التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

استثمار أدوات الذكاء الاصطناعي في مكافحة الإرهاب

د / عبيد صالح المختن

باحث في الذكاء الاصطناعي والجريمة الإلكترونية

قضايا الإرهاب 5
ديسمبر 2023

قضايا الإرهاب

إصدار شهري يصدر عن التحالف الإسلامي العسكري لمحاربة الإرهاب

المشرف العام

اللواء الطيار الركن محمد بن سعيد المغيدي

الأمين العام للتحالف الإسلامي العسكري لمحاربة الإرهاب / المكلّف

رئيس التحرير

عاشور بن إبراهيم الجهني

مدير إدارة الدراسات والبحوث

استثمار أدوات الذكاء الاصطناعي في مكافحة الإرهاب

د / عبيد صالح المختن

باحث في الذكاء الاصطناعي والجريمة الإلكترونية

استثمار الذكاء الاصطناعي في مكافحة الإرهاب يمكن أن يكون له تأثير كبير وإيجابي على الجهود المبذولة لمكافحة التهديد الإرهابي، ويتيح الذكاء الاصطناعي للأنظمة تحليل كميات ضخمة من المعلومات والبيانات بشكل أسرع وأكثر دقة، مما يساعدها على تحديد الأنماط والتهديدات المحتملة واتخاذ إجراءات مناسبة لمنع الهجمات الإرهابية (الحقيل، 2023) والتنبؤ بها وهناك توجه عالمي للاستفادة من الذكاء الاصطناعي (AI) في مكافحة الإرهاب والجريمة المنظمة، حيث تُعَدُّ البيانات جزءًا أساسيًا من استراتيجيات مكافحة الجريمة في المستقبل، وتتضمن استراتيجيات استخدام الذكاء الاصطناعي في مكافحة الجريمة والإرهاب التركيز على مجموعة من الجوانب، مثل تحليل البيانات واستخلاص الأنماط والتهديدات المحتملة، وتطوير أنظمة التعرف على الصور والفيديوهات، والكشف عن السلوكيات المشبوهة، والتحليل التنبؤي، وتقديم تقديرات بشأن التهديدات المستقبلية، وتحليل السلوك الإرهابي، وحذف المحتوى المتطرف من منصات التواصل الاجتماعي.

أولاً . أهداف الدراسة:

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 والتصعيدات الإرهابية قبل وقوعها .

استخدام تقنيات الذكاء الاصطناعي في مكافحة الإرهاب ورصد المحتوى الإرهابي على منصات التواصل الاجتماعي، وذلك من خلال فهم مراحل ومكونات هذه التقنيات، مثل: تعلم الآلة، والخوارزميات، ومعالجة اللغات الطبيعية، والشبكات العصبية الذكية، وتحديد محتوى التطرف العنيف، ومحاربة انتشار خطاب الكراهية ومحاربة نشر الأفكار المتطرفة والإرهابية على منصات التواصل الاجتماعي.

صياغة استراتيجية رقمية للتعاون الأمني الرقمي بين أجهزة الأمن العربية لمكافحة الإرهاب الممتد للبيئة السيبرانية.

الوقوف على ماهية الإنترنت المظلم (الخفي)، ووصف شبكة الإنترنت الخفي وكيفية عملها، وإلقاء الضوء على تكتيكات الإرهاب عبر الإنترنت العميق Deep Web، وتمويل الإرهاب.

ثانيًا – تساؤلات الدراسة:

– ما هي أليات استثمار الذكاء الاصطناعي لحماية المجتمعات والأفراد ضد التطرف والإرهاب؟

- ما هو مفهوم الذكاء الاصطناعي وفقاً لمواجهة التطرف والإرهاب بمنصات التواصل الاجتماعي، وما هي القدرات التي تستخدمها الشركات التكنولوجية (AI) لمكافحة المحتوى الإرهابي؟

- ما هي المخاطر الأمنية لمواقع التواصل الاجتماعي وتأثيرها على الأمن المجتمعي في المنطقة العربية؟

- كيفية تمويل الإرهاب عبر بيئة الإنترنت الخفي والتحديات الدولية التي تواجهها الأجهزة الأمنية حول العالم في رصد وتتبع النشاطات غير المشروعة؟

ثالثًا - مصطلحات الدراسة:

التطرف العنيف - الإرهاب- الفضاء الإلكتروني - الذكاء الاصطناعي (AI) -الشبكات العصبية- التعلم الآلي والعميق -الخوارزميات- منصات التواصل الاجتماعي.

رابعًا . خطة الدراسة:

بداية جاء المبحث الأول بعنوان التكتيكات الذكية للإرهاب في عمليات التمويل والتجنيد ونشر التطرف، ويضم **ثلاثة مطالب**: الأول، **استخدام الجماعات الإرهابية للتكنولوجيا والفضاء الإلكتروني**، **والثاني**، نشر التطرف العنيف من خلال المنصات الإلكترونية، **والثالث**، تكتيكات نشر التطرف والإرهاب في الإنترنت المظلم Dark Web ، **وجاء المبحث الثاني** بعنوان الذكاء الاصطناعي وفرص مكافحة التطرف والإرهاب واشتمل على **ثلاثة مطالب: الأول**، فرص استخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالعمليات الإرهابية **والثاني** استثمار البرمجيات المبنية على الخوارزميات لتعزيز مكافحة النشاط الإرهابي، **والثالث**، أليات التعاون الرقمي الأمني لمكافحة الإرهاب السيبراني، **ثم انتهت الدراسة بالخاتمة وأهم** النتائج والتوصيات.

المبحث الأول:
التكتيكات الذكية للإرهاب في عمليات التمويل والتجنيد ونشر التطرف

تمهيد:

تعتمد التكتيكات الذكية في الإرهاب على استخدام استراتيجيات متقدمة في التمويل والتجنيد ونشر التطرف، وتشمل هذه التكتيكات استخدام التمويل والاتصال السري ووسائل التواصل الاجتماعي والتشفير والاستغلال الذكي للوسائط المتعددة والوجود الرقمي المتنوع (استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، 2020)، والحقيقة في استخدام التنظيمات الإرهابية للذكاء الاصطناعي يمكن أن يكون خطيرًا للغاية إذا تم استخدامه بقصد ضار ومع سجل حافل في عالم الجرائم الإلكترونية، فهو أداة قوية يمكن تصور استخدامها لزيادة أو تسهيل الإرهاب والتطرف العنيف الذي يؤدي إلى الإرهاب، على سبيل المثال، من خلال توفير أساليب جديدة للهجمات الجسدية باستخدام الطائرات بدون طيار أو القيادة الذاتية للسيارات، أو زيادة الهجمات الإلكترونية على البنية التحتية الحيوية، أو تمكين انتشار خطاب الكراهية والتحريض على العنف بطريقة أسرع وأكثر كفاءة، ونتناول تلك المخاطر من خلال مطالب ثلاثة على النحو التالي:

المطلب الأول
استخدام الجماعات الإرهابية للتكنولوجيا والفضاء الإلكتروني

تستغل الجماعات المتطرفة التكنولوجيا وتتطور في استخدامها بسرعة، ولذلك، من المهم جدًا فهم التهديدات المتعلقة بالتطرف وتطوير استراتيجيات فعالة لمنع ومكافحة هذه التهديدات، وفهم التهديد المتزايد للتطرف وتطور أدوات التكنولوجيا التي تستخدمها الجماعات المتطرفة يعد أمرًا حاسمًا في تطوير استراتيجيات فعالة لمنع ومكافحة هذه الظاهرة مع تزايد استخدام الإنترنت ووسائل التواصل الاجتماعي كأدوات لنشر الأيديولوجيا المتطرفة، ويعزز الحاجة إلى تحليل ومراقبة المحتوى الرقمي وتطوير تقنيات التعرف على النمط والتنبؤ بالسلوك القادم للمتطرفين.

وهناك أمثلة حديثة لاستخدام الإرهابيين للتكنولوجيا مجموعة من الأجهزة المتقدمة. على سبيل المثال، تم استخدام أجهزة نظام تحديد المواقع العالمي (GPS) والهواتف المحمولة والإنترنت من قبل مرتكبي هجمات مومباي في عام 2008 للتخطيط لمهتهم وتنسيقها وتنفيذها، حيث كان يمثل في ذلك الوقت استخدامًا مبتكرًا لأحدث التطورات التكنولوجية، وفي الآونة الأخيرة، استخدم الإرهابيون الأصول الافتراضية المستندة إلى Blockchain، مثل "Bitcoin"، وكذلك الخدمات المصرفية عبر الهاتف المحمول، والتمويل الجماعي لأغراض جمع التبرعات أو

لنقل الأموال، بينما تعمل شبكة الويب المظلمة كسوق للمواد والأسلحة والمستندات المزورة.

وهناك أدلة كثيرة على استغلال هذه الجماعات للتقنيات المتعلقة بالذكاء الاصطناعي، ويلاحظ هذا على وجه الخصوص، في استغلال الأنظمة الجوية بدون طيار، والمعروفة أيضًا باسم Drone حيث تعتبر الطائرات بدون طيار تقنية مرتبطة بالذكاء الاصطناعي، لقد تباينت طبيعة استخدام الطائرات بدون طيار من قبل هذه الجماعات وتشمل، الهجمات الفعلية، والمحاولة، والتعطيل، والمراقبة، والدعاية، والتعبئة، والحشد، وتجنيد إرهابيين جدد حيث يتم تجنيد عناصر جديدة داخل المنظمات الإرهابية يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الإنترنت مع قضاياهم ويجتذبون هؤلاء بعبارات براقة وحماسية من خلال غرف الدردشة الإلكترونية كالتالي (عبد المعطي، 2012):

إعطاء التعليمات والتلقين الإلكتروني: يمتلئ الإنترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل، والأسلحة الكيمائية الفتاكة.

الحرب النفسية: نشر معلومات مضللة ونشر الرعب والخوف في نفوس الأفراد عن طريق تصوير الجرائم التي يرتكبونها والعمليات الإرهابية التي يقومون بها، وتوثيق العمليات الإرهابية وتمجيد مرتكبيها (عبد السلام، 2020).

التمويل: يستخدم الانترنت للحصول على التبرعات باستخدام التحويلات المالية عبر الإنترنت وقد يتم استخدام منظمات عالمية ذات طابع إنساني أو خيري كمظلة لتوفير التمويل أو العمل تحت غطائها.

المطلب الثاني

نشر التطرف العنيف من خلال المنصات الإلكترونية

تستند سياسة التنظيمات الإرهابية، ومنها تنظيم داعش إلى الاستقطاب الجماهيري واختراق الخصوصية الرقمية وانتهاك حقوق الإنسان بنشر مشاهد العنف، وقرصنة الرسوم (الهاشتاغات) والتطبيقات، وبرامج الحوار (الدردشة) وما يسمَّى (روبوت الويب bots) المعدَّة محلياً، ولا يكتمل مشهد التطرف والإرهاب إلا بعامل السرعة فالسرعة والخفاء تميِّزان الإنتاجَ الإعلامي لتنظيم داعش ونشرَه بعد ذلك، فإن السلوك الإعلامي لهذا التنظيم الذي رافق التفجيرات الانتحارية في 14 نوفمبر 2015م التي استهدفت العاصمة الفرنسية باريس وأسفرت عن مقتل 127 شخصًا و8 من المتطرفين؛ دلَّ على عمل إعلامي منسَّق ومعَدٍّ سابقًا، وهذا يوضح التزامنَ بين العمليات المنفَّذة والتواصل الإعلامي في المشهد الإرهابي (الإرهاب وحقوق الإنسان).

ومع بروز وسائل التواصل الاجتماعي يمكن أن يجعل الناس عرضة للتلاعب من خلال المعلومات المضللة والكشف عن المعلومات، ودمج الذكاء الاصطناعي في هذه المعادلة على سبيل المثال من خلال انتشار التزييف العميق، سيعزز إلى حد كبير طبيعة التهديدات الأمنية (ALGORITHMS AND TERRORISM، 2023)، ونتناول نشر التطرف العنيف من خلال المنصات الإلكترونية وانتهاكات البشرية على النحو التالي

أولاً: منصات التواصل وستار الأعمال الإرهابية:

تستخدم المنظمات الإرهابية مواقع التواصل الاجتماعي كأداة لتحديد أهدافها والتعرف عليها ومراقبة تحركاتها، خاصة في إطار عمليات الاغتيالات في الدول المستهدفة وذلك إما بمراقبة من يمتلك حسابات على تلك المواقع أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم وجمع البيانات اللازمة عن تحركاتهم، وهناك عدة أهداف رئيسية للجماعات الإرهابية من وسائل التواصل وهي

أغراض الاتصالات التشغيلية، وجمع المعلومات الاستخباراتية وتبادل المعلومات، والتجنيد والتدريب، وغير ذلك من استخدامات وظيفية، ففي عام 2014 أشار أحد التقارير الصادرة عن مركز «سيمون ويزنتال» Simon Wie-senthal ومقره «لوس أنجلوس»، إلى أن هناك أكثر من ثلاثين ألف منتدى وموقع إلكتروني وحساب على مواقع التواصل الاجتماعي، تروج للإرهاب في الولايات المتحدة الأمريكية وخارجها، كما اكتشفوا تزايد انضمام المتطرفين إلى شبكات التواصل الاجتماعي، ويلاحظ أن العديد من الجماعات اليمينية في وسائل التواصل الاجتماعي تعيد توجيه الجمهور نحو منتدياتها وتكشف باستمرار عن صفحات وحسابات أعضاء هذه الجماعات والمجموعات على منصات التواصل الاجتماعي مثل: الفيسبوك وتويتر (wiesenthal، 2021).

ثانياً: استغلال المجموعات الإرهابية الذكاء الاصطناعي:

تستغل المجموعات الإرهابية الذكاء الاصطناعي وهذا يعد اختراقاً، لحقوق الإنسان حيث الاستخدام السيئ للتكنولوجيا وإحداث إضرار بالمجتمعات والبشرية، وخاصة مع ازدياد إمكانية وصول الأفراد إلى تكنولوجيا التعلّم الذاتي، وفي

فبراير 2020 تم التشغيل السليم للأنظمة القائمة على الذكاء الاصطناعي ، عندما خدع فنان ألماني خرائط Google للاعتقاد بأن حركة المرور في شوارع برلين كانت أعلى مما كانت عليه في الواقع من خلال تغذية بيانات غير صحيحة إلى جهاز خريطة Google نماذج التعلم الآلي، وذلك من خلال حمل 99 هاتفاً محمولاً معه أثناء سيره في الشوارع، وهو ما فهمته خرائط Google بشكل خاطئ على أنه يقدم أشخاصاً في سياراتهم ، مما تسبب في تشغيل النظام بشكل خاطئ، وتم استخدام الإمكانات الخبيثة لخلق الفوضى والارتباك عند الاستفادة منها بشكل ضار.

ثالثاً: انتشار خطاب الكراهية والتزييف العميق عبر المنصات الإلكترونية:

تستخدم وسائل التواصل الاجتماعي كأداة لنشر الكراهية والشائعات عبر الإنترنت مما يؤدي إلى زيادة حالات العنف في المجتمع، نتيجة لتسهيل وتسريع وسائل التواصل الاجتماعي للأشخاص للنشر أو الانخراط في سلوك عنيف أو تحريضي تحت ستار الاختباء خلف شاشة الحاسوب.

كما تستخدم منصات التواصل الاجتماعي بوابة خلفية للإرهاب: لنشر خطاب الكراهية والمعلومات المضللة والمحتوى المتطرف؛ فمنحت وسائل التواصل الاجتماعي لكل عنصري عنيف منصة عامة متاحة للاستخدام الدائم، بجانب أن إخفاء الهوية في وسائل التواصل الاجتماعي منح الدول القدرة على احتضان الكراهية والتحريض عليها عبر الحدود الدولية، وكذلك تعتمد الجماعات الإرهابية على منصات التواصل الاجتماعي؛ في إضفاء الشرعية على العنف وتجنيد القتلة وتمجيد الانتصارات؛ فكان لـ «تنظيم داعش» في العراق والشام أثناء صعوده وجود متطور على وسائل التواصل وبث من خلاله مقاطع الفيديو المصوّرة لعمليات الإعدام والهجمات والمحتويات الأخرى (الشرقاوي نسرين، 2022).

وهناك أشكال للتهديدات الأمنية التي تطرحها تكنولوجيا الخداع العميق والتي تؤثر على الأمن القومي والمجتمعي، هي (خليفة، 2018)

فبركة تصريحات مسيئة لسياسيين قد تؤدي إلى اندلاع أعمال عنف أو تظاهرات أو حتى توتر العلاقات مع دول أخرى.

تتوقع شركة الأمن السيبراني فورس بوينت (Forcepoint) أن يستخدم مجرمو الإنترنت الخداع العميق لتوليد صور ومقاطع فيديو يُمكن توظيفها لطلب فدية، وبالتوازي لذلك، فمن المحتمل تزايد عمليات سرقة البيانات من خلال خداع الموظفين للتخلي عن المعلومات، بما في ذلك: بيانات اعتماد الوصول، والسجلات المالية، وغير ذلك، كما يُتوقع تزايد هجمات التصيد الاحتيالي من خلال نشر مقاطع فيديو تحتوي على البرامج الضارة، أو تسجيل الرسائل المصممة لجذب المستخدمين إلى النقر على الروابط كجزءٍ من هجمات التصيد الاحتيالي (Hames، 2020).

رابعاً: وسائل التواصل الاجتماعي وخطورتها على الأمن المجتمعي:

تلعب وسائل التواصل الاجتماعي دوراً فاعلاً في صناعة الرأي العام وتشكيله، حيث تسهم في ترويج الأفكار التي تعتنقها النخبة في المجتمع، ومن أخطر البرامج والمستجدات في العالم الرقمي برنامج تيك توك الأشهر عالمياً، وهناك تحديات أمنية عالمية لتطبيق «تيك توك»، ومنها اتهام التطبيق بالإفراط في جمع واستخراج البيانات الخاصة بالمستخدمين وإخضاعها لعمليات التحليل الموسعة، بما في ذلك النسخ غير الضروري للبيانات من الهواتف، وجمع المعلومات التي يمكن استخدامها لتحديد موقع المستخدم وتتبعه، واستخدامه وسيلة لبث الشائعات خاصة تلك التي من شأنها تهديد الأمن القومي والعربي، كما تروج بعض الفيديوهات لصور من خطابات الكراهية ونشر الأفكار المتطرفة والإرهابية ، ويقوم البرنامج بجمع كافة البيانات الأولية «Metadata»عن المستخدمين والمتابعين، وتروج بعض فيديوهات تيك توك لصور من خطابات الكراهية ونشر الأفكار المتطرفة بما يخلق حالات من النزاع والصراع داخل المجتمع، وتهدد أمنه واستقراره.

ونتناول بعض المخاطر الأمنية لتطبيق (TikTok) وسلبيات الذكاء الاصطناعي على النحو التالي: -

هناك العديد من الفيديوهات المصورة لأطفال يتم اغتصابهم وقتلهم.

تزداد التهديدات الأمنية، ويتنامى الانتباه لتوظيف بعض المتطرفين والإرهابيين باستخدام تطبيق «تيك توك»، واستخدامه في بعض الممارسات الإجرامية والمتطرفة، مثل: استخدام بعض المتطرفين في المجتمع الأمريكي لتطبيق -تيك توك- خلال أعمال الشغب واقتحام مبنى الكابيتول في يناير 2021 م، من أجل تجنيد الأشخاص ودعوتهم للعنف، والترويج للأسلحة، وتبادل الإرشادات التكتيكية المرتبطة بالأنشطة الإجرامية التي تم القيام بها (أبو دوح خالد كاظم، 2022).

المطلب الثالث

تكتيكات نشر التطرف والإرهاب في الإنترنت المظلم Dark Web

تطورت عمليات التنظيم فيما يخص التمويل وتبادل الأموال وجمع التبرعات، ولم يعد في حاجة لتلقي التمويلات من داعميه عبر حسابات بنكية في بنوك تخضع للرقابة والمساءلة، ولم يعد أيضًا في حاجة لشركات ومؤسسات لغسل الأموال أو مضاعفتها، فالإنترنت أصبح بديلاً مهمًا وكافيًا وخطيرًا، وأصبح تنظيم «داعش» قادرًا على جمع ملايين الدولارات ومضاعفتها وإنفاقها عن طريق الشبكة العنكبوتية ، بواسطة عملة «البيتكوين»، حيث تمكن القائمون على التنظيمات الإرهابية من التواصل بسرية تامة وجمع التبرعات وذلك عن طريق الإنترنت المظلم أو ما يسمى "Deep web" .

والأمر الذي دعا كثيراً من أجهزة الأمن في دول العالم، إلى ابتكار منصات وأدوات ذكاء اصطناعي، لمراقبة المحتويات الممنوع تداولها من خلال تسريب محتويات إلى مواقع أقل شهرة وأحيانًا غير معروفة، لا تملك موارد كافية تخصصها للرقابة.

ويكفي أي تنظيم إرهابي أو إجرامي في العالم لتأسيس وإدارة شبكات مالية إلكترونية، أن يوفر اتصالاً بالإنترنت وأن يمتلك حسابات افتراضية ومحافظ مالية في عدد من البنوك الإلكترونية، وأن يمتلك عناصر مدربة للعمل داخل سوق العملات الافتراضية وأن يملأ محافظه المالية بالعملات الافتراضية، إما عن طريق تبرعات أنصاره ومحبيه أو باستقبال التمويل عن طريق الإنترنت من الأجهزة والدول والكيانات الداعمة له (belfercenter. ksg. harvard, 2023).

ونتناول تكتيكات الإرهاب عبر بيئة الإنترنت المظلم كالتالي:

أولاً: تجنيد الشباب وغسيل المخ كأحد ديناميكيات التهديد الإرهابي عبر المنصات الإلكترونية:

إن تجنيد الشباب وتأثير الجماعات الإرهابية على الشباب من خلال منصات التواصل الاجتماعي والدارك ويب dark web يعد جزءًا مهماً من ديناميكيات التهديد الإرهابي للدول، ويستخدم الإرهابيون هذه المنصات للترويج للأيديولوجيات المتطرفة وجمع المعلومات وتوجيه الشباب نحو العمل الإرهابي. **وفيما يلي بعض الجوانب الرئيسية لهذه العمليات: (المنهج المرجعي لمكافحة الإرهاب، 2023)**

تأثير الثقة والترويج للتطرف: يسعى الإرهابيون إلى إقامة علاقة ثقة مع الشباب وإقناعهم بأفكارهم المتطرفة، حيث يستخدمون التلاعب النفسي والمناورات العاطفية لجذب الشباب وتجنيدهم في صفوفهم، ويتم ترويج الأفكار المتطرفة من خلال منشورات ومقاطع فيديو محفزة تستهدف هؤلاء الشباب.

ثانيًا: استخدام عملة البيتكوين في تمويل الإرهاب عبر البيئة السيبرانية:

يقوم تنظيم «داعش» باستغلال البيتكوين بطريقتين مختلفتين، الأولى: هي شراء احتياجاته من متاجر غير مشروعة عبر الإنترنت المظلم (العطار أحمد شوقي، 2021)، والثانية: هي تحويل هذه الأموال الافتراضية إلى أموال سائلة لإنفاقها على متطلباته المعيشية وعملياته المنظمة، وتعتبر الأسواق غير المشروعة على شبكة الإنترنت المظلمة لشراء وبيع السلع الممنوع تداولها بين الأفراد أحد أهم الأماكن التي ينفق فيها داعش ما بحوزته من بيتكوين لتلبية احتياجاته التشغيلية، مثل شراء جوازات سفر مزورة تمكن المتطرفين من عبور الحدود بسهولة، واستئجار المركبات والمنازل الآمنة، وشراء الأسلحة وإمدادات صنع القنابل وطائرات صغيرة دون طيار وأيضا سرقة البيانات الحساسة بشأن الأهداف التي يرصدها التنظيم في أي مكان بالعالم كالخرائط السرية والأكواد والأرقام السرية، والتي يمكن أن تيسر تنفيذ العمليات الإرهابية.

وتضمنت مواقع داعش في «الديب ويب» إعلانات للتبرع لعمليات « إرهابية»، فيظهر على الصفحة الرئيسية لموقع الأخبار التابع لتنظيم «داعش» إعلان يحمل عنوان يستخدم الإسلام كغطاء على عمليات الإرهابيين وهو «تمويل المعركة الإسلامية من هنا» (صاغور هشام، 2019) بينما هي معارك إرهابية الإسلام منها بريء وتترجم هذه العناوين باللغة العربية والإنجليزية معًا. وبالضغط على الإعلان نتحول لصفحة اسمها «صندوق الكفاح للتبرع للعمليات الإرهابية» بعملات إلكترونية من خلال عنوان إلكتروني خاص بالمعاملات المالية، يذكر أن وكالة الشرطة الأوروبية «يوروبول»، حذرت من خطر شن تنظيم داعش هجمات في أوروبا وأن ذلك الخطر لا يزال مرتفعاً للغاية، وقال رئيس جهاز مكافحة الإرهاب «في يوروبول» «مانيول نفاريت» : «مع تراجع قوة داعش، أصبح يحث أعضاءه على شن هجمات منفردة في بلدانهم بدلاً من توجيههم للسفر».

المبحث الثاني
الذكاء الاصطناعي وفرص مكافحة التطرف والإرهاب

تمهيد:

هناك فرص عديدة لتطويع أنظمة لمكافحة العمليات الإرهابية واستثمار مخرجات الذكاء الاصطناعي لتحليل السلوك الإرهابي المتوقع وكشف دلالات الإرهاب بالإضافة إلى صرف المحتوى الإرهابي على مواقع التواصل الاجتماعي واستخدام الخوارزميات لمواجهة تهريب الأسلحة النارية وتطوير التحصينات الإرهابية بنظم الشبكات العصبية الاصطناعية (course.elementsofai, 2020) **ويتم تناول ذلك من خلال مطالب ثلاثة على النحو التالي:**

المطلب الأول
فرص استخدام تطبيقات الذكاء الاصطناعي في التنبؤ بالعمليات الإرهابية

يعتبر الذكاء الاصطناعي (AI) أداة قوية في تطوير مجال مكافحة الجريمة المنظمة وتعزيز الاستخبارات، ويمكن استخدام الذكاء الاصطناعي في العديد من المجالات المختلفة في مجال البحث الجنائي، مثل التحليل الجنائي والتحقيقات والتحليل الجيني والتعرف على الوجوه وتحديد المواقع (البابلي عمار، 2023)، وباستخدام تقنيات الذكاء الاصطناعي يمكن للمحققين الجنائيين تحليل كميات كبيرة من البيانات والمعلومات المتاحة، مما يزيد من فرص نجاحهم ويتيح لهم اتخاذ القرارات المناسبة بشأن الجرائم المشابهة في المستقبل، وبالإضافة إلى ذلك يمكن للذكاء الاصطناعي تحليل البيانات الجينية والمساعدة في التعرف على المشتبه بهم وإثبات أدلة الاتهام .

ويمكن تحسين عمليات مكافحة الإرهاب بتحليل 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.

وباستخدام الذكاء الاصطناعي بشكل صحيح وفعّال يمكن أن يساهم في تحسين جهود مكافحة الإرهاب وتعزيز الأمن العام.

وتكمن التطبيقات الأمنية للذكاء الاصطناعي في التصوير، والمراقبة، وتقنية التعرف على الوجه وتعد أداة أساسية في تحديد هوية مرتكبي الحوادث الإرهابية، وقد استُخدم الذكاء الاصطناعي ونجح بالفعل في تقليص احتمالات الخطأ في مراحل البحث والتحري وكذلك في مراحل الملاحقة والسعي لإنفاذ القانون، حيث يتم تضييق دوائر الاشتباه وتسهيل عمليات الحصر والفرز للمعلومات والأشخاص والمعطيات كلها ذات الصلة، كل ذلك ساعد في رفع مستوى الدقة والكفاءة في الجانب الأمني المباشر لمواجهة الإرهاب، كما وفر مناخاً من الثقة بأجهزة الأمن وخلق طمأنينة لدى الرأي العام تجاه المؤسسات والآليات المنخرطة (فهد، وجدان، 2022) ومما سبق نتناول مفهوم الذكاء الاصطناعي كالتالي:

أولاً: تعريف الذكاء الاصطناعي:

هو أحد فروع علوم الحاسب الآلي والذي يهتم بجعل الآلات أو الحاسبات الإلية قادرة على التصرف مثل الإنسان بشكل ذكي أو عقلاني عند اتخاذ القرارات وذلك وفقاً للمعرفة المخزنة بها أو التي تتعلمها الآلة بواسطة تغذيتها بهذه المعرفة.

ثانياً: مفهوم الذكاء الاصطناعي وفقاً لمواجهة التطرف والإرهاب بمنصات التواصل الاجتماعي:

هو تفعيل البرمجيات الذكية والخوارزميات نحو أهداف سلوكية وتقنية معينة بهدف خدمة الأفراد حول العالم بهدف نشر معلومات معينة لأهداف متعددة، وعن الجانب الأمني والاستخباراتي تقوم البرمجيات الذكية بالعمل نحو سرعة تحديد المعلومات والكلمات والمعاني والصور والفيديوهات التي توحي بمحتوى إرهابي عبر المنصات سواء (العنف – نشر الثقافة الإرهابية)، والمناط بها حصرها ومتابعتها ومعرفة مسارها لدى الشركات التكنولوجية العملاقة تمهيداً لتحليلها وحذفها.

يقوم الذكاء الاصطناعي بمواجهة التطرف العنيف عبر

الإنترنت وخاصة منصات التواصل الاجتماعي بتحديد نوعية الأشخاص القابلين للتأثر بأفكار متطرفة، أي المستهدفين المحتملين سواء للجماعات المتطرفة فكرياً أو التنظيمات الإرهابية الحركية من خلال تحليل منصات التواصل الاجتماعي بالخوارزميات الذكية.

لقد استطاع استخدام الذكاء الاصطناعي في مجال مكافحة الإرهاب أن يحقق بعض المميزات التي شكلت نقاط قوة واضحة، استطاعت أن تحد من بعض الجرائم الإرهابية وذلك من خلال إيجاد الفرص التالية أو بمعنى أدق النجاحات التي حققتها تلك الاستراتيجيات لمكافحة الإرهاب العنيف: -

تحليل البيانات الضخمة والتنبؤ بالمستقبل، ومن أهم الأدوات القائمة على الذكاء الاصطناعي كمحركات البحث وأنظمة التحليل والمعالجة اللغوية الطبيعية التي تمكن شركات التكنولوجيا والأجهزة الأمنية من فهم والتعرف على لغة الإرهاب والمتطرفين وترجمة الكتابة المشبوهة التي توفر إمكانية إدارة المحتوى عبر الإنترنت خاصة فيما يتعلق باللغات التي تتواصل بها مجموعات من الأشخاص (Valentini D.; Lorusso A.; Stephan A., 2020).

هناك منصات أخرى تدعم ما يعد تطرفاً بدعوى إتاحة حرية التعبير بزعم أنها لا تريد تقييد المستخدمين، وهنا فقد أتاحت المعالجة اللغوية الطبيعية NLP المحسَّنة ترجمة المحتوى إلى لغات يجيدها المشرفون ويمكنها اكتشاف أنماط دلالية غير عادية على المواقع الإلكترونية أيضاً، بهدف التعرف على النشاط المتطرف والإرهاب ومروجيه ونوعية النشاط المتطرف عبر منصات التواصل الاجتماعي.

القابلية للتطرف: قامت شركات التكنولوجيا بتطوير أدوات لتقييم قابلية التعرض للأيديولوجيات المتطرفة العنيفة؛ مثل شركة (Jigsaw) التابعة لشركة (Alphabet Inc) المعروفة سابقاً باسم "Google Ideas"، التي أعلنت مشروعها باسم "إعادة التوجيه" الذي يستهدف مستخدمي مواقع مشاركة الفيديو الذين قد يكونون عُرضة للدعاية من الجماعات الإرهابية مثل تنظيم "داعش"(Kathleen، 2019).

الرصد: تسهم تطبيقات الذكاء الاصطناعي في تحديد الجماعة أو الطرف أو الشخص المتورط في العمل الإرهابي سواء بالتنفيذ أو التخطيط وذلك بتحليل المعطيات الخاصة بالعمليات محل التحري، مثل (نوع العملية- المكان- نوع السلاح- الهدف- مطابقة المعلومات مع التاريخ السابق للجماعات أو الأفراد المشتبه بهم).

المطلب الثاني

استثمار البرمجيات المبنية على الخوارزميات لتعزيز مكافحة النشاط الإرهابي

يمكن لتقنيات التعرف على الوجوه وتحديد المواقع المدمجة في الذكاء الاصطناعي مساعدة المحققين الجنائيين في تحديد هويات المشتبه بهم وتحديد مواقعهم، مما يزيد من فعالية التحقيقات ويساعد في الحفاظ على الأمن، ونتناول دور الذكاء الاصطناعي في تعزيز عمليات مكافحة الإرهاب على النحو التالي: -

أولاً - الأدوات التي يمكن استخدامها لتحليل الأدلة الجنائية باستخدام الذكاء الاصطناعي:

الذكاء الاصطناعي المتقدم (AI): هو نظام ذكاء اصطناعي متقدم يستخدم التعلم الآلي وتقنيات التعرف على الصوت والصورة واللغة الطبيعية لتحليل الأدلة الجنائية، ويعتمد هذا النظام على البيانات المتعلقة بالجرائم والمشتبه بهم والضحايا والشهود وغيرهم من المعلومات المتاحة لتحليل الأدلة بشكل دقيق وفعال. (صالح أحمد، 2022):

ثانياً - دور الخوارزميات في الاستدلال والكشف عن دلالات الإرهاب:

يعد استخدام الذكاء الاصطناعي للتنبؤ بالإرهاب جزءًا من الانتقال من نهج رد الفعل إلى نهج استباقي لمكافحة الإرهاب (عيسى هايدي، 2021).

تستخدم الخوارزميات للاستدلال للكشف عن علامات الإرهاب في أي بيئة ولتحديد الأنماط أو الاتجاهات في البيانات أو المعلومات الاستخباراتية التي قد تشير إلى احتمال وقوع هجوم إرهابي، وتقوم الخوارزميات بتحليل البيانات للبحث عن أنماط أو ارتباطات معينة بين العناصر المختلفة التي قد تشير إلى مؤامرة إرهابية (فهد، وجدان، 2022).

تحليل البيانات من كاميرات المراقبة والمصادر الأخرى لاكتشاف السلوك أو الأنشطة المشبوهة، ويمكن بعد ذلك استخدام الاستدلال لاستخلاص النتائج من هذه البيانات (البابلي عمار، 2023).

تحليل البيانات الضخمة: تحليل البيانات المتعلقة بالإرهاب، وتحديد النماذج والأنماط والمعلومات التي يمكن استخدامها للكشف عن التهديدات الإرهابية المحتملة.

تقنيات التعلم الآلي: مثل التصنيف والتجميع والتنبؤ لتحليل البيانات المتعلقة بالإرهاب وتحديد النماذج المحتملة للأنشطة الإرهابية (شروتر ماري، 2022).

التحليل النصي: تحليل النصوص المتعلقة بالإرهاب، وتحديد الكلمات والعبارات والأنماط المستخدمة في الاتصالات الإرهابية.

التحليل الزمني: يمكن استخدام التحليل الزمني لتحديد الأوقات التي يكون فيها الإرهابيون نشطين والعمليات الإرهابية المحتملة.

تحليل السلوك: تحليل سلوك المشتبه به والأنشطة الإرهابية المحتملة، وتحديد المعلومات التي تساعد في التعرف على المشتبه بهم ومنع الهجمات الإرهابية.

ويتم استخدام هذه الأدوات والتقنيات بشكل شائع في أجهزة الأمن والمخابرات لمكافحة الإرهاب والحد من الهجمات الإرهابية المحتملة، وتوجد العديد من الأمثلة الواقعية التي تظهر كيف يمكن استخدام الذكاء الاصطناعي والخوارزميات لمكافحة الإرهاب وتنبؤ للعمليات الإرهابية.

ثالثاً - الذكاء الاصطناعي في مكافحة تهريب الأسلحة النارية:

تلعب تدفقات الأسلحة غير المشروعة دوراً كبيراً في تأجيج الصراعات في العديد من الدول من الجرائم الصغيرة إلى التمرد والأنشطة الإرهابية، كما تتعدد آثارها السلبية خاصة الأسلحة الصغيرة والخفيفة غير المشروعة على الأمن القومي وتهديد الأمن والسلم للدول، حيث يمتلك المدنيون ما يقرب من 80% من الأسلحة الخفيفة من بينهم ميليشيات وجماعات إرهابية.

ويمكن للذكاء الاصطناعي أن يلعب دورًا حاسمًا في مكافحة تهريب الأسلحة النارية للإرهابيين. ونتناول بعض الأمثلة على كيفية استخدام الذكاء الاصطناعي في هذا السياق:

مراقبة الحدود والموانئ: تحليل البيانات الجغرافية والتدفقات المرورية ومعلومات الموانئ لتحديد النماذج غير العادية أو المشتبه بها في عمليات تهريب الأسلحة النارية، ويمكن للنظم المزودة (AI) تنبيه الجهات الأمنية إلى النشاطات المشتبه فيها.

التحليل الاستخباراتي: تحليل المعلومات والاستخبارات المتعلقة بشبكات الإرهاب والتجارة غير الشرعية للأسلحة النارية، ويمكن للتقنيات المتقدمة لتعلم الآلة تحليل البيانات الضخمة واستخلاص الأنماط والاتجاهات وربط العناصر المشتبه بها بالتهريب.

التحليل السلوكي والتعرف على الأنماط: تحليل البيانات السلوكية والتعرف على الأنماط المشتركة في سلوك المهربين والإرهابيين المحتملين من خلال مراقبة السلوك وتحليله، ويمكن اكتشاف السلوك غير العادي أو المشتبه به الذي يشير إلى تهريب الأسلحة النارية.

وبالتطبيق الذكي على تهريب الأسلحة النارية للإرهابيين، يمكن استخدام العديد من الأدوات والأساليب والخوارزميات التي تعتمد على الذكاء الاصطناعي كالتالي: -

تعلم الآلة: (Machine Learning) يمكن استخدام تقنيات تعلم الآلة لتطوير نماذج تكون قادرة على التعرف على أنماط تهريب الأسلحة النارية ويتم تدريب هذه النماذج باستخدام مجموعة واسعة من البيانات التي تشمل الأمثلة المعروفة لحالات التهريب.

التعرف على الصور والفيديو: (Computer Vision) يمكن استخدام تقنيات التعرف على الصور والفيديو للكشف عن الأسلحة النارية في الصور، وتقوم خوارزميات التعرف على الأشكال والأنماط بتحليل الصور والفيديوهات والتعرف على الأسلحة الموجودة فيها، ويمكن استخدام هذه التقنيات في نقاط التفتيش أو المراقبة الحدودية للكشف عن الأسلحة المهربة.

الشبكات العصبية العميقة: (Deep Neural Networks) استخلاص المعلومات من البيانات غير المرتبطة والمعقدة، ويمكن استخدامها في تحليل النصوص والصور والفيديوهات المتعلقة بعمليات التهريب للكشف عن النماذج والأنماط غير العادية، وتقوم الشبكات العصبية الاصطناعية بالربط بين الأشخاص والمؤسسات الإرهابية والإجرامية التي تعمل في الخفاء، وتقوم الشبكات بالربط العنقودي بين تلك المجموعات ورصدها واستخراج معلومات للأجهزة الأمنية بالمجال ذاته.

رابعاً - تطوير الشبكات العصبية والخوارزميات في التحقيقات الجنائية الإرهابية:

يلعب تطوير الشبكات العصبية والخوارزميات دورًا مهمًا في التحقيقات الجنائية الإرهابية، والشبكات العصبية الاصطناعية هي نماذج حوسبية مستوحاة من نظام الدماغ البشري، وتعتبر جزءًا من مجموعة أدوات الذكاء الاصطناعي المستخدمة في تحليل البيانات واستخلاص المعلومات المهمة ونتناول دورها كالتالي: -

تتيح الشبكات العصبية والخوارزميات استخلاص المعلومات المهمة وتحليل البيانات الضخمة المرتبطة بالجرائم الإرهابية، وهناك عدة طرق يمكن استخدامها في هذا السياق:

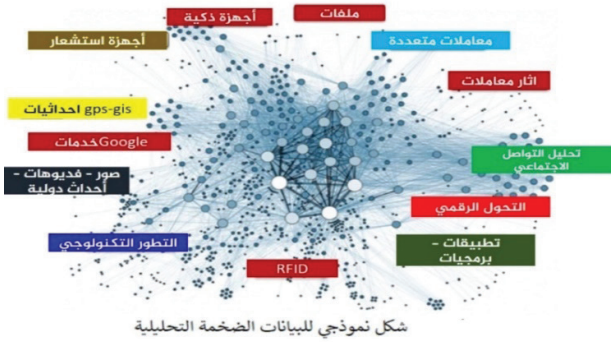
الشبكات العصبية العميقة: (Deep Neural Networks) يمكن استخدام الشبكات العصبية العميقة لتحليل البيانات المرتبطة بالجرائم الإرهابية، وتتيح هذه الشبكات تدريب نماذج تعمل على استخلاص المعلومات والأنماط المميزة لتحديد السلوك الإرهابي والتنبؤ بالأنشطة المحتملة.

خوارزميات التصنيف: (Classification Algorithms) يمكن استخدام خوارزميات التصنيف مثل آلة الدعم النموذجية (Support Vector Machine) ، والشجرة القرارية (Deci-

sion Tree) لتصنيف البيانات المرتبطة بالتحقيقات الجنائية الإرهابية، وتساعد هذه الخوارزميات في تحديد السلوك الإرهابي والتمييز بين الأنشطة العادية وغير العادية.

تحليل التجمعات: (Cluster Analysis) يمكن استخدام تقنيات تحليل التجمعات لتحليل البيانات المتعلقة بالجرائم الإرهابية وتجميعها في مجموعات متشابهة، ويمكن أن يساعد ذلك في تحديد الأنماط المشتركة والترابطات بين الجرائم وتحديد المجموعات المحتملة للمشتبه بهم.

خامساً - دور الذكاء الاصطناعي الاستخبارات العلنية وتحسين عملية اتخاذ القرار وتحليل البيانات الضخمة على المستوى الأمني:



شكل نموذجي للبيانات الضخمة التحليلية

أصبح تحليل البيانات الضخمة والمعلومات يؤسّس لأخذ القرارات الاستراتيجية لمحاربة الجرائم والإرهاب وتهديدات الأمن القومي وبناء القدرات والخطط المستقبلية البشرية واللوجستية، حيث إن معالجة وتحليل البيانات الضخمة واستخدام الذكاء الاصطناعي يكشف رؤوس الخيوط الضرورية لاكتشاف المخططات الإجرامية والإرهابية في مراحلها الأولية وتضييق مساحة العمل وبالتالي توفير الجهود والأموال، مما يؤدي إلى رفع الكفاءة والحرفية، ويتم ذلك من خلال وضع الروابط والأنماط وبناء الخوارزميات يسمح باستخراج التوقّعات والدلالات العلمية والخطوات التنفيذية من تدفّق البيانات والمعلومات، ونتناول أنواع التحليل كالآتي (الحجايا زياد، 2021):

من خلال استخدام تحليل المعلومات المتنوعة تساعد نظم (AI) في فهم البيئة المحيطة بشكل أعمق وأشمل، وتحليل الأنماط والاتجاهات والتنبؤ بالأحداث المستقبلية، وتقديم حلول وإجراءات فعالة في مجالات الأمن والاستخبارات، وعبر تحليل هذا الكم الكبير من البيانات الضخمةBig Data يمكن تقديم تحليلات وسيناريوهات آنية وفورية تأخذ في الاعتبار التغيرات السريعة وتساعد في تحسين عملية اتخاذ القرار ومساندة القوات العسكرية في الميدان، وتستخدم البيانات الضخمة في مجال الأمن القومي لتحليل أفعال الأفراد وتحصيل معلومات حول سلوكياتهم من خلال شبكات التواصل الاجتماعي، وتتضمن هذه البيانات النقاشات في مواضيع حساسة ودقيقة، وتعتبر قيّمة للغاية ويمكن استخدام تحليل شبكات التواصل الاجتماعي لكشف الأشخاص الذين يمتلكون عدة «بروفايلات» على هذه الشبكات، وذلك من خلال تحليل وربط البيانات، ويعتبر تحليل شبكات التواصل الاجتماعي أداة فعالة في محاربة الإرهاب، حيث يمكن تحديد الشبكات الداعمة ومواقع الداعمين وتحليل البيانات (رجب إيمان، 2019).

المطلب الثالث

إلات التعاون الرقمي الأمني لمكافحة الإرهاب السيبراني

يحقق التعاون الدولي في المجال الأمني على الساحات المختلفة عدة أهداف رئيسية تمثل في حقيقتها أوجه مستحدثة لهذا التعاون، وتزيد من قدر الحرص على ضرورة الوصول إليه، ويمكن القول إن تلك الأهداف تمثل في حقيقتها غايات تسعى كافة المؤسسات الأمنية في الدول العربية لتحقيق هذا التعاون وصولاً إلى أهداف مد جسور التعاون بين المؤسسات الأمنية العربية وتحقيق الأمن القومي العربي (عبد الرحمن معتز ، 2020).

أولاً: محاور تطوير سياسات التعاون الرقمي بين الأجهزة الأمنية العربية:

من خلال جمع وتحليل وتقييم المعلومات المتعلقة بالإرهاب وتحديد مستويات التهديد وإصدار تحذيرات من التهديدات وتحليل المعلومات التي تم جمعها والجمع بين خبرة الشرطة والإدارات والوكالات الحكومية في مجال مكافحة الإرهاب، بحيث يتم تحليل المعلومات ومعالجتها على أساس مشترك، مع النظر إلى المشاركة مع الإنتربول واليوروبول بشأن تبادل التطبيقات المستحدثة وتطبيقات البصمات الوراثية.

ثانياً: سبل التعاون الرقمي الأمني للحد من انتشار الجرائم السيبرانية:

جرائم الإرهاب وتمويل الجماعات الإرهابية:

تبادل المعلومات حول الأنشطة وجرائم الجماعات والمنظمات الإرهابية وعلاقتها المتبادلة وقيادتها وعناصرها وهياكلها التنظيمية السرية وواجهتها العلنية وأماكن تمركزها ووسائل تمويلها وأساليب تدريبها والأسلحة التي تستخدمها. (حمودة منتصر، 2021):

تطوير وتدعيم أساليب المراقبة وتبادل المعلومات لكشف الخطط أو الأنشطة التي تهدف إلى (نقل –استيراد – تصدير– تخزين – استخدام الأسلحة – الذخيرة –المتفجرات) وغيرها من المواد والوسائل الأخرى

.التي تساعد على ارتكاب الأعمال الإرهابية، عبر الحدود

الاطلاع على سير البيانات من دولة لأخرى وبيانات تتبع بروتوكول الإنترنت (IP address).

الجريمة السيبرانية كخدمة إذ يستخدم المجرمون تقنيات جديدة لارتكاب هجمات سيبرانية ضد الحكومات والشركات والأفراد، وهذه الجرائم لا تقف عند الحدود سواء أكانت مادية أم افتراضية، وتسبب أضراراً خطيرة وتشكل تهديدات ملموسة للضحايا في جميع أنحاء العالم، الأمر الذي يجعل تبادل التكنولوجيا مهماً وخاصة لأجهزة الشرطة و المنوط بها مكافحة الجرائم السيبرانية لفهم الإمكانات التي تتيحها للمجرمين وكيفية استخدامها كأدوات لمكافحة الجريمة السيبرانية ، خاصة تغير السلوكيات والاتجاهات على الإنترنت واستغلالهما، في ظل وجود وباء كوفيد-19.

تبادل خبرات الأجهزة الأمنية بسد الثغرات الأمنية المرتبطة بجمع وتحليل جميع المعلومات المتاحة عن الأنشطة الإجرامية المرتكبة في الفضاء الرقمي بهدف تزويد الدول بمعلومات استخباراتية، مثل

حماية البنية التحتية الإلكترونية الحرجة من الاختراق الإلكتروني والحماية من الهجمات السيبرانية للمنشآت المهمة والحيوية وخاصة هجمات الحرمان من الخدمة Denial of Service (DoS)

المراجع

أولاً - المراجع باللغة العربية:

أبو دوح خالد كاظم. (2022). سياسات التعامل مع التحديات الأمنية لتطبيق "تيك توك" Policies to Deal with "Tik Tok" Application Security Challenges، مركز البحوث الأمنية، جامعة نايف العربية للعلوم الأمنية، https://spp.nauss.edu.sa/index.php/spp/article/view/82/60.

استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. (n.d.). استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. (م. ا. الإرهاب, Editor) Re-trieved from https://news.un.org/ar/focus/counter-terrorism.

الإرهاب وحقوق الإنسان. (n.d.). https://www.ohchr.org/ar/docu-ments/reports/terrorism-and-human-rights-report-united-na-tions-high-commissioner-human-rights. تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان A/HRC/45/27.

الأوروبي. (2021). عملة «البتكوين وصدقات الجهاد على الشبكة المظلمة، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات

البابلي عمار. (2023) الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية «التداعيات وسبل المواجهة"، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية

البابلي عمار.. (2023) أليات الذكاء الاصطناعي في مواجهة التطرف العنيف. مجلة العلوم الشرطية والقانونية: دورية علمية، المجلد 14.

البار عدنان مصطفي. (2020). البيانات الضخمة ومجالات تطبيقها، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز

البهي رغدة. (2021, 3 27). الخداع العميق: تحديات أمنية وإشكالات حقيقية. https://ecss.com.eg/14200/. المركز المصري للفكر والدراسات الاستراتيجية (ESCC)، وحدة الأمن السيبراني

الحجايا 10 مايو 2021 ز. (n.d.). معالجة البيانات الضخمة والذكاء الاصطناعي في مكافحة الجريمة المنظمة والإرهاب -BIG DATA & AI Artificial Intel" ligence"، الاردن، مركز شُرُفات لدراسات وبحوث العولمة والإرهاب

الحجايا, زياد. (2021, 5 10). معالجة البيانات الضخمة والذكاء الاصطناعي "BIG DATA & AI Artificial In-telligence" في مكافحة الجريمة المنظمة والإرهاب الأردن: مركز https://www.shorufatcenter.com/4326/.. شُرُفات لدراسات وبحوث العولمة والإرهاب.

الحقيل ن. ع. (2023, 6 21). فعالية الذكاء الاصطناعي لمكافحة الجريمة والإرهاب

السمالوطي نبيل. (2021, 9). التطرف والجماعات الإرهابية في مصر «النشأة - الأهداف - موقف الإسلام منها - أساليب مواجهتها» مجلة بحوث العلوم الاجتماعية والتنمية، العدد 3.

الشرقاوي نسرين. (2022, 10 13). الأدوار المزدوجة لمنصات التواصل الاجتماعي، المرصد المصري. https://marsad.ecss.com.eg/73432/. المركز المصري للفكر والدراسات الاستراتيجية

العطار أحمد شوقي. (2021, 4 5). بنوك «داعش» على الإنترنت تتعامل بالا "بتكوين» https://www.albawabhnews.com/ تاريخ الزيارة 2022/3/3.

العلوي، إبراهيم. (2023, 7 2). تطبيقات الذكاء الاصطناعي في علوم الأدلة الجنائية. المجلة العلمية لعلوم الأدلة الجنائية

العمري. (2013). التخطيط الأمني لمواجهة تداعيات الأزمات الدولية، رسالة دكتوراه، بأكاديمية الشرطة

المنهج المرجعي لمكافحة الإرهاب. (n.d.). https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-ara-bic.PDF(2020).

الوزان، السيد. (2014). سلطة المعلومات، رؤية أمنية معاصرة، دار النهضة العربية

أوروفينو، إلسا. (2022, 9 19). التطرف عبر الإنترنت: كيفية اكتشاف المحتوى المتطرف والتعامل معه (المملكة المتحدة نموذجًا). https:// eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/. تقرير موقع عين أوروبية على التطرف

برنامج الإنتربول لتعزيز القدرات الشرطية. (2019). منظمة الإنتربول، تقرير الإنتربول. Retrieved from https://www.interpol.int/ar/1/2/2019/88th-INTERPOL-General-Assembly.

حمودة، منتصر. (2021). المنظمة الدولية للشرطة الجنائية، الطبعة الثانية، دار الفكر الجامعي

خليفة إ. (2018). فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل

ديفيد أوماند، كارل. (2015). استخبارات وسائل التواصل الاجتماعي، العدد 152، مركز الإمارات للدراسات والبحوث الاستراتيجية

راشد سامح. (2021, 10). الذكاء الاصطناعي في مواجهة الإرهاب.. فرص وتحديات. مجلة آفاق استراتيجية (4)

القاضي رامى متولي. (2021, 10). المواجهة الأمنية الدولية للأنشطة الإجرامية المرتكبة عبر شبكة الإنترنت المظلمة. مجلة الأمن العام (253).

رجب إيمان. (2019). سياسات مكافحة الإرهاب في مصر (296) مركز الدراسات السياسية والاستراتيجية

شروتر ماري. (2022). الذكاء الاصطناعي ومكافحة التطرف العنيف. كينجز كوليدج لندن: مشروع GNET من المشرعات الخاصة التي يقدمها المركز

الدولي لدراسة الراديكإلية
صاغور هشام. (2019, 7 11). مواقع التواصل الاجتماعي: منصة خصبة لنشر التطرف واستقطاب "الجهاديين". https://www.europarabct.com/?p=53141. المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات
صالح أحمد. (2022). تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود، [رسالة دكتوراه، أكاديمية الشرطة]
صالح ج. ا. (2014). "الإرهاب الفكري أشكاله وممارساته، مكتبة القانون والاقتصاد
عبد السلام ش. (2020). حروب الجيل الخامس: أسإلب التفجير من الداخل على الساحة الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة
عبد الصادق عادل . (2018). العملات المشفرة تهديد للاقتصاد والأمن القومي المركز العربي لأبحاث الفضاء الإلكترونى
عبد المعطي ن. (2012). منصات الإعلام الاجتماعي وصناعة التطرف والإرهاب.. الواقع وإلبات المواجهة: ..مجلة السياسة الدولية (213)
البابلى عمار. (2022). التعاون الرقمى الأمني بين أجهزة الأمن العربية، أوراق السياسات الأمنية، أكاديمية نايف العربية للعلوم الأمنية
فهد وجدان. (2022, 3 1). دراسة الذكاء الاصطناعي.. بين التكتيكات الإرهابية والاستراتيجيات الوطنية. https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/. مركز ترينذز للأبحاث والدراسات
فودة هالة. (2020, 11 22). وسائل التواصل الاجتماعي والأمن القومي للدول. https://marsad.ecss.com.eg/21163. المركز المصري للفكر والدراسات الاستراتيجية
قانصو على. (2021). الحرب الإلكترونيةمجلة الدفاع الوطني اللبناني « .مجلة علمية محكمة، (118)
مركز الإنتربول للابتكار. (2019). منظومة الذكاء الاصطناعي وإنفاذ القانون، المشاركة في الإنشاء من أجل تهديدات الأمن في المستقبل. https://www.interpol.int/ar/4/4/2. منظمة الإنتربول، .التقرير الدولي للأمن
عبد الرحمن معتز. (2020). دور التبادل الدولي للمعلومات في الإثبات الجنائى، [رسالة دكتوراه، أكاديمية الشرطة].
مقدادي صالح. (2021, 3 5). تقرير دولى، محفِّزات التعاون الدَّولي في محاربة الإرهاب، التحالف الإسلامي العسكري لمحاربة الإرهاب. Retrieved from https://imctc.org/ar/Pages/default.aspx.
مكتب الأمم المتحدة المعنى بالمخدرات والجريمة. (2021). التعاون الدولي في المسائل الجنائية المتعلقة بمكافحة الإرهاب. https://www.unov.org/unov/ar/unodc.html.
موقع اندبندنت بالعربية (2021, 12 17). الهجمات الإلكترونية أخطر «سلاح اقتصادي» عالمي في 2022. Retrieved from https://www.independentarabia.com.
عيسى هايدي. (2021,1). حقوق الإنسان في عصر الذكاء الاصطناعي: معطيات ورؤى وحلول. مجلة الشريعة والقانون، مجلد 35.

ثانياً - المراجع باللغة الإنجليزية:

المنهج المرجعي لمكافحة الإرهاب. (2023). https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF(2020).
ALGORITHMS AND TERRORISM. (2023). THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE FOR TERRORIST PURPOSES, United Nations Office of Counterterrorism (UNOCT), 2021 New York, AT. https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1.
belfercenter.ksg.harvard. (2023). Joseph S. Nye, The Future of Power. Press Release, Harvard Kennedy School, Belter Center for Science and International Affairs , December 2019 .at: http://belfercenter.ksg.harvard.edu/publication/20690/joseph_s_nyes_the_future_of_power.html. تم الاسترداد من belfercenter.ksg.harvard.
blog.khamsat. (2022). https://blog.khamsat.com/tiktok-prof-it-guide/. تم الاسترداد من https://blog.khamsat.com/tiktok-prof-it-guide/
Canada Police. (2021). Police use of Facial Recognition Technology in Canada and the way forward'. police science, Canada.
Christopher Rigano. (January, 2019). 'Using Artificial Intelligence to Address Criminal Justice Needs', (US NIJ Journal 280, January 2019). تم الاسترداد من www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx accessed 2 December 2021.
course.elementsofai. (2020). https://course.elementsofai.com/1/1: Reaktor & University of Helsinki) 2018(, How should we define AI?' 2. Page 10.... تم الاسترداد من https://course.elementsofai.com/1/1.
demandsage. (2, 2023). https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of%. تم الاسترداد من https://www.demandsage.com/tiktok-user-statistics/#:~:text=One%20billion%20active%20users%20spread,media%20platforms%20as%20of
Hames. (4 sep, 2020). Terror and Technology from Dynamite to Drones. War on the Rocks. Accessible at https://warontherocks.com/2020/09/terror-and-technology-from-dynamite-to-drones/. تم الاسترداد من
Kathleen. (2019). International security Department, CHATHAM HOUSE, August 2019. P.9. CHATHAM HOUSE.
molla, R. and Stewart, E. (3 12, 2019). (2019), How 2020 Democrats think about breaking up Big Tech', Vox. Accessed https://www.vox.com/policy-and-politics/2019/12/3/20965447/tech-2020-candidate-policies-break-up-big-tech. تم الاسترداد من
Office of the Privacy Commissioner of Canada. (بلا تاريخ). Office of the Privacy Commissioner of Canada, 'Police use of Facial Recognition Technology in Canada and the way forward'.
Quemener (M). (2017). Quemener (M), Enquetes dans le Dark-web, Dalloz IP/IT (الإصدار Dalloz IP/IT).
Valentini D.; Lorusso A.; Stephan A. (2020). Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization, in Frontiers in Psychology,
wiesenthal. (2021). تم الاسترداد من https://www.wiesenthal.com/about/regional-offices/los-angeles.html.
أبو دوح، خالد كاظم. (2022). سياسات التعامل مع التحديات الأمنية لتطبيق "تيك توك" Policies to Deal with "Tik Tok" Application، مركز البحوث الأمنية - جامعة نايف العربية للعلوم الأمنية.. https://spp.nauss.edu.sa/index.php/spp/article/view/82/60. الرياض
استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. (2020). استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. (مكتب الأمم المتحدة لمكافحة الإرهاب، المحرر) تم الاسترداد من https://news.un.org/ar/focus/counter-terrorism.
الإرهاب وحقوق الإنسان. (بلا تاريخ). https://www.ohchr.org/ar/documents/reports/terrorism-and-human-rights-report-unit-ed-nations-high-commissioner-human-rights. تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان A/HRC/45/27.
الأوروبي. (2021). عملة "البتكوين" وصدقات "الجهاد" على الشبكة المظلمة، المانيا: المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات
البابلي، عمار. (2023). الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية «التداعيات وسبل المواجهة». القاهرة: المنظمة العربية للتنمية الإدارية، جامعة الدول العربية
البابلي، عمار. (2023). إلبات الذكاء الاصطناعي في مواجهة التطرف العنيف، مجلة العلوم الشرطية والقانونية: دورية علمية، المجلد 14.

البار، عدنان مصطفي. (2020). البيانات الضخمة ومجالات تطبيقها. السعودية: كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز
البهي، رغدة. (27 3, 2021). الخداع العميق: تحديات أمنية وإشكاليات حقيقية. https://ecss.com.eg/14200/. المركز المصري للفكر والدراسات الاستراتيجية (ESCC)، وحدة الأمن السيبراني
الحجايا، زياد. (10 5, 2021). معالجة البيانات الضخمة والذكاء الاصطناعي في مكافحة الجريمة المنظمة والإرهاب -"BIG DATA & AI Artificial In telligence"./. https://www.shorufatcenter.com/4326. الأردن: مركز شُرُفات لدراسات وبحوث العولمة والإرهاب
السمالوطي، نبيل. (9, 2021). التطرف والجماعات الإرهابية في مصر «النشأة - الأهداف - موقف الإسلام منها - أساليب مواجهتها». مجلة بحوث علوم الاجتماعية والتمية، العدد 3.
الشرقاوي، نسرين. (13 10, 2022). الأدوار المزدوجة لمنصات التواصل الاجتماعي، المرصد المصري. https://marsad.ecss.com.eg/73432/. القاهرة: المركز المصري للفكر والدراسات الاستراتيجية
العطار، أحمد شوقي. (5 4, 2021). بنوك «داعش» على الإنترنت تتعامل بالـ "بتكوين». https://www.albawabhnews.com/ تاريخ الزيارة 2022/3/3.
العلوي، إبراهيم. (2 7, 2023). تطبيقات الذكاء الاصطناعي في علوم الأدلة الجنائية. المجلة العلمية لعلوم الأدلة الجنائية
العلوي، على إبراهيم. (2 7, 2023). تطبيقات الذكاء الاصطناعي في علوم الأدلة الجنائية. المجلة العلمية لعلوم الأدلة الجنائية
العمري. (2013). التخطيط الأمني لمواجهة تداعيات الأزمات الدولية، رسالة دكتوراه. القاهرة: كلية الدراسات العليا، بأكاديمية الشرطة
العمري، أحمد عادل. (2013). التخطيط الأمني لمواجهة تداعيات الأزمات الدولية، رسالة دكتوراه. القاهرة: كلية الدراسات العليا، بأكاديمية الشرطة
الوزان، السيد. (2014). سلطة المعلومات، رؤية أمنية معاصرة. القاهرة: دار النهضة العربية
الوزان، السيد حلمى. (2014). سلطة المعلومات، رؤية أمنية معاصرة. القاهرة: دار النهضة العربية
أوروفينو، إلسا. (19 9, 2022). التطرف عبر الإنترنت: كيفية اكتشاف المحتوى المتطرف والتعامل معه (المملكة المتحدة نموذجًا). https://eeradicalization.com/exploring-online-radicalization-how-to-spot-extremist-content-and-what-to-do-about-it/. المملكة المتحدة: تقرير موقع عين أوروبية على التطرف
إيهاب خليفة. (2018). فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل
برنامج الإنتربول لتعزيز القدرات الشرطية. (2019). منظمة الإنتربول، تقرير الإنتربول. تم الاسترداد من https://www.interpol.int/ar/1/2/2019/88th-INTERPOL-General-Assembly.
جمال الدين محمد صالح. (2014). "الإرهاب الفكري أشكاله وممارساته" (المجلد الأولى). الرياض: مكتبة القانون والاقتصاد
حمودة، منتصر. (2021). المنظمة الدولية للشرطة الجنائية (المجلد الطبعة الثانية). الإسكندرية: دار الفكر الجامعى
حمودة، منتصر سعيد. (2021). المنظمة الدولية للشرطة الجنائية (المجلد الطبعة الثانية). الإسكندرية: دار الفكر الجامعى
ديفيد أوماند، كارل. (2015). استخبارات وسائل التواصل الاجتماعي (المجلد العدد 152). أبو ظبي، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية
راشد، سامح. (10, 2021). الذكاء الاصطناعي في مواجهة الإرهاب.. فرص وتحديات. مجلة آفاق استراتيجية، العدد (4)
رامى متولي القاضي. (10, 2021). المواجهة الأمنية الدولية للأنشطة الإجرامية المرتكبة عبر شبكة الإنترنت المظلمة. مجلة الأمن العام، العدد 253.
رجب، أيمان. (2019). سياسات مكافحة الإرهاب في مصر (المجلد العدد 296). القاهرة: مركز الدراسات السياسية والإستراتيجية
زياد الحجايا. (بلا تاريخ). معالجة البيانات الضخمة والذكاء الاصطناعي في مكافحة الجريمة المنظمة والإرهاب -"BIG DATA & AI Artificial Intel ligence"، الاردن، 10 مايو 2021. الأردن: مركز شُرُفات لدراسات وبحوث العولمة والإرهاب
شادي عبد السلام،. (2020). حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية. الإمارات، أبو ظبى: مركز المستقبل للأبحاث والدراسات المتقدمة
شروتر، ماري. (2022). الذكاء الاصطناعي ومكافحة التطرف العنيف. كينجز كوليدج لندن: مشروع GNET من المشرعات الخاصة التي يقدمها المركز الدولي لدراسة الراديكالية
صاغور، هشام. (11 7, 2019). مواقع التواصل الاجتماعي: منصة خصبة لنشر التطرف واستقطاب "الجهاديين". https://www.europarabct.com/?p=53141. المانيا: المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات
صالح، أحمد. (2022). تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود، رسالة دكتوراه. القاهرة: كلية الدراسات العليا، اكاديمية الشرطة
عبد الصادق، عادل . (2018). العملات المشفرة تهديدا للاقتصاد والأمن القومي. القاهرة: المركز العربي لأبحاث الفضاء الإلكترونى
على، معتز عبد الرحمن. (2020). دور التبادل الدولي للمعلومات في الإثبات الجنائى، رسالة دكتوراه. القاهرة: كلية الدراسات العليا، أكاديمية الشرطة
عمار البابلى. (2022). التعاون الرقمى الأمني بين أجهزة الأمن العربية، أوراق السياسات الأمنية. الرياض: أكاديمية نايف العربية للعلوم الأمنية
عمار ياسر البابلى. (2022). التعاون الرقمى الأمني بين أجهزة الأمن العربية، أوراق السياسات الأمنية. الرياض: أكاديمية نايف العربية للعلوم الأمنية
فهد، وجدان. (1 3, 2022). دراسة الذكاء الاصطناعي.. بين التكتيكات الإرهابية والاستراتيجيات الوطنية. https://trendsresearch.org/ar/insight/ai-between-terrorist-actics-and-national-strategies/.
الإمارات، أبو ظبى: مركز ترينـدز للأبحاث والدراسات
فودة، هالة. (22 11, 2020). وسائل التواصل الاجتماعي والأمن القومي للدول. https://marsad.ecss.com.eg/21163. القاهرة: المركز المصري للفكر والدراسات الاستراتيجية
قانصو، على. (2021). الحرب الإلكترونية (المجلد العدد 118). لبنان: مجلة الدفاع الوطني اللبناني « مجلة علمية محكمة «
مركز الإنتربول للابتكار. (2019). منظومة الذكاء الاصطناعي وانفاذ القانون، المشاركة في الإنشاء من أجل تهديدات الأمن في المستقبل. https://www.interpol.int/ar/4/4/2. سنغافورا: منظمة الإنتربول، التقرير الدولي للأمن
معتز عبد الرحمن. (2020). دور التبادل الدولي للمعلومات في الإثبات الجنائى، رسالة دكتوراه. القاهرة: كلية الدراسات العليا، أكاديمية الشرطة
مقدادي، صالح. (5 3, 2021). تقرير دولى، محفّزات التعاون الدَّولي في محاربة الإرهاب، التحالف الاسلامي العسكري لمحاربة الإرهاب. تم الاسترداد من https://imctc.org/ar/Pages/default.aspx.
مقدادي، صالح السعد. (5 3, 2021). تقرير دولى، محفِّزات التعاون الدَّولي في محاربة الإرهاب، التحالف الاسلامي العسكري لمحاربة الإرهاب. تم الاسترداد من https://imctc.org/ar/Pages/default.aspx.
مكتب الأمم المتحدة المعنى بالمخدرات والجريمة. (2021). التعاون الدولي في المسائل الجنائية المتعلقة بمكافحة الإرهاب. https://www.unov.org/unov/ar/unodc.html.
موقع اندبنتد بالعربية. (17 12, 2021). موقع اندبنتد بالعربية الهجمات الإلكترونية أخطر «سلاح اقتصادي» عالمي في 2022. تم الاسترداد من https://www.independentarabia.com.
موقع اندبنتد بالعربية الهجمات الإلكترونية. (17 12, 2021). موقع اندبنتد بالعربية الهجمات الإلكترونية أخطر «سلاح اقتصادي» عالمي في 2022. تم الاسترداد من https://www.independentarabia.com.
ميلر، السيد ديفيد أوماند، كارل. (2015). استخبارات وسائل التواصل الاجتماعي (المجلد العدد 152). أبو ظبي، الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الإستراتيجية
نجلاء عبد الرحمن الحقيل. (21 6, 2023). فعالية الذكاء الاصطناعي لمكافحة الجريمة والإرهاب
نها عبد المعطي. (2012). منصات الإعلام الاجتماعي وصناعة التطرف والإرهاب.. الواقع وإليات المواجهة
هايدي عيسى. (1, 2021). حقوق الإنسان في عصر الذكاء الاصطناعي: معطيات ورؤى وحلول. مجلة الشريعة والقانون، مجلد 35.