Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

فرص استخدام الخوارزميَّات في تعزيز الاستخبارات الأمنيَّة

Opportunities of Algorithms in Enhancing Security Intelligence

المخرجات الرئيسة:

- إن أحد أهم أهداف الاستفادة من الذكاء الاصطناعي في تحليل البيانات الضخمة لعمليات الاستخبارات هو سرعة الوصول إلى المعلومات المطلوبة، وسرعة القبض على الجناة، والتنبؤ بالأعمال والتصاعدات الإرهابية قبل وقوعها؛ كما يهدف إلى استثمار المعلومات والبيانات المعالجة من خلال الخوارزميَّات المبنية على نظم الذكاء الاصطناعي في تعزيز المهام الأمنيَّة والاستخباريَّة، والوصول إلى أعلى معدلات استخدام مخرجات التكنولوجيا في تحليل المعلومات.
- تستخدم تقنيات الذكاء الاصطناعي في مكافحة الإرهاب ورصد المحتوى الإرهابي على منصات التواصل الاجتماعي، ويتم ذلك من خلال فهم مراحل ومكونات هذه التقنيات؛ مثل: تعلم الآلة، والخوارزميَّات، ومعالجة اللغات الطبيعيَّة، والشبكات العصبية الذكية، وتحديد محتوى التطرف العنيف ومحاربة انتشار خطاب الكراهية ونشر الأفكار المتطرفة والإرهابية على منصات التواصل الاجتماعي والتنبؤ بالأحداث السياسية والعمليات الإرهابية والعنف وارتكاب الجرائم من خلال الخوارزميَّات التحليلية.

المستخلص

يتحقق التنبؤ الأمني من خلال دمج نظم المعلومات والأنظمة الذكية التي تتضمن قوالب بيانات السكان وجغرافية الأماكن المرتبطة بأنظمة المعلومات الأمنيَّة والاستخباراتية؛ حيث يقوم الذكاء الاصطناعي بفهم الخوارزميَّات الرياضية للقيام بعمليات حسابية

Abstract

Prediction in the security field is achieved through integrating information systems and intelligent technologies, utilizing population data templates and geographical information associated with security and intelligence systems. Artificial intelligence algorithms enable computational and inferential operations that serve security objectives,

1658-8886© 2024. SPP. This is an open access article, distributed under the terms of the Creative Commons Attribution-NonCommercial License.

واستنتاجية، تخدم الأغراض الأمنيَّة ومحاربة الإرهاب والجريمة والتنبؤ بهما، وتوفر الوصول إلى المعلومات المطلوبة في عملية البحث الجنائي وعمليات الاستخبارات وقدرات التعرُّف إلى الوجه والهوية الرقمية بمنتهى الدقة.

ويُعد الذكاء الاصطناعي أداة فاعلة لتحليل المعلومات والبيانات من خلال الخوارزميَّات الناتجة عن المعالجة الذكية، واستخلاص الأدلة الجنائية والرقمية، بالإضافة إلى رصد الحركات المالية المشبوهة المرتبطة بالإرهاب وتقليل المخاطر التي تواجهها الجهات المختصة في مكافحة الإرهاب، مما يعزز دوره في تقديم الدعم للجهات الأمنيَّة والاستخبارات من خلال توفير مواقف تحليلية دقيقة.

يمثل استخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالعمليات الإرهابية والإجرام المنظم، نقلة نوعية في مجال تعزيز الجهود الأمنيَّة، من خلال تحليل البيانات الضخمة واستخدام تقنيات تعلم الآلة والشبكات العصبية الاصطناعية، حيث تقوم هذه التطبيقات بالكشف عن أنماط تشير إلى أنشطة مشتبه فيها وتحديد المجموعات الإرهابية والمتطرفة وأماكنها ونوعية النشاط الإرهابي ومؤشرات للتهديدات الأمنية.

including counterterrorism, crime prevention, and prediction. They facilitate quick access to relevant information in criminal investigations, intelligence operations, and accurate facial and digital identity recognition. This enhances security awareness, aids in accurate decision-making, enables the identification of wanted individuals, and supports effective information gathering for maintaining security and preventing crimes, crises, and incidents.

Artificial intelligence is a valuable tool for analyzing information and data by employing intelligent processing algorithms. It assists in extracting criminal and digital evidence, monitoring suspicious financial transactions linked to terrorism, and reducing risks counterterrorism authorities face. Its role is further enhanced by providing analytical support to security and intelligence agencies, delivering precise analysis.

The utilization of artificial intelligence applications in predicting terrorist activities and organized crime represents a significant advancement in bolstering security efforts. These applications involve the analysis of extensive data, employing machine learning techniques and artificial neural networks. They detect patterns indicative of suspicious activities, identify terrorist and extremist groups, determine their locations and the nature of their activities, and provide indicators of security threats.

المقدمة

أصبحت ثورة الذكاء الاصطناعي جزءًا لا ينفصل عن حياتنا اليومية. وقد تطورت حتى أصبحت تستخدم في مجال مكافحة الجرائم والإرهاب واستنباط معلومات لها مدلول استخباراتي من خلال الخوارزميَّات، خاصة مع تطور الأسلوب الإجرامي والإرهابي. فالذكاء الاصطناعي يمكنه البحث والتنقيب والتحليل (data mining) في ملايين الصور والفيديوهات والمعلومات والبيانات الرقمية ومنشورات وسائل التواصل الاجتماعي وقواعد البيانات داخل

الأجهزة الأمنيَّة والاستخباراتية والإنتربول واليوروبول من أجل تحديد الجناة والمشتبه فيهم، وتحليل طبقات الإنترنت السفلية DARK WEB (رجب، 2019).

وباستخدام خوارزميات التعلم الآلى والعميق من قبل أجهزة المعلومات بالأجهزة الأمنيَّة، يتم التنبؤ بالأوقات التي قد يقع بها ارتكاب الجرائم، ومعرفة نوعياتها. وتلك التقنيات الذكية تساعد في تقليل تلك الجرائم في المدن؛ لتصل إلى 40% وفقًا لتقرير BBC في 2023 (تيدي، 2023) بشأن عصابات الجرائم الإلكترونية، وفي خلال ساعات يتم اكتشاف جرائم كاملة وتقديمها للعدالة؛ حيث يتم الاعتماد على الكاميرات الذكية وتحليل البيانات الأولية، وتحديد الوجوه والأصوات والتسجيلات من خلال عملية التحليل الذكي من خلال تقنيات الذكاء الاصطناعي، فالذكاء الاصطناعي يوفر عدالة لضبط الأمن، ويوفر أسلوب الحماية للدولة والمجتمع من الجرائم. فالخوارزميَّات تعزز الأنظمة التنبئية للعمليات والجرائم الإرهابية، وتوقع حدوثها من خلال الرصد السابق للمعلومات الرقمية المستنبطة من أدوات الذكاء الاصطناعي داخل الأجهزة الأمنيَّة والاستخباراتية؛ بهدف الحفاظ على الأمن والنظام العام وحماية المجتمعات من الإجرام. وتظهر أهمية تحليل ورقة السياسات في استخدام أنظمة تحليل المعلومات والبيانات من المصادر المفتوحة، وشبكات الإنترنت بطبقاتها المتعددة لجمع معلومات استباقية عن المحتوى الجنائي والإرهابي والسلوك العنيف على شبكات التواصل الاجتماعي، ومعلومات استباقية عن الجرائم والتنبؤ بها؛ لتعزيز قدرة أجهزة الأمن في الدول على مواجهة التحديات الإرهابية والجنائية "خاصة الإجرام المنظم" بشتى أشكاله؛ حيث يتيح جمع المعلومات بالذكاء الاصطناعي والخوارزميَّات إعداد مخرجات ونماذج لتحديد المحتوى الإرهابي والمشاركين في تلك المجموعات الخطرة، ويعزز الاستباقية المعلوماتية في تحديد الأزمات الأمنيَّة المستقبلية داخل المجتمعات، ويتم ذلك باستخدام تقنيات الذكاء الاصطناعي وأدوات التحليل التنبئي في أداء أجهزة الشرطة.

المفاهيم والمصطلحات

الإرهاب: هو استخدام العنف أو التهديد به؛ لتحقيق أهداف سياسية، أو دينية، أو اجتماعية كما يتضمن الإرهاب أعمالًا قد تكون عنيفة، أو تستهدف المدنيين، أو المؤسسات؛ بغية إيجاد رعبٍ وهلعٍ في المجتمع، ويتم تنفيذ الأعمال الإرهابية عادةً بواسطة جماعات، أو أفراد يسعون لتحقيق أهدافهم عبر تكوين تأثير نفسي، وتأثير على القرارات السياسية. وتطوَّر الإرهاب إلى استغلال التقنيات والذكاء الاصطناعي والطيارات بدون طيار، والتغلغل في تطبيقات التواصل الاجتماعي وطبقات الدارك ويب الخطيرة؛ بهدف نشر المعتقدات الإرهابية والجريمة المنظمة ودعم تمويل

الإرهاب، والتجسس وتجنيد الشباب ونشر ثقافة العنف والتطرف.

الذكاء الاصطناعي: (AI) هو مجال من مجالات علوم الحاسوب، يعنى بتطوير أنظمة وبرمجيات تكنولوجية قادرة على أداء مهام تتطلب ذكاءً بشريًّا، ويهدف إلى تصميم وبناء الحاسبات والبرمجيات التي يمكنها تنفيذ مهام ذكية، واتخاذ القرارات، وحل المشكلات. وعلى المستوى الأمني هو العقل المساعد للعناصر البشرية الأمنيَّة في تخزين ومعالجة البيانات والمعلومات، وصولًا إلى القدرة على الاستنتاج، واستنباط واستخلاص الحلول والدلائل الأمنيَّة، وحل لغز القضايا الجنائية والإرهابية.

الخوارزميَّات: تشير إلى مجموعة محددة من التعليمات البرمجية، أو الخطوات الرياضية التي تُستخدم لحل مشكلة محددة، أو إجراء مهمة محددة، ويتم استخدامها في مجال الأمن والاستخبارات في الكشف المتقدم عن التهديدات، وفي تحليل البيانات الضخمة وتحليل السلوك. والخوارزميَّات هي المعادلات الرياضية التي تتغلغل داخل المعطيات "المعلومات والبيانات والأدلة الرقمية والجنائية" والمحتوى الأمني والجنائي لتحقيق نتائج أمنية هائلة في أسرع وقت.

الشبكات العصبية الاصطناعية: وهي تُعلِّم أجهزة الحاسوب معالجة البيانات بطريقة مستوحاة من الدماغ البشري، باستخدام عقد أو عصبونات مترابطة في بنية مكونة من طبقات تشبه الدماغ البشري وإنشاء نظام تكيفي تستخدمه أجهزة الحاسوب لتتعلم من أخطائها، وللتحسين المستمر، ومن ثم، تحاول الشبكات الاصطناعية حل المشكلات المعقدة، حيث تقوم بتدريب مجموعة من الشبكات العصبية الاصطناعية، التي تسمح بتبادل المعلومات والتحقق منها على هيئة مدخلات ومخرجات يتوسطهما المعالجة "Processing" وصولًا لمرحلة النتائج والاستدلال والاستنتاج والوصول إلى الحلول الأمنيَّة السريعة التي تحقق مكاسب أمنية (خليفة، 2021).

التعلم الآلي والعميق: يمكِّن الأجهزة من استخدام الخبرة لتحسين المهام، ويقوم بتدريب النماذج الذكية لاتخاذ القرارات الأمنيَّة الصائبة، وهنا يسمى بالتعلم العميق؛ لتطور قدرة الخوارزميَّات على تحسين واتخاذ القرارات وسرعة التنبؤات والاستنتاج الدقيق.

الميتاداتا: (**Metadata**) هي البيانات الأولية التي يتم من خلالها بناء أسلوب البحث والتحري وجمع المعلومات الإلكترونية والرقمية عن القضايا أو الحوادث أو الأشخاص المتورطين في القضايا من خلال تحليل المعلومات والأرقام والبيانات وأماكن الوجود والبصمة الرقمية Digital Bimoatric prints والعناوين البريدية IP.

فرص استخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالعمليات الإرهابية

- **يعتبر الذكاء الاصطناعي (AI) أداةً قويةً في تطوير مجال مكافحة الجريمة المنظمة وتعزيز الاستخبارات،** ويمكن استخدام الذكاء الاصطناعي في الكثير من المجالات المختلفة في مجال البحث الجنائي؛ مثل: التحليل الجنائي والتحقيقات، والتحليل الجيني، والتعرُّف إلى الوجوه وتحديد المواقع (Office of the Privacy Commissioner of Canada, 2021).
- **يساهم الذكاء الاصطناعي في رفع كفاءة عمليات مكافحة الإرهاب؛** من خلال تحليل كميات كبيرة من البيانات والمعلومات المتاحة؛ مثل: السجلات الجنائية والتقارير الشرطية والوثائق القضائية؛ للكشف عن الأنماط والاتجاهات والمعلومات المهمة التي يمكن استخدامها في التحقيقات الجنائية. ويمكن أيضًا استخدام التعلم الآلي وتقنيات التصنيف والتنبؤ لتحليل البيانات وتوليد توقعات دقيقة حول الأحداث المستقبلية المحتملة وتحليل الصور والفيديوهات والصوتيات للكشف عن الأدلة والمعلومات المهمة التي يمكن استخدامها في التحقيقات الجنائية (البابلي، 2023).
- **تحليل البيانات وتحديد الجماعات والتنظيمات المتورطة في العمليات الإرهابية؛** حيث يسهم ذلك في تعزيز الأمن ومكافحة التهديدات الإرهابية بطرق أكثر فاعلية ودقة من خلال تحليل الشبكات الاجتماعية والمواقع المفتوحة، وتحليل سجل المكالمات التي تقع داخلها مفاتيح كلمات تدل على حدث إرهابي أو جنائي، أو تشكيلات عصابية، أو مخدرات أو غسل أموال وتهريب أسلحة، وتحليل المحادثات السرية داخل المجموعات المغلقة في مواقع التواصل التي تجمع الأشخاص ذوي الخطورة أو الإرهابيين، أو من هم على قوائم منع السفر والإرهاب؛ وذلك بالتنسيق مع الأجهزة الأمنيَّة والشرطة الدولية كالإنتربول واليوروبول.
- **التعرُّف إلى الأنماط المشبوهة أو السلوكيات غير الطبيعية؛** مثل: الأنشطة الإرهابية المحتملة، أو الجرائم المنظمة، أو التهديدات السيبرانية، ويمكن أن تساعد هذه القدرة على اتخاذ إجراءات استباقية للحد من التهديدات والأضرار المحتملة.
- **تحليل مصادر الاستخبارات المفتوحة: (OSINT)** مثل: الأخبار والمقالات ووسائل التواصل الاجتماعي والمنتديات العامة، كما يمكن أن يكشف الذكاء الاصطناعي عن الروابط والمعلومات الضمنية والتحليلات الإستراتيجية لتلك المعلومات (الغسية، 2022).
- **فهم وتحليل اللغة الطبيعية؛** ممَّا يُمكنه من فهم النصوص والتواصل بشكل أكثر فاعلية، ويمكن استخدام هذه التقنيات لتحليل التهديدات

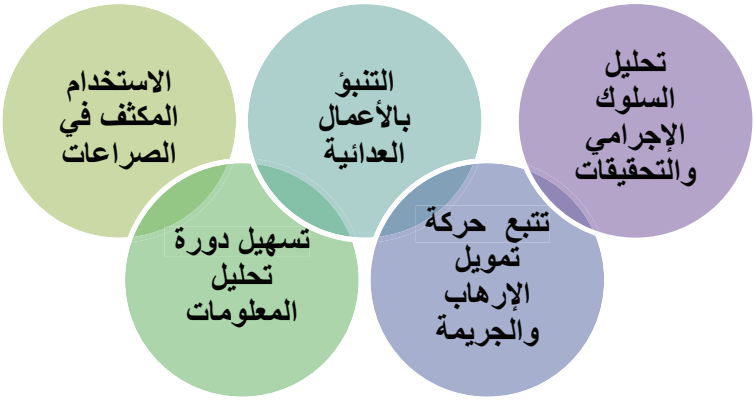
الشكل رقم (1): فرص استخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالعمليات الإرهابية

المحتملة الموجودة في الرسائل الإلكترونية، والمحادثات عبر الإنترنت، والوثائق النصية وفهم لغة الحوار بين الأطراف الإرهابية والمتطرفة، وفهم أهدافهم وتحركاتهم، وكذلك على المستوى الجنائي والجريمة المنظمة.

- **تطوير أنظمة مراقبة متقدمة للحدود والمناطق الحساسة من خلال الكاميرات الذكية والمزودة بالرؤية الليلية،** وتحليل المعلومات. ويمكن أن تساعد تقنيات التعرُّف إلى الصور والوجوه والاستشعار الحراري في تحسين عمليات التحقق والتعقب والتفتيش.
- **تحسين عمليات التحقق البيومتري والتعرُّف إلى الأشخاص من خلال ميزات فريدة ومتقدمة؛** مثل: بصمات الأصابع والوجوه وبصمات العين والصوت، ويمكن استخدام هذه التقنيات للتحقق من هوية الأفراد ومنع دخول الأشخاص غير المصرح لهم.
- **تطوير مفهوم الاستشراف الأمني بتحليل البيانات التاريخية والحالية للتنبؤ بالأحداث المستقبلية،** ودراسة وتحليل سجلات الحوادث الإرهابية والجنائية وتحليل الوقوف على أسبابها، وإجراء دراسة حالة لها ومعالجة القصور الأمني بها، وتطوير آليات مواجهة للعمليات الإرهابية بالنظم المتقدمة والخوارزميَّات. ويمكن للأنظمة الذكية تحليل البيانات الضخمة، وتقديم توقعات دقيقة للأحداث الإستراتيجية والتطورات الأمنيَّة المحتملة، ويشمل ذلك القدرة على التنبؤ بالتحولات المستقبلية، وتحديد الفرص الأمنيَّة المتاحة.

الجدول رقم (1): دور الاستشراف المستقبلي في عملية توسعة آفاق الإدراك الأمني عبر المراحل التالية:

	المرحلة الأولى	المرحلة الثانية	المرحلة الثالثة
الاستشراف المستقبلي عملية تساعد في توسعة آفاق الإدراك الأمني	تقييم المعلومات والبيانات الحاليَّة للأحداث المستقبلية لإدارة الأزمات والطوارئ والأحداث الأمنيَّة الطارئة والعمليات الإرهابية وأنماط الجريمة المنظمة	الكشف عن المشكلات وأسبابها وتجنبها قبل حدوثها باستخدام الذكاء الاصطناعي وتحليل المعلومات لاستباق الأزمات، ومنع حدوثها وسرعة التعافي منها في حالة تكرارها	الانتقال من التفكير الإستراتيجي إلى الاستشراف الإستراتيجي على حسب التغيرات المستقبلية وزيادة نسبة التركيبة السكانية والأوضاع الأمنيَّة والسياسية والدولية



الشكل رقم (2): أهمية الاستشراف الأمني في العمل الشرطي والاستخباراتي

كما يساعد الاستشراف في وضع إستراتيجيات مبكرة للتعامل مع التغيرات والتحديات المحتملة كالأزمات الإرهابية والأحداث السياسية والهجمات العدائية، وكذلك تحقيق الأمن السيبراني الفعَّال والمستديم، والعمل على استغلال الفرص الأمنيَّة المتاحة لعملية الاستشراف؛ بهدف مكافحة التنظيمات الإرهابية والإجرامية والمحافظة على استقرار الدول، وحماية المجتمعات البشرية؛ حيث يتضمن الاستشراف تحليل المعلومات السابقة للتنبؤ بالأحداث القادمة، وتجنب مخاطرها، للحفاظ على الأمن الوطني والعربي (الغسية، 2022) .

- **الاستشراف الأمني له أهمية كبيرة في العمل الشرطي والاستخباراتي؛** حيث يسهم في تحليل البيانات الجرمية والمعلومات للتنبؤ بأنماط

الجريمة ومواقعها المحتملة؛ ممَّا يمكن الشرطة من التدخل المبكر لمنع الجرائم وتوجيه الجهود والموارد إلى المناطق ذات المخاطر العالية، كما يقوم الاستشراف الأمني بتقييم وفحص ورصد ومعالجة التهديدات الأمنيَّة الكبرى؛ مثل: الإرهاب والجريمة المنظمة التي تتمثل في جمع معلومات لها مدلول أمني بالمتغيرات الجنائية، وتطور مستويات الجرائم كالاتجار بالبشر وغسل الأموال وتمويل الإرهاب والمخدرات المصطنعة وتهريب المهاجرين لضمهم داخل خلايا الإرهاب والتنظيمات الإجرامية (الغسية، 2022).

مفهوم الذكاء الاصطناعي وفقًا لمواجهة التطرف والإرهاب بمنصات التواصل الاجتماعي

- **يشير مفهوم الذكاء الاصطناعي في مواجهة التطرف والإرهاب** لتفعيل البرمجيات الذكية والخوارزميَّات نحو اتجاهات تحديد السلوك المتطرف والإرهابي والإجرامي أيضًا، والميديا "الصور والفيديوهات" الدالة على الأعمال الإرهابية والجنائية، ومنها الجريمة المنظمة والأسلوب الإجرامي المُستحدث؛ حيث تقوم البرمجيات الذكية بسرعة تحديد المعلومات والكلمات والمعاني والأشكال التي توحي بمحتوي إرهابي عبر المنصات، مثل: (العنف، الإجرام، نشر الأفكار المتطرفة). ومع ذلك، يتطلب ذلك أيضًا التوازن بين الأمان وحقوق الخصوصية، والتأكُّد من تنفيذ هذه التقنيات بطرق قانونية وأخلاقية (Schröter, 2020).

- **يقوم الذكاء الاصطناعي بمواجهة التطرف العنيف والراديكالية** "ضعف ثقافة الشباب ضد المخاطر" عبر الإنترنت، خاصةً منصات التواصل الاجتماعي بتحديد نوعية الأشخاص القابلين للتأثر بأفكار متطرفة، أو المستهدفين المحتملين من قبل الجماعات المتطرفة فكرياً، أو التنظيمات الإرهابية من خلال تحليل منصات التواصل الاجتماعي بالخوارزميَّات الذكية وحصر وتحليل نقاط الضعف وفحصها، والعمل على آليات تطويرها من قبل الأمن والمجتمع والإعلام والمدارس والجامعات.

- **تؤدي خوارزميات الذكاء الاصطناعي إلى التحليل الشامل للبيانات الضخمة والمعلومات المتاحة عبر الإنترنت** لاكتشاف الأنماط والاتجاهات المرتبطة بالأنشطة الجنائية والإرهابية، ويمكن استخدام التحليل التنبئي لتوقع وتحليل الجرائم المحتملة والهجمات الإرهابية في المستقبل. كما يُستخدم الذكاء الاصطناعي أيضًا في رصد السلوك المتطرف والإجرامى عبر الإنترنت؛ مثل: مسح المحتوى الإلكتروني والتعرُّف إلى الأنماط المشبوهة ونوعيات الجرائم الجنائية والإرهابية المستحدثة. وتُستخدم تقنيات معالجة اللغة الطبيعية لتحليل النصوص ذات الصلة بالجرائم

والأنشطة الإرهابية (تيدي، 2023).

- **يقدم الذكاء الاصطناعي فرصاً جديدة لتطوير قدرات التنبؤ والاستشراف تسهم في إدارة المحتوى المتطرف عبر الإنترنت.** ومن ضمن الأدوات التي يقدمها الذكاء الاصطناعي أنظمة التحليل والمعالجة اللغوية وقياس القابلية للتطرف والتي تمكن الأجهزة الأمنيةمن فهم وتحليل لغة التطرف عبر الانترنت.

استثمار البرمجيات المبنية على الخوارزميَّات لتعزيز مكافحة النشاط الإرهابي والتحقيقات الإرهابية

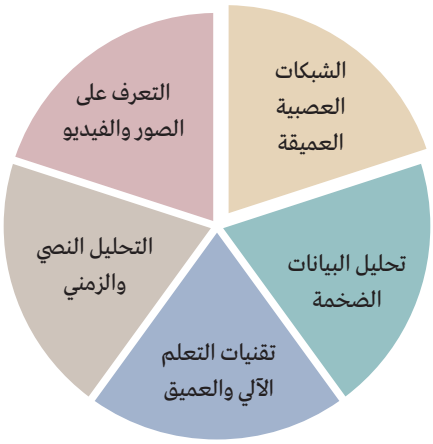
- يمكن لتقنيات التعرُّف إلى الوجوه وتحديد المواقع المدمجة في الذكاء الاصطناعي مساعدة المحققين الجنائيين في تحديد هويات المشتبه بهم، وتحديد مواقعهم؛ ممَّا يزيد من فاعليَّة التحقيقات ويساعد في الحفاظ على الأمن.
- يمكن تحليل الأدلة الجنائية والرقمية؛ لأنه نظام متقدم يستخدم التعلم الآلي وتقنيات التعرُّف إلى الصوت والصورة واللغة الطبيعية لتحليلها، ويعتمد هذا النظام على البيانات المتعلقة بالجرائم والمشتبه بهم والضحايا والشهود وغيرهم من المعلومات المتاحة لتحليل الأدلة بشكل دقيق وفعَّال وتحليل البصمة الوراثية DNA (صالح، 2022).

دور الخوارزميَّات في الاستدلال والكشف عن دلالات الإرهاب والتحقيق الجنائي

- **تستخدم الخوارزميَّات للاستدلال على علامات الإرهاب في أي بيئة، ولتحديد الأنماط أو الاتجاهات في البيانات أو المعلومات الاستخباراتية** التي قد تشير إلى احتمال وقوع هجوم إرهابي وتقوم الخوارزميَّات بتحليل البيانات للبحث عن أنماط، أو ارتباطات معينة بين العناصر المختلفة التي قد تشير إلى مؤامرة إرهابية (عبد المطلب، 2022).
- **التحليل الشبكي للتنظيمات:** تم استخدام مواقع

الجدول رقم (2): تحليل الخوارزميَّات للحصول على الأدلة الرقمية لتعزيز التحقيقات الجنائية والإرهابية

1	تحليل المحادثات الرقمية والاتصالات والرسائل البريدية وجمع معلومات الميتاداتا "البيانات الأولية والوصفية" للجناة وتحديد وإثبات أدلة الاتهام والتأكُّد من الأقوال بأمر من النيابة العامة وجهات التحقيق في قضايا الإرهاب والجريمة المنظمة والاتجار بالبشر، ورصد التواصل مع المنظمات الإرهابية والإجرامية عبر الإنترنت وقضايا الأمن الوطني، وفي حالة رصد الاتصالات الإرهابية وتسجيلها بشكل قانوني وقضائي، فسيكون ذلك بمنزلة دليل جنائي حتى في المحكمة القانونية لمحاكمة هؤلاء الإرهابيين، ويعتقد أن هذا النهج سيقلل بشكل كبير من وتيرة الهجمات الإرهابية.
2	تحليل بيانات الهواتف الذكية وسجلات الاتصالات لتحديد هوية المشتبه بهم وعلاقاتهم بالنشاط الإرهابي والإجرام المنظم.
3	تحليل البيانات الرقمية لتحديد الأدلة المتعلقة بجرائم الإرهاب وتمويله وجمع التبرعات.
4	تحليل الرسائل النصية والبريد الإلكتروني وسجلات الاتصالات والشبكات الاجتماعية واستخلاص معلومات لها دلائل أمنية للحفاظ على الأمن الوطني والأمن المجتمعي.
5	تحليل الصور الرقمية لتحديد الأدلة المتعلقة بجرائم الابتزاز الجنسي وقضايا الإرهاب والقضايا الجنائية وحوادث المرور وقضايا المجتمع وأمنه ومواجهة التحديات المستقبلية وتحليل المعلومات الحيوية (علي، 2021)



الشكل رقم (3): أنواع تطبيقات الذكاء الاصطناعي في التعرف على المحتوى الإرهابي والتحقيقات الجنائية في الحوادث والأزمات

التواصل لإجراء التحليل والعلاقات بين الأفراد والتنظيمات الإرهابية والإجرامية المنظمة وجمع البيانات الإرهابية المختلفة من أجل تحليل الضربات الإرهابية في جميع أنحاء العالم باستخدام Apriorism al - gorithm الذي يستخدم تقنيات البحث في قاعدة الارتباط داخل أنظمة الشبكات والاتصالات وتحليل المكالمات والمحادثات مع ربطها بقاعدة بيانات الإرهاب العالمي (GTD)، فإن خوارزمية Apriorism لديها القدرة على إنتاج قواعد شاملة ومناسبة تصف ربط شبكات الإرهاب والإجرام المنظم (Iorliam et al.,, 2021). وكأداة للتنقيب عن البيانات لتقييم وفحص وتحديد مستوى التهديد الذي تشكله الجماعات الإرهابية العشر الأكثر نشاطًا وعنفًا. واستخدمت تلك الخوارزمية في نيجيريا من أجل فهم تواتر الهجمات الإرهابية لتحقيقات الطب الشرعي؛ حيث تقوم تقنيات التعلم الآلي: مثل: التصنيف والتجميع والتنبؤ لتحليل البيانات المتعلقة بالإرهاب وتحديد النماذج المحتملة للأنشطة الإرهابية (شروتر، 2022).

- **يتم استخدام هذه الأدوات والتقنيات بشكل شائع في أجهزة الأمن والمخابرات لمكافحة الإرهاب والحد من الهجمات الإرهابية المحتملة.** وتوجد الكثير من الأمثلة الواقعية التي تظهر كيف يمكن استخدام الذكاء الاصطناعي والخوارزميَّات لمكافحة الإرهاب والتنبؤ بالعمليات الإرهابية (Reinsel et al., 2018):

(1) في عام 2019، استخدمت الشرطة الفرنسية الخوارزميَّات لتحليل بيانات مواقع التواصل الاجتماعي والإنترنت للكشف عن المشتبه بهم في

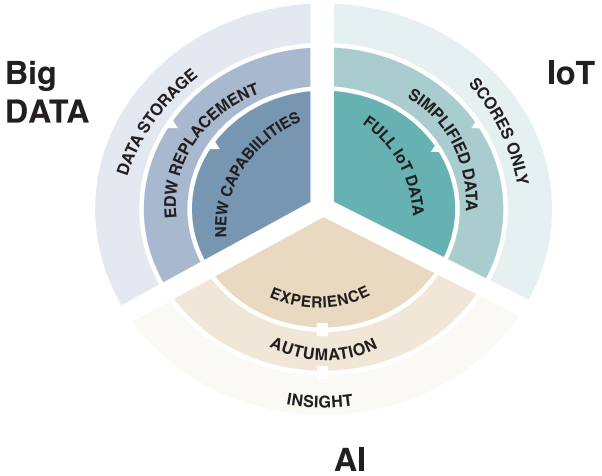
هجوم ستراسبورغ الإرهابي.

(2) في عام 2020، أعلنت شركة سيسكو عن استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات لتوقع وتحليل الأحداث المحتملة، ومن ذلك الهجمات الإرهابية، وقدمت الشركة حلولًا تقنية قائمة على البيانات لمساعدة الحكومات والجهات الأمنيَّة في فهم الأنماط والاتجاهات في حركة المرور والتنقل، وتوفير توقعات دقيقة بشأن المناطق التي قد تكون عرضة للهجمات الإرهابية، وتؤدي تلك التقنيات دورًا مهمًّا في دعم الجهود الأمنيَّة، وتعزيز القدرة على استجابة فعَّالة للتهديدات الأمنيَّة (Global Conflict Tracker, 2023).

دور الذكاء الاصطناعي في تعزيز الدلائل الأمنيَّة

- **تعتبر البيانات هي النواة التي تمكِّن من تفعيل حلول الذكاء الاصطناعي،** ويرجع جزء كبير من جاذبية تعلم الآلة machine learning إلى قُدرتها على تدريب المزيد من النماذج الدقيقة المبنية على البيانات، على عكس الأساليب التقليدية. ويلاحظ استمرار البيانات في النمو بمعدل أسرع، حيث تتضاعف كل عامين، ومن المُتوقع أن تصل إلى 175 زيتابايت بحلول عام 2055، ومن ثَمَّ يمكن استخدام البيانات المُصنفة "labeled data" وغير المُصنفة "unlabeled data"، عن طريق التقاط هذه البيانات الخام وتخزينها، ومن ثَمَّ العمل على تحليلها للوقوف على صحة المعلومات (Reinsel et al., 2018).

- **تُعد هذه الأجهزة والبرامج جزءًا حيويًّا من نظم تقييم المخاطر، وقوائم المراقبة** في المطارات



الشكل رقم (4): العلاقة الأمنية في تحليل واستنباط المعلومات من البيانات الضخمة وإنترنت الأشياء ومعالجتها بأنظمة الذكاء الاصطناعي لتعزيز الدلائل الأمنية

ونقاط المراقبة الحدودية. وتتيح قدرة الذكاء الاصطناعي تحليل وتفسير البيانات الضخمة، ورصد السلوكيات المشبوهة والتهديدات الأمنيَّة؛ ممَّا يسهم في تعزيز الأمان وتقديم إجراءات وقائية فعَّالة في مواجهة التحديات المعقدة للبيانات الكبيرة.

- **تقوم الخوارزميَّات بتمييز الأشياء والأشخاص والمشاعر الإنسانية المعقَّدة،** فضلًا عن المعلومات والظروف اليومية، وتقوم البرمجيات وأجهزة الحاسوب، على سبيل المثال، بتعلم ذاتي عبر تحليل مجموعات كبيرة من البيانات لفهم كيفية تمييز الأفراد؛ استنادًا إلى صورهم. وتتميز هذه البرمجيات بقدرتها على التعرُّف إلى أنماط السفر واللغة، وتحليلها، وربطها بالأفراد والأماكن والأحداث (Reinsel et al., 2018).
- **تحليل المعلومات باستخدام الخوارزميَّات والشبكات العصبية الاصطناعية قد يصل إلى نسبة دقيقة في تحديد الاشتباه؛** وذلك لقدرة الذكاء الاصطناعي على تتبع الأشخاص وصورهم وتحديد أماكنهم ورصدهم بتقنية EXIF واتصالاتهم وبصمتهم الرقمية Digital footprint والبصمات الحيوية Biosigna-ture المسجلة على الأجهزة الذكية والمحمولة، ومعلوماتهم على شبكات التواصل الاجتماعي والبروفيلات على الإنترنت "الميتاداتا" والعناوين البريدية المتعددة IP (عبد المطلب، 2022).

تطوير الشبكات العصبية والخوارزميات في التحقيقات الجنائية الإرهابية

- **الشبكات العصبية والخوارزميَّات** تتيح استخلاص المعلومات المهمة وتحليل البيانات الضخمة المرتبطة بالجرائم الإرهابية، وهناك عدة طرق يمكن استخدامها في هذا السياق (United Nations In-ter regional Crime and Justice Research Institute, 2019).
- **الشبكات العصبية العميقة:** (Deep Neural Networks) يمكن استخدام الشبكات العصبية العميقة لتحليل البيانات المرتبطة بالجرائم الإرهابية، وتتيح هذه الشبكات تدريب نماذج تعمل على استخلاص المعلومات والأنماط المميزة لتحديد السلوك الإرهابي والتنبؤ بالأنشطة المحتملة.
- **خوارزميات التصنيف:** (Classification Algo-rithms) يمكن استخدام خوارزميات التصنيف مثل: آلة الدعم النموذجية (Support Vector Machine) والشجرة القرارية (Decision Tree) لتصنيف البيانات المرتبطة بالتحقيقات الجنائية الإرهابية، وتساعد هذه الخوارزميَّات في تحديد السلوك الإرهابي والتمييز بين الأنشطة العادية وغير العادية.

- **التعرُّف إلى السلوك المحتمل:** يمكن استخدام الشبكات العصبية والخوارزميَّات لتحليل السلوك الإرهابي المحتمل للأفراد المشتبه فيهم، ويمكن تدريب هذه الشبكات على البيانات السابقة وتحديد السلوكيات والمعلومات المشتبه فيها التي تشير إلى النشاط الإرهابي (Baker et al., 2021).
- **التحقق من مصداقية المعلومات:** في تحقيقات مكافحة الإرهاب، غالبًا ما تكون هناك الكثير من المعلومات المتضاربة والكاذبة، ويمكن استخدام الشبكات العصبية للتحقق من مصداقية البيانات والمعلومات، وهو ما يساعد في اتخاذ قرارات استنتاجية أكثر دقةً وتأكيد المعلومات الموثوقة.
- **الكشف عن الكذب:** تقنيات تحليل الصوت والوجه والنصوص المدعومة بالذكاء الاصطناعي قد تساعد في تحديد السلوك غير الصادق ومساعدة المحققين في اكتشاف الكذب والمعلومات الزائفة.
- **تطوير تقنية بصمة المخ بالذكاء الاصطناعي في التحقيقات الإرهابية،** تهدف إلى تحديد مدى تورط المشتبه بهم في أعمال إرهابية معينة، أو معرفة المعلومات التي يمكن أن يكونوا على علم بها؛ حيث تعتمد هذه التقنية على فرضية (البرمجيات المبنية على الذكاء الاصطناعي) فالأفراد الذين شهدوا أو شاركوا في أعمال إرهابية سيُظهِرون استجابات عصبية مميزة تجاه المحتوى المرتبط بهذه الأعمال. (علاء الدين، 2021).
- **استثمار الذكاء الاصطناعي في دعم القوة الناعمة، ونزع التطرف من السجون** – من خلال استثمار الخوارزميَّات أثناء التحقيقات في تحديد سلوك المتطرفين ونواياهم وتحديد مسار تفكيرهم وتصنيفهم من خلال النظم الذكية والمتقدمة، ثم القيام بإعادة تأهيلهم (قانصو، 2021).

التوصيات

- استقدام برامج تحليل ذكية إلى داخل أنظمة المعلومات الجنائية ومراكز المعلومات والأزمات، بهدف تعزيز تحليل المعلومات وتوفير بيانات دقيقة لحل الألغاز ومعالجة القضايا الجنائية. ويُعدُّ اعتماد برامج التحليل الذكي في هذا السياق وسيلة فعَّالة لمواجهة التحديات الأمنيَّة المتزايدة؛ ما يعزز القدرة التحليلية للأجهزة الأمنيَّة، والفاعليَّة في إدارة الأزمات ومعالجة القضايا الجنائية.
- تعزيز التفاعل والتواصل المستمر بين العمل الأمني والاستخباراتي والمجتمع المحلي، وضرورة الاستفادة الفعَّالة من مخرجات ومعلومات التواصل الاجتماعي ودمجها بشكل شامل في خوارزميات قنوات الاستخبارات المعلوماتية، وتحليل تلك البيانات بشكل شامل لضمان الاستفادة الكاملة من الأدلة والتحاليل بالنظم الذكية.
- على الدول تثبيت المجسات الذكية وكاميرات المراقبة الحية التي تحمل خاصية التعرُّف إلى الوجوه

في المدن الكبرى، وينبغي ربط هذه المجسات والكاميرات بأنظمة المراقبة والدوريات الأمنيَّة ومراكز الأزمات لتحقيق رصد فعَّال واستجابة سريعة للأزمات والأحداث.

- تعزيز التعاون الأمني الرقمي مع المنصات الرقمية؛ بهدف جمع المعلومات وتحليل البيانات للتنبؤ بالأزمات والطوارئ، ومن ذلك جهود مكافحة الإرهاب والإجرام المنظم، بحيث يسعى إلى استغلال قدرات الذكاء الاصطناعي والتكنولوجيات الناشئة ذات الصلة لمواجهة التهديدات الإرهابية، خاصة في سياق مكافحة التطرف والإرهاب.

المراجع

المراجع العربية:

- البابلي، عمار ياسر. (2023). الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية "التداعيات وسبل المواجهة". المنظمة العربية للتنمية الإدارية. جامعة الدول العربية. القاهرة، مصر.
- تيدي، جو. (2023) بي بي سي ومؤسسات بريطانية كبرى تتلقى إنذارًا نهائيًّا من عصابة "كلوب". متوافر على الرابط التالي: https://www.bbc.com/arabic/science-and-tech-65778747
- خليفة، إيهاب (2021) الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس. دار العربي للنشر والتوزيع. القاهرة، مصر.
- رجب، إيمان (2019) . سياسات مكافحة الإرهاب في مصر، مجلة السياسة الدولية. مؤسسة الأهرام. العدد 296. مركز الدراسات السياسية والإستراتيجية. القاهرة، مصر.
- شروتر، ماري (2022). الذكاء الاصطناعي ومكافحة التطرف العنيف. كينجز كوليدج لندن: مشروع GNET من المشرعات الخاصة التي يقدمها المركز الدولي لدراسة الراديكالية.
- صالح، أحمد محمد .(2022) تطبيقات الذكاء الاصطناعي، ودورها في الإدارة الأمنية للحشود، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة. القاهرة، مصر.
- علاء الدين، دينيز .(2021) بصمة المخ في الإثبات الجنائي. حولية المنتدى. المجلد 1 (48).
- علي، هايدي عيسى حسن (2021). حقوق الإنسان في عصر الذكاء الاصطناعي: معطيات ورؤى وحلول. مجلة الشريعة والقانون. القاهرة، مصر.
- عبد المطلب، ممدوح (2022). الذكاء الاصطناعي وإنفاذ القانون. دار النهضة العربية. القاهرة، مصر.
- الغسية، حمدان. (2022). خارطة الطريق لاستشراف المستقبل في العمل الأمني. مركز استشراف المستقبل ودعم اتخاذ القرار. دبي،

الإمارات.
- قانصو، علي (2021) الحرب الإلكترونية. مجلة الدفاع الوطني اللبناني. بيروت، لبنان.

المراجع الأجنبية:

- Artificial Intelligence and Robotics for Law Enforcement. (2019). United Nations Interregional Crime and Justice Research Institute (UNICRI). Available at: https://www.europarl.europa.eu/cmsdata/196207/UNICRI%20 -%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf
- Baker, J., Hobart, L. & Mittelsteadt, M. (2021). AI for Judges: A Framework. Center for Security and Emerging Technology. Available at: https://www.armfor.uscourts.gov/ConfHandout/2022ConfHandout/Baker2021DecCenterForSecurityAndEmergingTechnology1.pdf.
- Global Conflict Tracker (2024). Violent Extremism in the Sahel. Available at: Violent Extremism in the Sahel | Global Conflict Tracker (cfr.org)
- Iorliam, A., Dugeri, R., Akumba, B., & Otor, S. (2021). A Forensic Investigation of Terrorism in Nigeria: an Apriori Algorithm Approach. Journal of Information Security, 12(4), 270-280.
- McKendrick, K. (2019). Artificial Intelligence Prediction and Counterterrorism. International security Department. CHATHAM HOUSE.
- Office of the Privacy Commissioner of Canada. (2021). Police use of Facial Recognition Technology in Canada and the way forward. https://www.priv.gc.ca/en/opc - actions - and - decisions/ar_index/202021/sr_rcmp/.
- Reinsel, D., Gantz, J., Rydning, J. (2018). The Digitization of the World from Edge to Core. IDC. Available at: The Digitization of the World from Edge to Core (seagate.com)
- Stewart, E. & Moll, R. (2020). How 2020 Democrats think about breaking up Big Tech. Vox. Available at: Should we break up Big Tech? Where 2020 Democratic candidates stand. - Vox
- Schröter, M. (2020). Artificial intelligence

and countering violent extremism: A primer. Global Network on Extremism and Technology.

- Valentini, D. (2020). Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization. Frontiers in Psychology.

Received 30 July. 2023; Accepted 18 Jan. 2024; Available Online 15 May. 2024.

Amar Yasser Elbably
Researcher in Information Security
Egypt

عمار ياسر البابلي
باحث في أمن المعلومات
جمهورية مصر العربية

Keywords: violent extremism, terrorism, artificial intelligence, algorithms, social media platforms

الكلمات المفتاحية: التطرف العنيف، الإرهاب، الذكاء الاصطناعي، الخوارزميات، منصات التواصل الاجتماعي.

Production and hosting by NAUSS

* Corresponding Author: Amar Yasser Elbably
Email: 3marelbably@gmail.com
doi: 10.26735/FWWV5082