأنها: إنتاج أو عرض أو نشر أو حيازة أو تداول صورة أو فيلم أو رسم عن طريق وسيلة من وسائل الاتصال أو شبكات التواصل الاجتماعية أو غيرها أو أية وسيلة أخرى يظهر فيها الطفل في وضع مشين في عمل جنسي أو عرض جنسي واقعي وحقيقي أو خيالي أو بالمحاكاة (قانون الجرائم الإلكترونية الإماراتي ٢٠٢١: ٣٦٥).

ويعرف المشرع الإماراتي الإعلان المضلل بأنه: الإعلان عن سلعة أو خدمة بناءً على معلومات خادعة أو إغفال معلومات جوهرية أو أساسية ذات ارتباط بالسلعة أو الخدمة بما قد يؤثر على قرار المستهلك ويدفعه إلى التعاقد بحيث أنه ما كان ليتعاقد لولا تلك المعلومات (قانون الجرائم الإلكترونية ٢٠٢١: ٣٦٥).

أنواع الجرائم الإلكترونية:

يذكر (كزيز وقط، ٢٠١٨: ١٢٩_١٣٦) أهم مظاهر الهجمات والجرائم الإلكترونية التي تهدد أمن الدولة واستقرارها على النحو الآتي:

- التجسس الإلكتروني، أثر الفضاء الإلكتروني على الأدوات الاستخباراتية ،وسهل القدرة على جمع المعلومات والتصنت والتجسس.
- الحرب الإلكترونية، هي جملة من الممارسات والإجراءات التي تسعى لإلحاق الخلل والعطل بالأنظمة والوسائل الإلكترونية الخاصة بالعدو.

السرقة والاحتيال عبر الإنترنت، وتتم عن طريق:

- سرقة المعلومات وتزويرها..
- سرقة الأموال وابتزازها.
- التخريب والإتلاف.
- الغش التجاري
- التحويل الإلكتروني غير الشرعي للمال
- الجرائم المنظمة عبر الإنترنت، ومن صورها غسيل الأموال عبر الإنترنت، وتجارة المخدرات عبر الإنترنت.
- الإرهاب الإلكتروني.

أولا: آليات عمل تطبيقات الذكاء الاصطناعي في كشف الهجمات السيبرانية ومنعها كما وردت في الأدبيات العلمية.

<u>تطبيقات الذكاء الاصطناعي في دولة الإمارات العربية في مجال الأمن والعمل الشرطي:</u>

١. خطت دولة الإمارات خطوات سريعة لتقنين استعمال تطبيقات الذكاء الاصطناعي، ولأجل ذلك أصدرت الهيئة العامة للطيران المدني بالإمارات قرارًا، وبدأ تنفيذه من أول فبراير ٢٠١٦ يقضي بإلزام تسجيل كل الطائرات من دون طيار كأحد أهم تطبيقات الذكاء الاصطناعي وأكثرها شيوعًا، وهو نفس ما نصت عليه المادة (١٥) من قانون تنظيم الطائرات من دون طيار في إمارة دبي رقم (٤) لسنة ٢٠٢٠م، وينطبق ذلك على طائرات التحكم عن بعد، والتي يستعملها الأفراد لأغراض ترفيهية، بغض النظر عن وزن الطائرة، ويخضع المخالف لتلك التعليمات لما جاء من عقوبات في المادتين

٧٠،٦٩ من القانون الاتحادي للطيران المدني رقم ٢٠ لسنة ١٩٩١،ويتم التسجيل إلكترونيًا من دون رسوم بعد استيفاء الأوراق المطلوبة، وكذلك صدر قانون تنظيم الرياضات الجوية الخفيفة رقم ٧ لسنة ٢٠٢١م في رأس الخيمة، ونص على قواعد استعمال الطائرات المسيرة في إمارة رأس الخيمة (علاي وعبد المجيد، ٣٧٣:٢٠٢٣).

٢. وسعت شرطة دبي إلى ابتكار نظام التنبؤ الأمني الذكي للجرائم،والذي بدأ في العام ٢٠١٦، ضمن خطة شرطة دبي للحد من الجريمة عبر العمل على توفير معلومات عن الأماكن المتوقع أن ترتكب فيها الجرائم ،وتحليل تلك البيانات وسرعة التحرك لمنعها (علاي وعبد المجيد، ٣٩٦:٢٠٢٣)

٣. وكشفت شرطة دبي عن مركبات ذاتية القيادة من المتوقع أن تجوب شوارع دبي بنهاية عام ٢٠١٧، والدورية ذاتية القيادة يمكن برمجتها للتجوال في منطقة معينة ومزودة بالكاميرات ،ورادار استشعار، ولديها خاصية المحادثة الصوتية مع غرفة العمليات، ويمكنها التعرف إلى الأشخاص العاملين في أي منطقة والزوار، وكشف الأجسام المشبوهة. (عبد الحكيم، ٩٦٨،٢٠٢١).

٤. ولقد اعتمدت عدد من تطبيقات الذكاء الاصطناعي في العمل الشرطي، إذ استعملت عددا من أساليب الذكاء الاصطناعي في كل العمليات الشرطية ومنها: نظام توقع الجرائم ،والتنبؤ ،والبحث، والتحري، والتحقيقات الجنائية (علاي وعبد المجيد، ٣٧٢:٢٠٢٣).

٥. وتستعمل شرطة أبو ظبي بصمة العين للتعرف على هوية الأشخاص، ويعتمد هذا النظام تقنية حيوية دقيقة تعمل عن طريق التقاط صورة لقزحية العين، ومن ثم تخزينها ،وإنشاء رموز مشفرة، وهو نظام سريع وفاعل في أثناء البحث عن المطلوبين، ولا يستغرق سوى ثوانٍ معدودة (عبد الحكيم: ٩٦٧:٢٠٢١).

٦. واعتمدت الدولة تقنيات الذكاء الاصطناعي لمراقبة الحدود وحمايتها، كما يوجد في مطار دبي الدولي نحو ٨٠ كاميرا للتعرف إلى الوجه لتأكيد هوية المسافرين في غضون ١٠ ثوان مما يساعد على اكتشاف أي تهديد أمني بسرعة، وقد تم اعتماد النظام من أجل أتمتة "التشغيل الإلكتروني" مكاتب الهجرة

في دولة الإمارات العربية المتحدة بالكامل بحلول عام ٢٠٢٠ عبر استعمال تقنيات الذكاء الاصطناعي ،والتعرف إلى الوجه لتأكيد هوية الأشخاص المسموح لهم بدخول البلاد (علاي وعبد المجيد، ٢٠٢٣:٣٨٨).

تقنيات الذكاء الاصطناعي لمكافحة الجريمة في دولة الإمارات

استطاعت منظومة الشرطة الذكية في دولة الإمارات وعبر حكومات الدولة بوظائفها سواء التفاعلية أو التنبؤية أن تكون قادرة على مكافحة الجريمة ،والحد من ارتكابها، وذلك عن طريق منظومتها الذكية القائمة على الذكاء الاصطناعي، وكاميرات الدوائر التلفزيونية المغلقة، والتقنيات اللاسلكية الخلوية ومنخفضة الطاقة واسعة النطاق، وأجهزة الاستشعار الذكية، والطائرات من دون طيار، وغيرها من الأجهزة والتقنيات الحديثة المتطورة (بوابة الإمارات)، وسوف نتناول بعضا منها بالقدر الذي يتناسب مع جوهر البحث والهدف منه.

أولًا حكومة أبو ظبي :

١. نظام عين الصقر للمراقبة والتحكم في مدينة أبو ظبي.
٢. أجهزة القياس الحيوية مثل" نظام بصمة العين"IRIS.
٣. خدمة أمان الذكية

ثانيًا: حكومة دبي:

١. الدوريات ذاتية القيادة.
٢. الدراجة الذكية هوفر سيرف.
٣. خدمة الأمين.
٤. منصة: Crime e للإبلاغ عن الجرائم السيبرانية .
٥. الشرطي الآلي الذكي.
٦. الروبوت الآلي للإنقاذ البحري .

ثالثًا حكومة الشارقة:

١. خدمة نجيد لاستقبال البلاغات سرًا.
٢. خدمة أمني من أمن جاري.

جهود وزارة الداخلية بدولة الإمارات في مكافحة الجرائم الإلكترونية

ووزارة الداخلية بدولة الإمارات لها دور فاعل في مكافحة الجرائم الإلكترونية، وذلك عبر خطوات جريئة لضمان حماية الأفراد والمؤسسات من محاولات استغلال المجرمين للشبكة الإلكترونية في ارتكاب الجرائم الإلكترونية وهي (النقبي والمصعبي، ٢٠٢٣: ٥٤٦٤-)

١. إنشاء قاعدة معلومات متطورة تهتم بحصر عناصر "مجرمي المعلوماتية" التي تستعمل الشبكة الإلكترونية في الداخل والخارج، ومعرفة الجماعات والجهات والخلايا التي تدعمهم ،وأهدافهم ،ومخططاتهم.

٢. تسهيل إجراءات تبادل المعلومات بصورة عاجلة على وفق طرائق وأساليب سرية محكمة بين الأجهزة الأمنية المعنية داخل الدولة.

٣. إقامة تعاون فاعل بين الأجهزة المعنية وبين المواطنين، وإيجاد ضمانات وحوافز مناسبة لتشجيعهم على الإبلاغ عن أية جريمة إلكترونية.

٤. تشديد إجراءات المراقبة الداخلية لمعرفة الأشخاص الذين لهم توجيهات وميول نحو الجرائم الإلكترونية في الخارج، واتخاذ التدابير الأمنية اللازمة كافة؛ لتجميد نشاطهم ومنعهم من تفعيل هذه الأنشطة في الداخل والخارج.

٥. تكثيف اللقاءات والاجتماعات الدورية بين الأجهزة الأمنية، وتبادل وجهات النظر والمعلومات المستجدة، وإعادة تقويم المواقف من وقت لآخر لمنع حدوث جرائم إلكترونية.

٦. عدم توفير الملاذ لمن يمولون الأعمال الإرهابية الإلكترونية ومن يديرونها ويدعمونها وكذلك مرتكبيها ومن يوفرون الحماية لهم.

٧. رصد أسماء المتورطين في أعمال إرهابية إلكترونية في القاعة السوداء ،وتعميمها على المطارات والموانئ والمنافذ الحدودية.

٨. الدورات التدريبية التي تنظمها وزارة الداخلية بصفة دورية للعاملين لديها لمكافحة الجرائم الإلكترونية لتزويدهم بالوسائل الفنية والتقنية المساعدة لكشف هذه الجرائم.

٩. دعم البحوث الأمنية ومراكز البحوث والدراسات ،وتشجيعها، وحثها على دراسة الجرائم الإلكترونية، وتحليلها للتعرف على أسبابها وأساليبها ووسائلها والآثار الناجمة عنها وكيفية مواجهتها، وكذلك استخلاص أوجه القصور في الاستعداد أو المواجهة لتلافيها، وتحقيق تطوير مستمر في هذا المجال.

١٠. تبادل المعلومات الجنائية مع شُعب الاتصال بالدول العربية والمكتب العربي للشرطة الجنائية والتنسيق والتعاون معها في هذا المجال

١١. تبادل المعلومات الجنائية والمعلومات عن الجرائم الإلكترونية مع المكاتب المركزية للشرطة الدولية الإنتربول في الدول الأعضاء في المنظمة الدولية وأماناتها العامة، والتنسيق والتعاون معها في هذا المجال.

١٢. تجاوب وزارة الداخلية لطلبات الدول التي تتقدم للحصول على معلومات في شأن الجرائم

الإلكترونية عن طريق شعبة الاتصال بالإنتربول .

تصدي دولة الإمارات العربية المتحدة للجرائم الإلكترونية:

لقد تصدت دولة الإمارات العربية المتحدة للجرائم الإلكترونية على النحو الآتي: (الجبري وآخرون ، ٢٠٢٢: ٢٤٠-٢٤١)

١. من الناحية العلمية والتدريبية، فقد عرف عن الدولة نهجها الدؤوب في تفردها في تطبيق أفضل ممارسات علمية وعملية على أجهزة التحقيق الجنائي عن طريق التدريبات، والمناهج العالمية لصقل مهارات المحققين حتى يتمكنوا من اكتشاف تلك الجرائم وتحديدها ومعالجتها ، فضلا عن عقد مؤتمرات علمية دولية تخص مجال التحقيق الجنائي الرقمي لكسب الخبرات العالمية.

٢. من الناحية التشريعية، فقد عالج المشرع الإماراتي الفجوات في القوانين السابقة بسن تشريعات جديدة تواكب الأفعال الإجرامية المستحدثة، والتي تشكل تحديا لجهات التحقيق الجنائي مما سهل على المحققين في أثناء القيام بمهامهم المنوطة في عمليات الاستدلال والتحقيق.

ثانيا: النظريات والمبادئ المفاهيمية الأساسية التي تفسر دور الذكاء الاصطناعي في مكافحة الجرائم السيبرانية

المحور الأول: نظريات الجريمة

١.نظرية الاختيار العقلاني choice Theory Rational ونظرية النشاط الروتيني Routine Activity Theory

تعد نظرية الاختيار العقلاني choice Theory Rational لكلارك وكورنيش" نهجا يستعمله علماء الاجتماع لفهم السلوك البشري، وكيف يتخذ أفراد المجتمع قرارًا بارتكاب أو عدم ارتكاب جريمة، بناء على تحليل بسيط للتكلفة والعائد. ويشير هنا مصطلح 'العقلانية' إلى تصرف الفرد كما لو كان يوازن بين التكاليف والفوائد، للتوصل إلى إجراء يزيد من المنفعة الشخصية مثل: "المال أو الجنس أو الإثارة'. كما تقر النظرية بأن تصورات الجناة للتكاليف والفوائد، تحكمها عوامل عدة مثل: الوقت، والقدرات المعرفية للجاني، وتوافر المعلومات ذات الصلة عن مكان الجريمة، وأدواتها، والضحية، ومن ثم يزن الجناة نوع المنفعة المحتملة ومقدارها، مقابل المخاطر المتصورة للاكتشاف والعقاب. فيما يتعلق بالجرائم الرقمية على سبيل المثال، يمكن للآليات الإلكترونية مثل معرف المستخدم (كلمات السر). وأنظمة التحكم في الوصول الآلي، وكاميرات المراقبة، أن

تكون بمثابة الرادع؛ لأنها تزيد من نسبة اكتشاف المجرم الرقمي؛ لذلك، لمنع الجريمة، يجب التركيز بشكل أكبر على العقوبة كرادع.

٢.نظرية الارتباط التفاضلي Theory of different association ونظرية التعلم الاجتماعي social learning Theory

تنطلق نظرية الارتباط التفاضلي' لساذرلاند "من أن السلوك الإجرامي وتقنيات ارتكاب الجريمة هما سلوك طبيعي يتم تعلمه عن طريق التفاعل مع الآخرين؛ واكتساب مجموعة الدوافع العقلانية والمواقف سواء أكانت مؤيدة أم معارضة لارتكاب الجريمة، فترتكب الجريمة عندما تتجاوز تلك التعريفات المؤيدة لارتكاب الجريمة تلك التعريفات المعارضة لارتكابها. ومن ثم فهناك نوعان من العناصر الأساسية للرابطة التفاضلية، الأول هو العنصر المعرفي؛ أو محتوى ما يتم تعلمه؛ مثل: تقنيات ارتكاب الجرائم، والدوافع العقلانية، والمواقف المناسبة المؤيدة لانتهاك القانون؛ ولم يحدد 'ساذرلاند" آليات التعلم؛ وأكد أن عملية تعلم السلوك الإجرامي مثلها مثل أي تعلم آخر. العنصر الثاني من الارتباط التفاضلي هو الارتباط مع أشخاص آخرين في مجموعات شخصية، حيث يتم التعلم وفّسر سبب قيام الأشخاص المختلفين الذين يتعرضون لنفس الظروف الاجتماعية بسلوك إجرامي وآخرون لا، بأن المعاني التي يعطونها لهذه الظروف التي يواجهونها هي التي تحدد ما إذا كانوا ينتهكون القانون أم لا، وتختلف هذه المعاني باختلاف "التكرار والمدة والأولوية والشدة".

٣. نظرية الانتقال في الفضاء Space Transition Theory

ظهرت الحاجة إلى نظرية جديدة منفصلة للجرائم الرقمية، لشرح أسباب الجرائم في الفضاء الإلكتروني؛ لأن التفسيرات النظرية العامة كانت غير كافية للتفسير، ومن هنا ظهرت "نظرية الانتقال الفضائي" في كتاب بعنوان "جرائم الإنترنت" للعالم قرانك شماليجر' ومايكل بيتارو"؛ وهي تركز على شرح طبيعة سلوك الأشخاص الذين يظهرون في الفضاء المادي والإلكتروني، ويقصد بالانتقال الفضائي هناء عملية حركة الأشخاص من الفضاء المادي 'الواقع"؛ إلى الفضاء السيبراني "الإنترنت" والعكس، وتصرفهم بشكل مختلف. وللنظرية مجموعة فروض تتمثل في أولا: يميل الأشخاص أصحاب السلوك الإجرامي المكبوت (في الفضاء المادي) إلى ارتكاب

الجريمة في الفضاء السيبراني؛ لصعوبة ارتكابها في الفضاء المادي؛ بسبب وضعهم الاجتماعي أو الوظيفي.

٤. نظرية الضغط البنيوي Structural straintheory ونظرية الضغوط والجرائم الالكترونية Strain theory and Cypercrimes

تركز هذه النظرية على البنية الاجتماعية، والتحليل على مستوى الوحدات الكبرى macro ، فتنص نظرية الضغوط ل "ميرتون" والتي تعرف أيضًا باسم نظرية الفرص المحظورة Blocked opportunity theory على عدم المساواة بين الأهداف المحددة ثقافيا (المقاسة بالقيمة النقدية) والوسائل المشروعة (المقاسة عبر العمل والتعليم) لتحقيق هذه الأهداف. لكن ليس كل شخص تتاح له الوسائل المشروعة لتحقيق أهدافه؛ لذلك يتم خلق إجهاد أو ضغط على أفراد الطبقة الدنيا، الذين من المرجح أن يلجأوا إلى الوسائل غير المشروعة (الجريمة) لتحقيق الهدف. قام 'ميرتون 'بتحديد خمسة أنماط للتكيف مع الضغوط هي: التوافق، والطقوس، والابتكار، والتراجع، والتمرد، فالشخص المتوافق يقبل الأهداف الثقافية ،ويقبل الوسائل المؤسسية للحصول عليها؛ لذا فمن غير المرجح أن يرتكب أعمال إجرامية. ويرفض رجل الطقوس الأهداف الثقافية، لكنه يقبل الوسائل المؤسسية، كما أنه من غير المحتمل أن يرتكب الجرائم، ويقبل المبتكرون الأهداف؛ لكن ليس بالطريقة العادية لتحقيقها؛ وقد يلجأ المبتكرون إلى الجريمة لتحقيق أهدافهم. كما يرفض المتراجعون كلاً من الأهداف والوسائل: كما أنهم لا يطمحون ليكونوا ناجحين؛ ولا يهتمون بأهداف المجتمع التقليدية؛ لذلك قد يصبح المتراجعون مجرمين. وأخيرا، يرفض المتمردون الأهداف والوسائل الثقافية ،ويستبدلونها بأهداف ووسائل جديدة، غالبًا ما تكون هذه الأهداف الجديدة إجرامية.

٥. نظرية التسمية theory labelling

تنطلق نظرية التسمية ووضع العلامات للعالم "بيكر" من مكونين مهمين: الأول: يبحث في السلوكيات التي يتم تسميتها على أنها إجرامية، وإن الجماعات هي التي تتخذ هذه القرارات وتطلق تلك المسميات وفقًا "لبيكر' تعد الجريمة من صنع المجتمع؛ لأن الجماعات الاجتماعية تضع القواعد وتطبقها ،وتسمي أولئك الذين يخالفون القواعد بأنهم منحرفون؛ لذلك فإن أولئك الذين تبين أنهم خالفوا القانون يشاركون 'تسمية وخبرة

وصفهم بأنهم غرباء'؛ ومن ثم يجب أن تركز تفسيرات الجريمة على العملية التي يتم عن طريقها تصنيف الأفراد وتسميتهم كونهم مجرمين. المكون الثاني لنظرية بيكر مستمد من 'المدخل التفاعلي الرمزي"، والذي يفحص معاني الجريمة للفرد والمجتمع ،إذ ذكر بيكر أن المجرمين؛ وباعتماد خطورة الجريمة، يمكن عدهم "غرباء" عند الآخرين؛ لأنهم انتهكوا قاعدة اجتماعية؛ تؤدي هذه التسمية إلى أن تبني الأفراد هويات إجرامية ،ويعيدون ارتكاب الجريمة لاحقًا.

ثالثاً: التحول النظري والعملي في استراتيجيات الدفاع السيبراني بدمج الذكاء الاصطناعي

تعريف الذكاء الاصطناعي:

الذكاء الاصطناعي حقل علمي متخصص من فروع علوم الحاسوب، تم ابتكاره عام ١٩٥٦م، ويهدف إلى برمجة الحواسيب، إذ يمكنها امتلاك القدرة على التفكير ،والتوصل إلى حل المشكلات، واتخاذ القرارات بطريقة تحاكي قدرات الإنسان (الملا، ٢٠١٨:١١٦) والذكاء الاصطناعي هو علم وهندسة صنع آلات ذكية (الظاهري، ٢٠١٧:٣)

ويعرفه (دهشان، ٢٠٢٠:١١٠) بأنه محاولة جعل الكمبيوتر أو الآلة التي تعمل بالبرمجة التي تعمل بالبرمجة مثل: الإنسان سواء في تفكيره أو تصرفاته أو حله لمشكلاته، وممارسته لنواحي الحياة اليومية كافة، وذلك عن طريق دراسات تُجرى على الإنسان ، وتستخلص منها نتائج تساعد في تفسير سلوك الإنسان ، وبرمجة ذلك لتطبيقه على الآلة.

خصائص تقنيات الذكاء الاصطناعي:

هناك خصائص عدة تنفرد بها أنظمة الذكاء الاصطناعي، ومن أهمها: (علاي وعبد المجيد:٢٠٢٣: ٣٨٠-٣٨٢)

١- قدرة الذكاء الاصطناعي على التنبؤ والتكيف، يستعمل الذكاء الاصطناعي الخوارزميات والبيانات التي تمت برمجتها فيه والتي يقوم باستعمالها في اتخاذ القرارات والتنبؤات المستقبلية.

٢- الذكاء الاصطناعي قادر على الحركة والإدراك، يتمتع الذكاء الاصطناعي بقدرات إدراكية ذكية متقدمة كالإدراك البصري والسمعي، وإدراك الكلام، ومعالجة المعلومات والتعلم.

٣- الذكاء الاصطناعي يتمتع بالاستقلالية الكاملة لاتخاذ القرار من دون تدخل بشري، يمتلك الذكاء الاصطناعي القدرة على التعرف على حادثة ما ،واتخاذ قرارات

مستقلة عبر التعلم الآلي غير الخاضع للإشراف ومن دون تدخل العنصر البشري.

موقف المشرع الإماراتي من الذكاء الاصطناعي:

تسعى دولة الإمارات العربية المتحدة إلى عملية دمج تقنيات الذكاء الاصطناعي في العمل الجنائي عبر التنبؤ بالجرائم بطريقة ذكية، وتعمل على إدخال الذكاء الاصطناعي في مجال عمل الأدلة الجنائية وعمليات الشرطة إلى جانب استعماله في تعزيز الأمن والسلامة في الطرقات، وإدارة الكوارث والأزمات (الشاعر، ١٩:٢٠٢٠)

ولقد مر تطبيق الذكاء الاصطناعي في دولة الإمارات بمراحل عدة ، ففي عام ٢٠٠٠ بدأت دولة الإمارات الخطوة الأولى للتحول الإلكتروني، فأطلقت في العام ٢٠١٣ مبادرة الحكومة الذكية لتوفير الخدمات للجمهور، وأنشئت أول مدينة ذكية متكاملة سيليكون بارك في العام ٢٠١٤، وفي العام التالي أكملت الدولة التحول الذكي للخدمات الحكومية بنسبة ١٠٠٪، وفي العام٢٠١٧ أطلقت الإمارات استراتيجية الذكاء الاصطناعي لأول مشروع ضخم ضمن مئوية الامارات٢٠٧١م (شيلي، ٢٠٢٢:١٠).

وتسعى دولة الإمارات إلى الاعتماد الكلي لتقنيات الذكاء الاصطناعي بحلول عام ٢٠٣١، وتتبنى الدولة أحدث التقنيات في الأداء المعلوماتي لإيجاد البيئة المتميزة عالميًا (عبد الرزاق، ١٨:٢٠٢٣)

وتعد دولة الإمارات العربية المتحدة من الدول القليلة التي نجحت في توظيف تقنيات الذكاء الاصطناعي في المجالات الحياتية المرتبطة بحياة الناس، من أجل الارتقاء بمستوى الخدمات، كما وتم استحداث منصبين وزاريين مهمين يعززان هذا التوجه، هما: وزير دولة للذكاء الاصطناعي، ووزير دولة للتعامل مع ملف العلوم المتقدمة (النيابة العامة بدبي، ٣٠:٢٠١٨)

وحققت دولة الإمارات العربية المتحدة السبق الخليجي عبؤر مبادرة دبي الذكية، وسن قانون البيانات المحلي عام ٢٠١٥م، كما أنها كانت الدولة الأولى في تعيين وزير للذكاء الاصطناعي عام ٢٠١٧م، ولقد استعملت إمارة أبو ظبي تطبيقات الذكاء الاصطناعي في المجال الأمني عبر اعتماد الشرطة التنبؤية البيانات الكبيرة والخوارزميات القائمة

على الذكاء الاصطناعي (العلماء، ٢٠١٩:٥٩).

وظائف الذكاء الاصطناعي في تحقيق الأمن السيبراني

يستعمل الذكاء الاصطناعي في تحسين الأمن السيبراني عن طريق ما يأتي: (الحداوي، وآخرون، ٢٠٢٣)

١. التعامل مع بيانات ضخمة / يتم تنفيذ عدد من الأنشطة على الخوادم، وتظهر التحديات التي تواجه محللو الأمن السيبراني في التحقق من كل شيء وتقويم المخاطر.

٢. توقع التهديدات المستقبلية، فالذكاء الاصطناعي يستطيع معالجة حجم كبير من البيانات في حد واحد، مما يمكن الكشف المبكر عن الأنشطة الضارة بفضل تحديد الإجراءات الوقائية ،والتهديدات المحتملة.

٣. تقليل وقت اكتشاف التهديد، ويمكن للذكاء الاصطناعي فحص كميات هائلة من البيانات في وقت واحد؛ للكشف عن التهديدات السيبرانية.

٤. التقليل في التكاليف، ووفقا للدراسات، فهناك فروقات كبيرة في توفير التكاليف بنسبة ٨٠٪ للمؤسسات التي تعتمد تقنيات الذكاء الاصطناعي في أمنها السيبراني.

ويؤدي الذكاء الاصطناعي أدورًا حاسمة في مجال التحقيق الجنائي ومن أهمها:

١. تصنيف المجرمين، فعن طريق الشرطة الرقمية يتم تصنيف المجرمين ،وتسهيل القبض عليهم بموضوعية، مما يؤدي إلى تخفيض نسبة الخطأ في عملية تصنيفهم (الشاعر، ٢٠٢٣:٢٤)

٢. التنبؤ بالجرائم، تساعد التقنيات على التنبؤ بوقوع الجريمة من البشر، فضلا عن توقع الجريمة الأكثر حدوثًا، وتوقع نسبة الإجرام، والأماكن التي يمكن أن تكون مراكزًا إجرامية مستقبلا، وذلك عبر خوارزميات برمجية يتم تزويدها ببيانات، إذ تعطي نتائج تساعد في الوقاية من حدوث جرائم متوقعة (الشاعر، ٢٠٢٣:٢٤).

٣. إعادة بناء مسرح الجريمة، فقدرة التنبؤ الكبيرة لدى تقنيات الذكاء الاصطناعي تساعد في بناء مسرح الجريمة عبر نموذج شبكة القرار للتنبؤ (الشاعر، ٢٠٢٣:٢٤).

استراتيجية الذكاء الاصطناعي بدولة الإمارات العربية المتحدة

في أكتوبر ٢٠١٧، أطلقت حكومة دولة الإمارات استراتيجية الإمارات للذكاء الاصطناعي (AI). وتمثل هذه المبادرة المرحلة الجديدة بعد الحكومة

الذكية، والتي تعتمدها الخدمات، والقطاعات، والبنية التحتية المستقبلية في الدولة بما ينسجم ورؤية الإمارات ٢٠٧١، الساعية إلى أن تكون دولة الإمارات الأفضل بالعالم في المجالات كافة. وباتت من نقاط القوة التي تمتلكها، وهي:

- الأصول الخاصة بالقطاع، والقطاعات الناشئة.
- الحكومة الذكية.

وستركز على الفرص التي يمكنها تحقيق الريادة فيها:

- مشاركة البيانات والحكومة.
- جيل جديد من المواهب الإقليمية.

أهداف استراتيجية الذكاء الاصطناعي:

تهدف استراتيجية الذكاء الاصطناعي في الإمارات العربية المتحدة ٢٠٣١ إلى:

١. تحقيق أهداف مئوية الإمارات ٢٠٧١، وتعجيل تنفيذ البرامج والمشروعات التنموية لبلوغ المستقبل.
٢. اعتماد الذكاء الاصطناعي في الخدمات ،وتحليل البيانات بمعدل ١٠٠% بحلول عام ٢٠٣١.
٣. الارتقاء بالأداء الحكومي ،وتسريع الإنجاز، وإيجاد بيئات عمل مبتكرة.
٤. تحقيق حكومة الإمارات الأولى في العالم، في استثمار الذكاء الاصطناعي بمختلف قطاعاتها الحيوية.
٥. إيجاد فرص جديدة وتعزيز تنافسية الدولة في القطاعات ذات القيمة الاقتصادية العالية.
٦. دعم القطاع الخاص وزيادة الإنتاجية، فضلا عن بناء قاعدة قوية في مجال البحث والتطوير.
٧. تبني الذكاء الاصطناعي وأدواته تطبيقياً في ميادين العمل بكفاءة عالية كافة.
٨. استغلال كل الطاقات على النحو الأمثل، واستغلال الموارد والإمكانات البشرية والمادية المتوافرة بطريقة خلاقة.

رابعاً: التحديات التقنية التي تواجه تطبيق الذكاء الاصطناعي في مجال الأمن السيبراني بحسب الأدبيات العلمية

تتميز الجرائم الإلكترونية بخصائص تميزها عن الجرائم التقليدية، ومن هذه الخصائص (شرعان، ٢٠٢٠ :٣٤):

١. عابرة للحدود وذلك لعالمية شبكة الإنترنت ،إذ يمكن ارتكابها من مسافات بعيدة، كما أن الجاني يستطيع ارتكاب فعله في دولة ،ويحقق نتائج جرمه في دولة أخرى مما يزيد من صعوبة اكتشافها وإثباتها.

٢. يصعب إثباتها ؛لعدم ترك أي آثار مادية بعد ارتكابها.

٣. سهلة الارتكاب فلا تحتاج لمجهود عضلي ولا تحتاج إلى سلوكيات مادية متعددة لتحقيق النتيجة فيها، فإن توافرت التقنية اللازمة ،والوسيلة المناسبة للمجرم المعلوماتي يستطيع ارتكابها بسهولة من دون عناء.

٤. يتمتع مركب الجريمة الإلكترونية بالثقافة والعلم التكنولوجي، إذ يتميز بذكاء فائق الأمر يمكنه من التخطيط الجيد للجريمة وإحاطتها بأساليب وتدابير أمنية وحماية فنية تحول من دون كشف أمره

ويضيف (أوتاني، ٢٠٢٣: ٤٣٤) خصائص أخرى للجرائم الإلكترونية وهي:

١. الاستناد إلى بعد الانفجار التكنولوجي الحديث، فكثرة التسهيلات التي ترتبت على تطور الاتصالات بعيدة المدى في مختلف مجالات الحياة فسح المجال على مصراعيه لارتكاب مختلف الجرائم باستعمال أساليب التقانة الحديثة.

٢. التحرر من الخصوصية المكانية والزمانية للبنى الاجتماعية التي نشأت فيه، في حين تتميز الجريمة التقليدية بوحدة الزمان ومحدودية المكان وطابعها المحلي، وذلك على خلاف المستحدثة فأصبحت تكتشف في غير المكان الذي نشأت وارتبطت به، وبالنتيجة فإن ذلك يؤدي إلى ما يسمى بتدويل الجريمة) Crime of Internationalization).

٣. ارتفاع درجة التنسيق والتنظيم على الصعيد الدولي لمكافحة الجرائم الإلكترونية ولاسيما لجرائم المنظمة العابرة للحدود، والتي أصبحت عبارة عن جماعات متعددة الجنسيات، الأمر الذي جعل مسؤولية ضبطها وملاحقتها خارج صلاحية السلطة القانونية للدولة الواحدة.

٤. اختفاء التوافق في الزمان والمكان بين الجاني والضحية في الجرائم الإلكترونية كما في جريمة الاحتيال والإرهاب الإلكتروني، ويترتب على ذلك هروب الجناة وبحوزتهم متحصلات الجريمة وصعوبة القبض عليهم من الشرطة، على عكس التعاصر في الزمان والمكان في الإجرام التقليدي كما في جرائم السرقة، والقتل، والخطف، وغيرها.

٥. غياب النصوص القانونية وآليات الضبط القانوني الرسمي الخاص بمكافحة الجرائم الإلكترونية على المستوى المحلي والدولي.

٦. جسامة الأضرار المترتبة على الجرائم الإلكترونية في الجوانب الاقتصادية، والاجتماعية، والثقافية.

٧. تفوق كلفة الجرائم الإلكترونية على المستوى المادي ومستوى الصعيد الأمني والهوية الثقافية مما يؤدي إلى انهيار البيئة الاجتماعية، وسيادة الفوضى والاضطرابات.

خامسا: الدراسات السابقة:

هدفت دراسات عدة إلى استكشاف دور تقنيات الذكاء الاصطناعي في الحد من الجرائم الإلكترونية، مثل: دراسة (قامن ٢٠٢٤) التي ركزت على استعمال الشبكات العصبية والخوارزميات لتحليل البيانات ،وكشف الهويات، في حين ناقشت دراسة (الأخنيش والعيداني، ٢٠٢٣) أهمية التعاون الدولي لمواجهة هذه الجرائم، كما قدمت دراسة (سالم وأبو الجدايل، ٢٠٢٣) تقويما لفاعلية الهيئة الوطنية للأمن السيبراني في السعودية في توظيف الذكاء الاصطناعي، وحذرت دراسة (كحيط وقدة، ٢٠٢٢) من ضرورة وضع إطار قانوني أخلاقي لتنظيم استعمال هذه التقنيات.

وركزت دراسة (علاي وعبد المجيد، ٢٠٢٣) ودراسة (Umair، ٢٠٢٢) على تطوير نماذج تنبؤية تعتمد الذكاء الاصطناعي، مثل: التحليلات التنبؤية، والتعلم العميق، لرصد أنماط الجريمة مسبقًا، أما دراسة (Al-Marghilani، ٢٠٢٢) فصممت خوارزميات للكشف عن المشتبه بهم باستعمال تقنيات التعرف على الوجه، مما يعزز قدرة الأجهزة الأمنية على التدخل الوقائي.

وناقشت دراسة (Walker & Asad، ٢٠٢٢) ودراسة (الراعي، ٢٠٢٣) الإشكاليات المتعلقة بمسؤولية الذكاء الاصطناعي في ارتكاب الأخطاء مثل: صعوبة تحديد الجهة المسؤولة قانونيًا (البشر أم الآلة)، وأشارت دراسة (غنيم، ٢٠٢٢) إلى تأثير استعمال تقنيات التعرف على الوجه على حقوق الإنسان، مؤكدةً ضرورة موازنة الكفاءة الأمنية مع الحفاظ على الخصوصية.

وسلطت كل من دراسة (اللنجاوي، ٢٠٢٣) و(بشير، ٢٠٢٣) الضوء على تجربة الإمارات في استعمال الذكاء الاصطناعي في العمل الشرطي، مثل: معالجة البيانات الضخمة، والتعرف على الوجوه. وفي المقابل، حذرت دراسة (الشهري، ٢٠٢٤) من تحديات مثل: اختراق برمجة الذكاء الاصطناعي، في حين اقترحت دراسة (عضيبات وأبو عيادة، ٢٠٢٣) تفعيل البنية الرقمية للمؤسسات الأمنية.

وقدمت دراسة (Thomas، ٢٠٢٣) حلولًا لتحسين قابلية تفسير نماذج الذكاء الاصطناعي (XAI)، في حين صممت دراسة (Rouhollahi، ٢٠٢١) أنموذجًا للكشف عن غسيل الأموال باستعمال التعلم الآلي، كما وناقشت دراسة (الشاعر، ٢٠٢٣) دور الذكاء الاصطناعي في تحسين التحقيقات الجنائية الرقمية.

ودعت كل من دراسة (الجبري وآخرون، ٢٠٢٢) و(محمد، ٢٠٢٢) إلى تعزيز التعاون بين الدول لملاحقة مجرمي الإنترنت، في حين ركزت دراسة (القحطاني، ٢٠٢٢) على تدريب الملاكات الجامعية على استراتيجيات الأمن السيبراني، وأكدت دراسة (الداغر، ٢٠٢١) دور الإعلام الأمني في نشر الوعي بتطبيقات الذكاء الاصطناعي.

وحللت دراسة (السنيدي، ٢٠١٨) السياسة العقابية الإماراتية في مواجهة الجرائم المعلوماتية، واقترحت تطبيق المراقبة الإلكترونية كونه تدبيرا احترازيا، أما دراسة (القحطاني، ٢٠٢٢) فناقشت دمج استراتيجيات الأمن السيبراني في الخطط الجامعية لمواجهة الإرهاب الإلكتروني.

سادساً: التعقيب على الدراسات السابقة

ركزت دراسة (قاسم، ٢٠٢٤)على تقنيات تحليل البيانات للكشف عن المجرمين، وربطت دراسة الهري، ٢٠٢٤)التطبيقات الأمنية بالمستقبل الإنساني، وركزت دراسة (النجاوي ٢٠٢٣)، ودراسة (بشير، ٢٠٢٣) على فوائد التعرف على الوجوه ومعالجة البيانات في السياق الإماراتي، في حين دعت دراسة (الأخنيش ٢٠٢٣) و(عيداني، ٢٠٢٣) لإنشاء شرطة رقمية ،وتعزيز التعاون الدولي، واستعملت دراسة (علاي، وعبد المجيد ٢٠٢٣) تقنيات متقدمة كالتحليل التؤي، وقارنت دراسة (توماس ٢٠٢٣) بين الممارسات الصناعية والأبحاث الأكاديمية، وناقشت دراسة (Walker،٢٠٢٢) قضايا المساءلة عند تفاعل البشر مع الآلات، واستعملت دراسة (Umai،٢٠٢٢) بيانات نيويورك التاريخية تحسين دقة التنبؤ.

وتنوعت الدراسات من حيث المنهج ،وأداة الدراسة، فاتبعت دراسة (قاسم ٢٠٢٤) المنهج الوصفي التحليلي والمنهج المقارن، وتمثلت الأداة بالتحليل الوثائقي، أما دراسة (سالم وأو الجدايل) فاتبعت المنهج المسحي، وتمثلت أداة الدراسة بالاستبانة،

واتبعت دراسة (الراعي) المنهج الوصفي التحليلي ،وتمثلت أداة الدراسة بتحليل التشريعات والأدبيات، أما دراسة (توماس) فاتبعت المنهج النوعي والمراجعة الأدبية ،وتمثلت الأداة بالمقابلة.

وبشكل عام ركزت أغلب الدراسات على الجريمة الإلكترونية ،وتناولت موضوع الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، كما أن أغلب الدراسات ولاسيما العربية اتبعت المنهج الوصفي التحليلي.

أوجه التشابه بين الدراسة الحالية والدراسات السابقة:

- الموضوع الرئيس، تركز الدراسة الحالية والدراسات السابقة في دور الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية.
- التحديات المشتركة، وتشمل ظهور تحديات تقنية وبشرية في معظم الدراسات، فالحاجة لتدريب الملاكات الأمنية ظهرت بالدراسة الحالية ،وكذلك دراسة (اللنجاوي ٢٠٢٣)، والتحديات المتعلقة بتحليل البيانات والهجمات الإلكترونية ظهرت في دراسة (علاي وعبد المجيد، ٢٠٢٣).

أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة:

- السياق التشريعي، أظهرت الدراسة الحالية التشريعات الإماراتية كقوة تميزها، أما دراسة (السنيدي، ٢٠١٨) فناقشت القصور التشريعي.

النتائج :

١. الإمارات تُظهر أداءً متميزًا في مكافحة الجرائم الإلكترونية عبر توظيف تقنيات ذكاء اصطناعي متطورة (كالبصمة الرقمية وتتبع العملات المشفرة)، مدعومةً باستثمارات ضخمة وتشريعات مرنة. وهي تُقارن بمنزلة الدول الرائدة عالميًا (مثل: الولايات المتحدة، والصين)، مع إمكانية تفوقها في جوانب مثل: السرعة التشريعية ومركزية القرار، ومع ذلك، لا تزال هناك حاجة لمعالجة تحديات مثل: زيادة الشفافية، وتعزيز التعاون الدولي.

٢. تظهر النتائج ثقة عالية في جهود الإمارات تطوير وتطبيق تقنيات الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية، مع حاجة طفيفة لتعزيز التفوق التقني مقارنة بالدول الأخرى.

٣. تتمحور التحديات الرئيسة في الجوانب التقنية (الهجمات، وتحليل البيانات)، في حين الجوانب

التنظيمية (التشريعات، والتمويل) أقل إلحاحًا في السياق الإماراتي، وهناك حاجة ماسة لتطوير أنظمة ذكاء اصطناعي مقاومة للاختراق، ووجود تقنيات متقدمة (مثل: التعلم العميق) لمعالجة البيانات المعقدة، وهناك ثقة من المشاركين في الإطار التشريعي والبنية التحتية للإمارات.

٤. تبني تقنيات الذكاء الاصطناعي في الرصد والكشف عن التهديدات يُمثل نجاحًا واضحًا لسياسات الإمارات.

٥. تُظهر النتائج تأييدًا عامًّا لاستراتيجيات استعمال الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، لكن هناك حاجة لتحسين الجوانب التدريبية والتمويلية، ويتوجب على الإمارات الاستفادة من شراكاتها العالمية، وتعزيز البنية التحتية ؛لتصبح نموذجًا رائدًا في الأمن السيبراني المدعوم بالذكاء الاصطناعي.

التوصيات:

١. تعزيز الشفافية حول آلية عمل التقنيات لزيادة ثقة الأقلية التي عبرت عن تحفظات (إجابات منخفضة).

٢. تطوير حملات توعوية تُوضح تفوق التقنيات الإماراتية مقارنةً بالدول الأخرى.

٣. تعزيز التعاون الدولي لتبادل الخبرات التقنية والقانونية.

٤. تعزيز التفوق التقني عن طريق تسليط الضوء على الإنجازات الإماراتية في المحافل الدولية.

٥. توعية الجمهور عن طريق توضيح دور الذكاء الاصطناعي في الحد من الجرائم الإلكترونية عبر حملات إعلامية.

٦. تطوير التشريعات كتحديث القوانين بشكل استباقي لمواكبة التحديات المستقبلية.

٧. تعزيز التدريب المستمر، عبر تطوير برامج تدريبية متخصصة ومكثفة بالشراكة مع مراكز الذكاء الاصطناعي العالمية، وتوفير منصات تعليمية رقمية لتحديث الملاكات بشكل دوري.

٨. زيادة التمويل، بتخصيص ميزانيات أكبر لتطوير البنية التحتية التكنولوجية ،وجذب الخبراء، ودعم مشاريع البحث والتطوير (R&D) بالتعاون مع الجامعات.

٩. تعزيز التعاون التشريعي، بإنشاء لجنة مشتركة بين المؤسسات الأمنية والجهات التشريعية لمراجعة القوانين بشكل نصف سنوي،

وإشراك القطاع الخاص في صياغة السياسات التنظيمية.

١٠. تحسين تبادل المعرفة، بتنظيم مؤتمر سنوي دولي في الإمارات حول الذكاء الاصطناعي والأمن السيبراني، وإنشاء منصة وطنية لتبادل البيانات بين المؤسسات الأمنية والأكاديمية.

١١. إجراء تقويم دوري لكفاءة تطبيقات الذكاء الاصطناعي المستعملة.

١٢. تعزيز الوعي المجتمعي بأهمية الأمن السيبراني عبر حملات تثقيفية.

الخاتمة

هناك نظريات عدة تفسر دور الذكاء الاصطناعي في مكافحة الجرائم السيبرانية ومن أهمها:

١. نظرية الاختيار العقلاني، تُبين دور الذكاء الاصطناعي في زيادة تكلفة الجريمة عبر أنظمة الرصد (كالتعرف على الوجوه وكاميرات المراقبة).

٢. نظرية النشاط الروتيني، تفسر كيف تقلل تقنيات الذكاء الاصطناعي فرص الجريمة عبر تعزيز "الوصاية" (مثل: أنظمة التنبيه الذكية في نظام "عين الصقر").

٣. نظرية الانتقال الفضائي، تشرح تحوّل الجريمة إلى الفضاء الرقمي، وضرورة استعمال الذكاء الاصطناعي لمواجهة طبيعتها العابرة للحدود. وفقًا للأدبيات العلمية، يُمكّن الذكاء الاصطناعي التحول من الدفاع التفاعلي إلى الاستباقي عبر الآليات الآتية:

وتصف الأدبيات آليات عمل تطبيقات الذكاء الاصطناعي في كشف الهجمات السيبرانية ومنعها في دولة الإمارات عن طريق:

- **آليات الكشف:**

١. تحليل حركة المرور الشبكية لاكتشاف التهديدات (وظيفة الذكاء الاصطناعي في الأمن السيبراني).

٢. استعمال التعلم الآلي للتنبؤ بالهجمات المستقبلية (نظام الشرطة التنبؤية في أبوظبي).

- **آليات المنع :**

١. الحوسبة السحابية لتعزيز الكفاءة (خاصية الذكاء الاصطناعي الرابعة).

٢. أنظمة مثل "أمان الذكية" و"eCrime" للإبلاغ الفوري عن الجرائم.

- **التطبيقات العملية:**

١. تقنيات "بصمة العين" في أبوظبي.

٢. الروبوتات الشرطية في دبي للكشف عن المشاعر المشبوهة.

أما التحول النظري في الاستراتيجيات فكان على النحو الآتي:

١. نظرية الكشف المبكر: استعمال خوارزميات التعلم الآلي ؛لتحليل أنماط البيانات الضخمة، واكتشاف الشذوذ قبل تحوُّلها إلى هجمات.

٢. نظرية التكيف الديناميكي، فأنظمة الذكاء الاصطناعي تُحدِّث نماذجها باستمرار بناءً على التهديدات الجديدة مما يُحقق مرونةً تفوق القواعد الثابتة.

- الأدوات الرئيسة للتحول:

١. أنظمة SIEM المُعزَّزة بالذكاء الاصطناعي، تجميع بيانات الشبكة في الوقت الفعلي ،وتصنيف التهديدات عبر خوارزميات التصنيف.

٢. محللو السلوك، رصد الانحرافات السلوكية للمستخدمين/الأجهزة باستعمال التعلم غير المُشرف.

٣. التنبؤ بالهجمات، نماذج التنبئية (Predictive Modeling) لتوقع نقاط الضعف المستقبلية بناءً على البيانات التاريخية.

ولقد أحدث الذكاء الاصطناعي تحولًا في استراتيجيات الدفاع السيبراني التقليدية في دولة الإمارات عبر التحول من النمط التفاعلي إلى الاستباقي، وأدوات مثل: التعلم الآلي لتحليل الأنماط، والمراقبة المستمرة للشبكات، والتكيف الديناميكي مع التهديدات الجديدة. وبمراجعة الأدبيات والدراسات السابقة يمكن تحديد التحديات على النحو الآتي:

- التحديات التقنية:

١. نقص البيانات المُصنَّفة، تدريب النماذج يتطلب بيانات ضخمة مُصنفة لكن ندرتها تُقلل دقة التنبؤ.

٢. هجمات الخصومة، محاولة تضليل أنظمة الذكاء الاصطناعي عبر بيانات دخل مُعدَّلة (مثل: ارسال عينات خبيثة تخدع أنموذج التعلم الآلي).

- التحديات الأخلاقية:

١. الانحياز الخوارزمي، تحيز النماذج ضد فئات محددة (مثل: تصنيف IPs من دول معينة كتهديدات) بسبب بيانات تدريب غير متنوعة.

٢. انتهاك الخصوصية، ومراقبة الشبكات، وتحليل سلوك المستخدمين قد يتعارض مع قوانين حماية البيانات.

٣. المساءلة القانونية، وصعوبة تحديد المسؤول عند فشل النظام.

قائمة المصادر والمراجع:

المراجع:

كزيز، صباح، وقط، سمير. (٢٠١٨). أثر الجرائم الإلكترونية على أمن واستقرار الدول: قرصنة الموقع الإلكتروني لوكالة الأنباء الإلكترونية نموذجا. بحث منشور في مجلة الناقد للدراسات السياسية، العدد)٣)، صفحة (١١٩_١٤٥).

الشاعر، سعود. ٢٠٢٠.دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة). جامعة عجمان: الإمارات العربية المتحدة.

عبد الرزاق، رانا. ٢٠٢٣.دور الذكاء الاصطناعي في مواجهة الإرهاب الإلكتروني. بحث منشور في مجلة القانون والعلوم البيئية، المجلد (٢)، العدد (٢).

البابلي، عمار. ٢٠٢١.دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة، شرطة دبي.

البابلي، عمار. ٢٠١٩، دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة. بحث منشور في مجلة الفكر الشرطي، القيادة العامة لشرطة الشارقة، المجلد (٢٨)، العدد (١١٠).

النيابة العامة بدبي. ٢٠١٨.مجلد دبي القانونية، العدد (٢٨)

الشاعر، سعود. ٢٠٢٣.دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة). بحث منشور في مجلة البحوث القانونية والاقتصادية المجلد (١٣) العدد (٨٣)، صفحة (١-٣٧).

الملا، إبراهيم. ٢٠١٨.الذكاء الاصطناعي والجريمة الإلكترونية. بحث منشور في مجلة الأمن والقانون، المجلد (٢٦)، العدد (١)، صفحة

الظاهري، سعيد. ٢٠١٧.الذكاء الاصطناعي "القوة التنافسية الجديدة". بحث منشور في مجلة مركز استشراف المستقبل ودعم اتخاذ القرار، العدد (٢٩٩)، شرطة دبي.

علاي، عمار، وعبد المجيد، محمد. ٢٠٢٣.استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها. بحث منشور في مجلة جامعة الشارقة للعلوم القانونية، المجلد (٢٠)، العدد (٤)، صفحة (٣٧١-٤٢٠).

دهشان، يحيى. ٢٠٢٠.المسؤولية الجنائية عن جرائم الذكاء الاصطناعي. بحث منشور في مجلة الشريعة والقانون، العدد (٨٢).

الجبري زايد، وعبد الشكور، شهيرة، ومحمد، بيدر. ٢٠٢٢.الاستدلال والتحقيق في جرائم الإنترنت في دولة الإمارات العربية المتحدة. بحث منشور في مجلة الحكمة العالمية للدراسات الإسلامية والعلوم الإنسانية، العدد (٥)، المجلد (٢)، صفحة (٢٢٨-٢٥٢).

سالمين، الراشد. ٢٠١٠.عرض التجارب والخبرات الأمنية المختلفة في التعامل مع جرائم تقنية المعلومات والاتصالات الخاصة بالأطفال. مركز بحوث الشرطة، أكاديمية شرطة دبي، الطبعة الأولى (١): دبي.

العلماء، عمر. ٢٠١٩.البرنامج الوطني للذكاء الاصطناعي، مكتب وزير الدولة للذكاء الاصطناعي: دبي.

حداوي، أميرة، ومسلم، ضرغام، ومحمد، صفاء (٢٠٢٣). القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات–دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الأشرف. مجلة العلوم.

شرعان، عمار. ٢٠٢٠. الجريمة المعلوماتية وأثرها على التنمية الاقتصادية. الطبعة (١)، المجلس الديموقراطي العربي: برلين.

أوتاني، صفاء. ٢٠٢١. المفهوم القانوني للجرائم المستحدثة وصلته بالجريمة المنظمة. بحث منشور في مجلة جامعة تشرين للعلوم الاقتصادية والقانونية، المجلد (٤٣)، العدد (١)، صفحة (٤٢٩_٤٤٦).

الحجار، عدنان، وبشير، فايز. ٢٠٢١. الأدلة الرقمية وإثبات الجرائم السيبرانية بين التأصيل والتأويل. بحث منشور في مجلة جامعة الاستقلال للأبحاث، المجلد (٦)، العدد (١)، صفحة) ١٢٩-١٥٢).

النقبي، جمال، والمصعبي، سلطان. ٢٠٢٣.التعاون الوطني، والدولي في الجرائم الإلكترونية المشكلات والحلول. بحث منشور في مجلة المعهد العالي للدراسات النوعية المجلد (٣)، العدد (١٦)، صفحة (٥٤٤٩-٥٥٥٠)

عبد الحكيم، محمد. ٢٠٢١.دور الاستراتيجيات الأمنية لمواجهة جرائم الذكاء الاصطناعي وتكنولوجيا المعلومات. بحث مقدم إلى مؤتمر الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات (٢٣-٢٤) مايو ٢٠٢١،كلية الحقوق بجامعة المنصورة.

شيلي، إلهام. ٢٠٢٢.التجربة الإماراتية في تطبيق الذكاء الاصطناعي وتحقيق الريادة. بحث مقدم إلى الملتقى الدولي الافتراضي الثاني حول: المعاملات الرقمية وأنظمة المركز الجامعي الشيخ أمود بن مختار ايليزي: الجزائر.

References

Kaziz, Sabah, and Qat, Samir. (2018). The Impact of Cybercrimes on the Security and Stability of States: Hacking the Website of an Electronic News Agency as a Case Study. Published in Al-Naqid Journal for Political Studies, Issue (3), pp. (119-145).

Al-Shaer, Saud. 2020. The Role of Artificial Intelligence in Activating Criminal Investigation Procedures in Cybercrimes (A Comparative Study). Ajman University: United Arab Emirates.

Abdul-Razzaq, Rana. 2023. The Role of Artificial Intelligence in Combating Cyberterrorism. Published in the Journal of Law and Environmental Sciences, Volume (2), Issue (2).

Al-Babli, Ammar. 2021. The Role of Artificial Intelligence Systems in Crime Prediction, Dubai Police.

Al-Babli, Ammar. 2019. The Role of Artificial Intelligence Systems in Crime Prediction. Published in the Journal of Police Thought, Sharjah Police General Command, Volume (28), Issue (110).

Dubai Public Prosecution. 2018. Dubai Legal Journal, Issue (28).

Al-Shaer, Saud. 2023. The Role of Artificial Intelligence in Activating Criminal Investigation Procedures in Cybercrimes (A Comparative Study). Research published in the Journal of Legal and Economic Research, Volume (13), Issue (83), pages (1-37).

Al-Mulla, Ibrahim. 2018. Artificial Intelligence and Cybercrime. Research published in the Journal of Security and Law, Volume (26), Issue (1), page (1).

Al-Dhaheri, Saeed. 2017. Artificial Intelligence: The New Competitive Force. Research published in the Journal of the Center for Future Foresight and Decision Support, Issue (299), Dubai Police.

Alai, Ammar, and Abdul Majeed, Muhammad. 2023. Using Artificial Intelligence Applications in Crime Prediction and Prevention. Research published in the University of Sharjah Journal of Legal Sciences, Volume (20), Issue (4), pages (371-420).

Dahshan, Yahya. 2020. Criminal Liability for Artificial Intelligence Crimes. Research published in the Journal of Sharia and Law, Issue (82).

Al-Jabri, Zayed, Abdul Shakour, Shahira, and Muhammad, Bader. 2022. Evidence and Investigation of Cybercrimes in the United Arab Emirates. Research published in Al-Hikma International Journal

for Islamic Studies and Humanities, Issue (5), Volume (2), pages (228-252).

Salmeen, Al-Rashed. 2010. Presenting Various Security Experiences and Expertise in Dealing with Information and Communication Technology Crimes Against Children. Police Research Center, Dubai Police Academy, First Edition (1): Dubai.

Al-Ulama, Omar. 2019. The National Artificial Intelligence Program, Office of the Minister of State for Artificial Intelligence: Dubai.

Hadawi, Amira, Muslim, Dirgham, and Muhammad, Safaa (2023). Digital Leadership and its Role in Promoting Cybersecurity Behavior in Organizations - An Analytical Study of the Opinions of a Sample of Employees in Private Banks in Najaf. Journal of Sciences.

Shar'an, Ammar. 2020. Cybercrime and its Impact on Economic Development. First Edition, Arab Democratic Council: Berlin.

Otani, Safaa. 2021. The Legal Concept of Emerging Crimes and its Relationship to Organized Crime. Published in the Tishreen University Journal of Economic and Legal Sciences, Volume (43), Issue (1), pp. (429-446).

Al-Hajjar, Adnan, and Bashir, Fayez. 2021. Digital Evidence and Proving Cybercrimes: Between Principles and Interpretation. Published in the Al-Istiqlal University Journal of Research, Volume (6), Issue (1), pp. (129-152).