رقم الترميز الدولي / ISSN (P): 2710-2653
ISSN (E): 2960-253X /
رقم الايداع الوطني / 2375 / 2019

تاريخ استلام البحث 3 / 1 / 2024
تاريخ قبول البحث 29 / 2 / 2024
تاريخ النشر 31 / 3 / 2024

توظيف التنظيمات الإرهابية للتطور التكنولوجي في تهديد الأمن والاستقرار الدوليين

Terrorist organizations employ technological development to threaten international security and stability

أ.م.د. أوراد محمد مالك كمونه

Dr. Awrad Muhammad Malik Kammona

جامعة بغداد / كلية العلوم السياسية

Baghdad University / College of Political Science

awrad.m@copolicy.uobaghdad.edu.iq

IRAQI Academic Scientific Journals

https://www.iasj.net/iasj/journal/393/issues

الملخص

يتداخل التطور التكنولوجى مع الإرهاب بدرجة كبيرة تتجاوز توظيف الإنترنت ووسائل التواصل الاجتماعي، من أجل نشر الأفكار والحصول على الدعم والتمويل وتجنيد عناصر جديدة، إلى مساحة التكتيكات وتقنيات الهجمات الإرهابية ، وكل ما يرتبط بترسانة أسلحة الإرهاب في الحاضر والمستقبل، وفي حين تقدم التكنولوجيا الكثير من الفوائد في مجالات مختلفة، وتسهم في تحقيق مكاسب متعددة للبشرية، فإنها توفر للتنظيمات والعناصر المتطرفة والإرهابية مجموعة من الأسلحة والوسائل التي تحاول من خلالها تجاوز جهود الرصد والمكافحة والقيود المفروضة على استخدام الأسلحة، كما تساعد على تخطيط عملياتها الإرهابية وتنفيذها ، وبعد أن كان الإرهابى جزءًا من السلاح المستخدم في العملية الإرهابية ، دخلت أنواع أخرى من الأسلحة والأدوات والوسائل على المشهد الإرهابي، وقد سمحت الأسلحة المستخدمة بتنفيذ عمليات عبر المسافات، من خلال أجهزة التحكم عن بعد، والطائرات بدون طيار «المسيرات» وغيرها من التقنيات التى تمكن العناصر الإرهابية من تضخيم تأثير العمليات وفقا لمعادلة تقليل التكاليف، بما فيها تكاليف العناصر الإرهابية المنفذة للعمليات، والتسبب في أكبر قدر من الخسائر والرعب فى المجتمع المستهدف أو الدولة المعنية.

الكلمات المفتاحية : "التطور التكنولوجي"،"التنظيمات الإرهابية" ، "توظيف"، "تهديد الأمن والأستقرار"

Abstract

Technological development intersects with terrorism to a large extent, beyond the use of the Internet and social media, in order to spread ideas, obtain support and financing, and recruit new elements, to the area of tactics and techniques of terrorist attacks, and everything related to the arsenal of terrorist weapons in the present and future, while technology offers many benefits. In various fields, and contribute to achieving multiple gains for humanity, they provide extremist and terrorist organizations and elements with a set of weapons and means through which they attempt to bypass monitoring and control efforts and the restrictions imposed on the use of weapons. They also help in planning and implementing their terrorist operations, after the terrorist was part of the weapon. Used in the terrorist operation, other types of weapons, tools and means have entered the terrorist scene. The weapons used have allowed the implementation of operations across distances, through remote control devices, drones and other technologies that enable terrorist elements to amplify the effect of operations according to In order to reduce costs, including the costs of terrorist elements carrying out operations, and causing the greatest amount of losses and terror in the targeted community or the country.

Keywords: technological development, terrorist organizations, employment, threat to security and stability.

المقدمة:

يشهد العالم تهديدات أمنية غير تقليدية ترتبط في أغلبها بالتطورات التكنولوجية المتسارعة، إذ أسهمت التكنولوجيا في تغير المفاهيم الخاصة بطبيعة التهديدات ودرجة تأثيرها على الأمن والاستقرار على الصعيدين الداخلي والدولي، فقد أسهمت القفزات التكنولوجية في بروز ساحة جديدة للتفاعلات الدولية تعتمد على شبكات رقمية ذات صلة بأجهزة الحواسيب بمختلف دول العالم، لتشكل "الفضاء السيبراني" الذي أضفى بعدا جديدا على نوعية الصراعات من حيث طبيعة الفاعلين وأساليب إدارة الصراع.

أضحى الإرهابيون بسبب التكنولوجيا لا يتسمون "بالصورة النمطية" التي قد ترتسم لهم، بل أصبحوا يمتلكون درجة عالية من التقنية، وعلى حد قول "جيرهارد شندلر" من قسم مكافحة الإرهاب في وزارة الداخلية الألمانية: "إنه أصبح أمرا اعتيادياً أن ترى الإرهابي غير متسلح ببندقية، بل بجهاز حاسوب متنقل"، كما يجمع مصطلح "الإرهاب الإلكتروني بين مفهوم الإرهاب والفضاء الإلكتروني ، وأدى تنوع استخدامات التطبيقات التكنولوجية إلى اتجاه التنظيمات الإرهابية لاستخدامها لتنفيذ أنشطتها والافادة مما توفره في زيادة فعاليتها، وقد وفرت التطبيقات الإلكترونية إمكانية تواصل العناصر الإرهابية الميدانية مع قيادتها المسؤولة عن تخطيط وإدارة العمليات الإرهابية قبل وأثناء وبعد تنفيذ عملياتهم، ويمكن من خلال تلك التطبيقات متابعة أكثر من خلية ميدانية في الوقت نفسه، وتنفيذ عمليات إرهابية متزامنة في مناطق جغرافية مختلفة، مما أتاح لعناصر التنظيمات المنتشرة التواصل بسرعة والتنسيق بشكل فعال، وزادت من تنوع وتعقيد المعلومات التي يمكن تداولها بينهم من خلال ما توفره من إمكانية تشفير تلك المعلومات.

المبحث الأول : التطور التقني للتكنولوجيا والإرهاب الدولي

لا تتوقف التكنولوجيا عن التطور، ربما بالقدر نفسه، الذي لا يتوقف الإنسان فيه عن الخوف من التكنولوجيا وما يمكن أن تصل إليه الأوضاع في المستقبل بحكم التطورات التي يعرف نتائجها ، وفي الوقت الذي ترتبط فيه التكنولوجيا بالكثير من الإنجازات المفيدة للبشرية، ترتبط بشكل أوسع بالحديث الدائم عن نهاية العالم.

اولاً : التكنولوجيا والإرهاب بين الامس واليوم

أن السؤال الذي يطرح نفسه هو سبب اهتمام التنظيمات الإرهابية بالتكنولوجيا، وكذلك فكرة استخدام المتاح من تقنيات المرحلة بوصفها أداة إضافية من أجل السيطرة ؟ وفي هذا السياق، أكد آدم دولنيك، أستاذ دراسات الإرهاب في جامعة ولونجونج الاسترالية، " أن الجماعات الإرهابية راديكالية تختار تكييف التكنولوجيا وفقا لأهدافها الإستراتيجية والتنظيمية والتكتيكية، وأن التكنولوجيا شيء يستخدمه المتطرفون لاستكمال التكتيكات التقليدية، واستخلص نتيجة مفادها: "أن الجماعات الإرهابية قد تكون مبتكرة في كيفية تطبيقها للتكنولوجيا، ولكن تفكيرها وأفعالها محدودة النطاق" وتمثل تلك النتيجة نقطة مهمة في التعامل مع الفكرة الحاكمة للعلاقة بين التطرف والإرهاب من جانب والتكنولوجيا من جانب آخر، فالتكنولوجيا ليست الهدف، والبحث عن

التكنولوجيا الأكثر تطورا لا يرتبط بالرغبة في مواكبة التطور، ولكن بالقدرة على استخدام تلك الأدوات وتوظيفها بسهولة وسط الجمهور المستهدف لتحقيق غايات تلك التنظيمات [1] .

يتضح من بعض مراحل التطور التاريخي كيف استطاعت العناصر المتمردة أو المتطرفة والإرهابية، حسب المرحلة والمسميات المستخدمة، توظيف الأسلحة العسكرية القائمة من أجل مصالحها، وكيف، وهو الأهم، استطاعت توظيف الأدوات العادية في معركة عسكرية، وترتبط علاقة تلك التنظيمات بالتكنولوجيا لدى البعض بضرب وإسقاط ثلاث طائرات سوفيتية في أفغانستان باستخدام أربعة صواريخ ستنجر في ١٩٨٦، ولكن تلك المعركة التي تم فيها توظيف الأسلحة المستخدمة من قبل الدول بواسطة التنظيمات من غير الدول تختلف عن استخدام العشائر الصومالية في 3 تشرين الأول ١٩٩٣ لكل من الراديو والتليفون المحمول في التعبئة ضد غارة للقوات الأمريكية في العاصمة مقديشيو، فيما عرف باسم حادث "سقوط الصقر الأسود"، والتي أثارت اهتمام القيادة الأمريكية بسبب الكيفية التي تم بها الجمع بين وسائل الاتصالات وعملية التعبئة [2].

لا سيما أن الديناميت يختلف عن تصورنا للتكنولوجيا بمفاهيم اليوم، إلا أنه دشن مرحلة جديدة مع استخدام العناصر الفوضوية للمتفجرات الصغيرة بشكل أدهش السلطات التي لم تنجح في صناعة الأسلحة نفسها، كما وفرت بندقية الكلاشينكوف AK– 47 قفزة تكنولوجية للعناصر الإرهابية، وسمحت لها بالتغلب على قوات الأمن في الأماكن التي لم تمتلك التكنولوجيا نفسها، ولأنها سلاح خفيف وسهل أتاح الكلاشينكوف للوحدات الإرهابية الصغيرة تحقيق نوع من التكافؤ في مواجهة القوات الحكومية ، وأدى انخفاض التكلفة والاستخدام الواسع للكلاشينكوف، كما حدث مع الديناميت، للانتشار الكبير الذي أثبت أنه مهم وحيوي مثل الاختراع نفسه ، ولهذا يتخوف البعض من التوسع والانتشار في الأسلحة الحديثة والتي يمكن أن تسبب الكثير من الخسائر في حالة ترك المجال لسباق التسلح ووصلت تلك الأسلحة للتنظيمات الإرهابية وانتشرت مثل الكلاشينوف [3].

وكما تم استخدام أدوات تقليدية بشكل يتجاوز الأهداف الإرهابية الأساسية في الأمس، استغلت التنظيمات الإرهابية شبكات التواصل الاجتماعي "السوشيال ميديا"، وشبكات التواصل مفتوحة المصدر للتجنيد والتخطيط وتنفيذ الهجمات والمنافسة في حرب المعلومات، وفي حين استمر أسامة بن لادن حتى مقتله في تحفيز أتباعه من خلال شرائط الفيديو، كما ساعد الإنترنت في شن هجمات محلية على الأراضي الأمريكية وصنع الإخوة تسارنايف القنبلة التي استخدمت في ماراثون بوسطن ٢٠١٣ من تعليمات مجلة "إنسباير"، التابعة لتنظيم القاعدة في جزيرة العرب، بعنوان: "كيف تصنع قنبلة في مطبخ والدتك"[4].

وساعدت التطورات في مجالات مثل المواصلات والاتصالات في زيادة استخدام التكنولوجيا من قبل العناصر الإرهابية ، وفشلت أجهزة تنفيذ القانون في العديد من الدول في توقع استخدام أشياء عادية مثل الهواتف وفاتح أبواب الكراج في إطلاق العبوات الناسفة، وأدهشت التنظيمات الإرهابية وما تستخدمه من تكنولوجيا تجارية غير مكلفة ويمكن الوصول إليها بسهولة خلال العقود الأخيرة ، ويتمثل الهدف الأساسي من

توظيف التكنولوجيا من قبل العناصرالإرهابية في طبيعة الخيال العنيف وفكرة المعركة الحاسمة التي يمكن لها إنهاء الصراع لصالحها ، وكلما تم اتخاذ الخطوات التي تسرع من حسم المعركة، عبر زيادة الصراع والكراهية وبث الرعب في المجتمعات المستهدفة، كلما تم تنفيذ الأهداف الإرهابية بشكل أسرع من وجهة نظر تلك التنظيمات، وهو ما يفسر أهمية الإنترنت والوجود على مسرح الأحداث للتنظيمات الإرهابية [5].

ثانياً : الذكاء الأصطناعي بين الإيجابيات والسلبيات

يعد الذكاء الاصطناعي أحد أنواع العلوم الحديثة التي أنتشرت على نطاق واسع خاصة مع دخوله في كثير من المجالات الصناعية والبحثية، ومنها الروبوتات والخدمات الذكية للحكومات والشركات ، ويكمن جزء أساسي من جاذبية الذكاء الاصطناعي في قدرته على تحليل كميات هائلة من البيانات، يطلق عليها البيانات الضخمة، والعثورعلى الأنماط والعلاقات بينها بسرعة، واستقراء النتائج المحتملة لسيناريو معين بناء على تلك البيانات ، ورغم الانتشار لا يوجد تعريف عالمي للذكاء الاصطناعي الذي يتم التعامل معه بوصفه تقنية متطورة تحاكي الذكاء البشرى عبر خوارزميات معقدة تتعامل مع معلومات تسهل في النهاية من تقديم مخرجات تتشابه مع السلوك الإنساني بما يجعل منها أداة مهمة لتنفيذ الكثير من المهام دون الحاجة لوجود البشر [6].

على الرغم من الحديث عن السلبيات التي ترتبط بالذكاء الاصطناعي في مجال العمل وسرقة الوظائف، وتهديد الخصوصية، إلا أن هناك الكثير من الاستخدامات الإيجابية وخاصة تلك التي تتعلق بالأمراض والأوبئة بشكل يجعل الروبوت وسيلة لتعزيز قدرات البشر، والتنبؤ بأماكن انتشار بعض الأمراض، أو مواجهة العنف، كما لعب الذكاء الاصطناعي دورا في المساعدة على تسريع تطوير لقاحات أساسها حمض الريبونوكليك مثل بعض اللقاحات التي استخدمت في مواجهة "كوفيد19[7].

ويؤدي تداخل الإيجابيات مع السلبيات إلى حالة من الجدل حول الذكاء الاصطناعي واستخداماته بين علماء الأخلاق ورجال السياسة والعاملين في مجال التكنولوجيا على مستوى العالم. ومحاسبتها ويشغل الروبوت مكانة خاصة في الجدل المثار في مجال التسليح وكل ما يرتبط بصناعة الجندي الخارق أو عالم الآلة المسيطرة بكل ما تحمله سيطرة تنظيمات إرهابية على سلاح متطور قائم على الروبوتات المسلحة أو تطويرها من مخاطر. تصورات تفتح المجال للحديث عن القتل العشوائي الذي لا يمكن إيقافه بسهولة في إشارة لفكرة قضاء الآلة على البشر، وهو خوف يحدث عندما يتجاوز "الروبوت" القوانين الثلاثة الحاكمة التي وضعها في عالم الخيال الكاتب الأمريكي – الروسي إسحق أزيموف في رواية "التملص"، الصادرة عام ١٩٤٢، والتي تؤكد على التزام الروبوت بحماية وطاعة البشر وحماية الروبوت نفسه مع مركزية القاعدة الأولى الممثلة في عدم إيذاء البشر [8].

وبشكل عام، مثلت الطائرات المسيرة واحدة من التقنيات التي استرعت انتباه المتخصصين بقوة مع رصد تطوير عناصر من "داعش" لها بعد استخدامها من قبل قوات التحالف في عمليات استهدفت شخصيات مهمة

في التنظيم، مثل محمد اموازى الشهير بالجهادي جون وجنيد حسين مسؤول ملف التجنيد في تحليل الإلكتروني بالتنظيم عام ٢٠١٥. وتم التحذير بشكل خاص من فرص امتلاك التنظيمات الإرهابية لطائرات بدون طيار مثل الطائرات الرخيصة التي تسعى الولايات المتحدة الأمريكية والصين على تطويرها، والخوف أن يؤدى سباق التسلح في الذكاء الاصطناعي إلى زيادة استخدام الطائرات الموجهة الذكية من التنظيمات الإرهابية. وتتجاوز المخاوف من "الدرونز" عمليات الاستهداف المباشر إلى استخدامها في نشر السموم والأوبئة في حرب بيولوجية تتزايد احتمالاتها والمخاوف منها في ظل زيادة الاستثمار في تلك التكنولوجيا وبالتالى فرص الانتشار والاستخدام كما حدث مع الديناميت والكلاشينكوف[9].

في المقابل، يمكن أن يكون الذكاء الاصطناعي أداة قوية في مكافحة الإرهاب وتمكين أجهزة تنفيذ القانون والمكافحة من تعزيز الفاعلية عبر خطوات، مثل تحديد العمليات المالية المشبوهة التي قد تكون مؤشرا على تمويل الإرهاب، ومراقبة نشاط الإرهاب على الإنترنت بسرعة تتجاوز القدرات البشرية. كما يوفر استخدام الإنترنت من قبل التنظيمات الإرهابية فرصة للحصول على المزيد من المعلومات عن أنشطتها وربما المخططات المستهدفة وفرص ردعها، ويتيح الذكاء الاصطناعي الفرصة للتعامل مع البيانات بكفاءة واكتشاف ما بينها من أنماط في أسرع وقت ممكن. ورغم جدل حول أهمية التنبؤ ومعرفة المخططات قبل التنفيذ، يظل من المهم، في حال فشلت تلك الجهود، كشف التنظيمات والخلايا المسئولة ومحاسبتها، وهو ما يؤكد على أهمية البيانات والقدرة على التسليح التعامل معها بشكل علمي ومنظم. في هذا السياق، أكد برايان لسيطرة دريك، مدير العلوم والتكنولوجيا الخاصة بالذكاء الاصطناعي في وكالة الاستخبارات الدفاعية الأمريكية، على أهمية الوثائق التي تم الحصول عليها بعد غارة مجمع أبوت آباد التي استهدفت أسامة بن لادن في ٢ ايار ٢٠١١، ودورها في اكتشاف الخطط المستقبلية للتنظيم بسبب الاستثمار في الذكاء الاصطناعي، وخاصة تكنولوجيا التعرف على النص والترجمة الآلية وتصنيف الصوت والصورة [10]، ورغم أهمية تعريف الجمهور بالمخاطر المرتبطة بالذكاء الاصطناعي ووجود الإرهاب في الفضاءات والمنصات المختلفة، وكيفية مكافحته وخاصة في ظل التحولات الرقمية والاعتماد المتزايد على الإنترنت، مازالت المعرفة بتلك المخاطر محدودة، بما فيها داخل أجهزة تنفيذ القانون.

ثالثاً : الهجمات السيبرانية وأستخدامها

يقصد بالهجمات السيبرانية استغلال الشبكات الحاسوبية لشن هجوم بهدف تعطيل النظم المستهدفة بما فيها نظم الحاسوب والخوادم وبنيتها التحتية الأساسية عبر الاختراق الحاسوبي، أو التقنيات المتقدمة للتهديد المستمر، أو فيروسات الحاسوب، أو البرمجيات الضارة، أو الإغراق أو غيرها من وسائل الدخول غير المصرح به أو الأهداف الضارة، وتحمل تلك الهجمات سمات العمليات الإرهابية عندما تعمد إلى نشر وبث الخوف والترويع من أجل تحقيق أهداف سياسية أو اجتماعية. ويتم تعريف الإرهاب الإلكتروني بأنه استخدام

البرمجيات في إحداث عمليات إرهابية واسعة النطاق مثل اختراق أنظمة عمل المطارات وشبكات النقل والمفاعلات النووية مما يؤدى إلى خسائر كبيرة في الأرواح [11].

ويعد استخدام الهجمات السيبرانية تحديثا في مشهد الإرهاب، إذ تقدم تلك العمليات عددا من المميزات للتنظيمات الإرهابية، ومنها: تتم خبرة مرحلة ما قبل الهجوم خلسة وتنخفض فيها مخاطر الهجوم السيبراني مقارنة بالهجمات الإرهابية التقليدية، كما تنخفض تكلفة السلاح السيبراني مقارنة بالأسلحة التقليدية (المتفجرات، والأسلحة، والمعدات وغيرها)، والعمل عبر المسافات الآمنة، مع تحقيق الآثار نفسها المترتبة على الهجمات الإرهابية ، ورغم امتلاك عدد قليل من الدول للبرامج اللازمة لشن الهجمات السيبرانية، تظل الإمكانية متاحة لشن هجمات بالوكالة من خلال توفير التقنيات اللازمة لتنظيمات إرهابية عبر دول أو عبر تسرب تلك التقنيات للتنظيمات الإرهابية، ويخشى الكثير من الخبراء من قدرات الإرهابيين في هذا المجال، إذ يتيح توافر الأدوات والاستخدام في عالم الجريمة السرى للإرهابيين بسهولة إصابة شبكات الكمبيوتر والبنية التحتية على مستوى العالم، ويمكن أن يهاجم الإرهابي بنية تحتية حيوية من أجل التخريب، أو أنظمة كمبيوتر من أجل سرقة بيانات حساسة واستخدامها في الهجمات، وبغض النظر عن حقيقة أن الجماعات الإرهابية ليس لديها الخبرة الضرورية من أجل تخطيط أسلحة سيبرانية جديدة، يظل الخطر قائما من محاولة تلك التنظيمات إجراء هندسة عكسية لقواعد البرامج الضارة المنتشرة عبر الإنترنت وتجنيد الهاكرز من أجل المشاركة في حملات الاختراق، وتستثمر تلك التنظيمات بقوة في التكنولوجيا، ويغشى الخبراء الأمنيون من إمكانية شن هجمات سيبرانية من خلايا منعزلة بشكل كامل، ويمكن أن تسبب تلك الهجمات تخريبا أو تسريب معلومات حساسة لها تأثيرات مهمة على الأمن القومي في الدول أو تؤدى إلى سقوط ضحايا والتسبب في خسائر ضخمة[12].

المبحث الثاني : أستخدام التكنولوجيا في تمويل ومكافحة الإرهاب الدولي

تعد قضية الإرهاب الإلكتروني من القضايا الصاعدة في الاهتمام الدولي في ظل ارتباطها بالتطور التقني المتسارع من جهة، وتحول المصالح الإستراتيجية إلى الفضاء السيبراني من جهة أخرى، ويأتي ذلك مع توجه العديد من الحكومات نحو التحول الرقمي، وتضاعف معدلات الانتشار والنفاذ لتكنولوجيا الاتصالات والمعلومات، وارتبط بتلك المتغيرات الجديدة حدوث تحول كمى ترافق معه تحول كيفى آخر كان لهما بالغ الأثر في القيم والسلوك للفاعلين، سواء من الدول أو من غير الدول.

أولا : استخدام التكنولوجيا في تمويل الإرهاب

تتطلب الأعمال الإرهابية في طبيعتها السرية، وحيثما لا تستطيع أساليب جمع الأموال التقليدية تلبية احتياجاتها يظهر تمويل جديد تدريجيا، ولتحسين سرية تمويل الإرهاب والحد من مخاطره كثيرا ما تختار المنظمات الإرهابية تنويع أنشطتها التمويلية وفقا للحالة الفعلية لتطور المنطقة التي يجمعون منها الأموال وتلك التي ينفذون فيها عملياتهم. ومع انتشار التكنولوجيا المالية Fin Tech التي تستخدم التقنيات الرقمية والإنترنت المطورة حديثا في صناعات الخدمات المصرفية والمالية، بدأت موجة جديدة من أساليب التمويل.

وقالت كريستين لاغارد، مدير عام صندوق النقد الدولي في جلسة عامة لـ "فرقة العمل المعنية بالإجراءات المالية" : (التكنولوجيا المالية هي سيف ذو حدين، يمكن استخدامها لتعزيز وتمويل الإرهاب من خلال إخفاء هوية العملات الافتراضية، ولكن يمكن أيضا أن تكون أداة قوية لتعزيز دفاعاتنا ضد تمويل الإرهاب)،[13] وفي السنوات الأخيرة، تزايدت كمية الأدلة على استخدام العملات المشفرة، وأكثرها انتشارا البيتكوين، في الأنشطة الإجرامية، وهو وضع يدفع المشرعين لإدخال علوم التشفير المتقدمة في العديد من هيئات الرقابة المالية.ومن اساليب تمويل التي مكنت منها التكنولوجيا هي:

1ــ منصات التمويل الجماعي

قامت المنظمات الإرهابية بالجمع بين التمويل الجماعي والتبرعات الخيرية، ولإخفاء الأغراض الحقيقية لحملات جمع الأموال وتجنب الحجب، يتم استخدام لغة غامضة أو ذريعة لجمع الأموال لأغراض خيرية وإنسانية، وبدلا من استخدام النص المكتوب يتم استخدام صورة أو فيديو وفيه عنوان التبرع، مما يجعل من المستحيل اكتشافها من خلال محركات البحث القياسية، ويجعل من الصعب تحديد المواقع التي تحتوى على هذه الإعلانات التي غالبا ما يتم تبادلها من خلال الشبكات الاجتماعية، كما يستخدم منظمو حملات جمع التبرعات عبر الإنترنت أنظمة وأدوات دفع متعددة لتلقى الأموال، بحسب ما يحظى بالشعبية بين مجموعات الداعمين [14]

ولتجنب الكشف، يضمن منظمو خطط التمويل "تناوب" متطلبات الدفع بين البطاقات المدفوعة مسبقا، والمحافظ الإلكترونية، وبطاقات الائتمان، والحسابات الإلكترونية، والهواتف المحمولة، وكذلك العملات المشفرة. ولا تستخدم تقنيات التمويل الجماعي فقط لجمع المال، ولكن لتحويل الأموال إلى الخارج، ويتم بها تجنب الكيانات المالية المنظمة، ووثقت السنوات القليلة الماضية عدة حالات لمنظمات حاولت الحصول على أموال باستخدام التمويل الجماعي بالعملات المشفرة ، وانتشر استخدام العملات المشفرة كأداة لدفع الفدية والابتزاز. ففي هجمات "برامج الفدية" يتم استخدام برمجيات القرصنة الالكترونية للاستيلاء على بيانات الشركات والمؤسسات وتشفيرها، ثم إخفاؤها والمطالبة بدفع فدية مقابل إعادة تلك البيانات، أو بيعها لمن يدفع أكثر[15] ،ويلاحظ أن معظم المعاملات غير المشروعة التي يجريها الإرهابيون والمجرمون العالميون تكون على الشبكة المظلمة Dark Net/Web. والتي تحوى مجموعة من المواقع المشفرة التي لا يمكن الوصول إليها إلا باستخدام مجموعة معقدة من أدوات الأمان.

2ــ العملات الرقمية(العملات غير الورقية)

يعود تاريخ نشوء العملات الرقمية إلى عام 1996، مع بدايات الأموال انتشار شبكة الإنترنت، إلا أنه مع نمو الحاجة استمرت هذه العملات في الظهور، وهي في تزايد متسارع، وكل منها له استخدام وخلفية مختلفة ، فالعملات غير الورقية تنقسم إلى ثلاثة أنواع هي: العملة الرقمية، والعملة الافتراضية، والعملة المشفرة، **العملة الرقمية** :هي مفهوم واسع يشير إلى جميع الأصول النقدية التي في شكل رقمي، **والعملة**

الافتراضية، مجموعة فرعية من العملة الرقمية، أما **العملة المشفرة** فهي مجموعة فرعية من العملة الافتراضية، وهي عملات غير موجودة في شكل مادى، ويتم تحديد القيمة حسب العرض والطلب[16] .

أظهرت الدراسات أنه منذ عام ٢٠١٤، بدأت المنظمات الإرهابية في استخدام العملات الرقمية المشفرة لتمويل عملياتها، على الرغم من أنه فيما يتعلق بالوضع الحالي، فإن العملة المشفرة لم تصبح قناة التمويل الرئيسة للمنظمات الإرهابية. ومن الصعب توقع مسار التوسع في استخدام العملات الرقمية من قبل المنظمات الإرهابية في المستقبل، فهذا يعتمد على العديد من العوامل غير المعروفة، مثل تطور تكنولوجيا العملات الرقمية وثقة الجمهور في العملة المشفرة، وإذا كانت العصابات الإجرامية عبر الدول تعتمد في السابق على نظام "الحوالة" و"الهوندى" كوسائل لتنفيذ المعاملات المالية الدولية بسبب ملاءمتهما للمعاملات غير المشروعة، إلا أن العملات المشفرة وفرت لهم خيارا أكثر قابلية للتطبيق كبديل لتلك الآليات. وتوفرت مؤشرات موثوقة على ضعف أجهزة إنفاذ القانون في ضبط العملات المشفرة التي تستخدم لتنفيذ التعاملات المتعلقة بالاتجار بالبشر والمخدرات والفساد[17] .

ثانياً : مكافحة الإرهاب التكنولوجي

بدأت الدول في استخدام أنظمة دفاع قوية تستخدم التكنولوجيا لمواجهة الإرهاب الإلكتروني، وهناك العديد من الطرق الواعدة للحد من هذه الهجمات الإرهابية، وتنمو الهجمات الإلكترونية بنفس سرعة نمو الابتكار التكنولوجي ، فالتقنيات التي تمكن الإرهاب الإلكتروني مفيدة أيضا لتقليل مخاطر التهديدات. ومن هذه التقنيات هي [18]:

1ــ شريحة الحاسوب عالية التقنية التي تمنع الهجمات بشكل استباقى:

أعلن الباحثون في جامعة ميشغان أنهم توصلوا إلى طريقة استباقية لردع أي هجوم إلكتروني، عن طريق شريحة تقوم بتشفير وتغيير بياناتها وترميزها ٢٠ مرة في الثانية، حتى إذا اخترق أحد المتطفلين جهاز حاسوب، فإن المعلومات التي يحتاجون إليها لاستغلال ثغرة أمنية تختفي في غضون أجزاء من الثانية. وأكد الباحثون أن الشريحة نجحت في منع كل نوع من اختراق التحكم في التدفق، وهو أحد أكثر الهجمات شيوعا وخطورة.

٢- تقنية البلوكتشين:

هي التقنية التي تضمن صلاحية العملات الرقمية، وبشكل عام يمكن أن تساعد في مكافحة الهجمات الإلكترونية، لأنه لا يمكن تغييرها أو حذفها بمرور الوقت، تعد تقنية البلوكتشين أحد الاحتمالات القابلة للتطبيق للحفاظ على التفاصيل القيمة في مأمن من الإرهابيين، ويتم التحقق من المعلومات وإضافتها بشكل دائم إلى دفتر الأستاذ الرقمي. ولهذا من الصعب التلاعب بالمحتوى، خاصة أنها تعطى الشفافية لجميع الأطراف المعنية.

3- الذكاء الاصطناعي:

جمع باحثو معهد ماساتشوستس للتكنولوجيا بين المعرفة والهيئات الت البشرية وأجهزة الحاسوب في منصة تسمى A12 واختبروها على 3,6مليار قطعة من البيانات، أظهرت النتائج أن النظام توقع أحداث الأمن السيبراني بدقة 85٪، وهو ما يقرب من ثلاث مرات أفضل من السابق. كذلك يقوم الذكاء الاصطناعي بأتمتة عمليات توظيف تحديد الهوية، وتقوم الأساليب القائمة عليه النظام بكفاءة ومقارنة مصادر المعلومات المختلفة لاكتشاف نقاط الضعف، كما يقوم بمنع الهجمات من خلال النظر في الأحداث السابقة (التعلم الآلى). ويمكن استخدام الذكاء الاصطناعي لمحاربة الإرهاب الإلكتروني عن طريق:

أ ــ **مكافحة الفيروسات** : تكتشف برامج مكافحة الفيروسات ذات الذكاء الاصطناعي الشذوذ في الشبكة عن طريق متابعة العمليات التي تتصرف بشكل مريب وتمنعها عند إطلاقها.

ب ــ **نمذجة سلوك المستخدم** : يقيم الذكاء الاصطناعي سلوك مستخدمي الشبكة لتقييم كيفية تفاعلهم مع النظام واكتشاف محاولات الإطاحة به، ويمكن له كذلك تحديد الأنشطة المشبوهة والاستجابة عن طريق تعطيل المستخدم أو عن طريق إخطار مسئولي النظام.

ج ــ **التحليل الآلى للشبكة والنظام** : يضمن التحليل الآلى لمعلومات الشبكة التقييم المستمر والكشف المبكر للهجمات الإلكترونية المشتبه بها.

4- استخدام منصات متعددة الكيانات للكشف والاستجابة:

من الحقائق الصعبة للأمن السيبراني أن المخاطر يمكن أن تأتي من مصادر متعددة، لذلك يستلزم نهج واحد للأمن السيبراني البحث عن أنواع عديدة من التهديدات والحماية ضدها جميعا. وهذا مثل ما أطلقته شركة تسمى Mistnet منتجا وهو عبارة عن أداة لنظام للكشف والاستجابة متعدد الكيانات، وتوفر هذه الأداة منعا في الوقت الفعلي للتهديدات وتوفر الرؤية المرتبطة بالمستخدمين أو الشبكات أو المضيفين. فهي تجمع بين الحوسبة المتطورة وتحليلات الذكاء الاصطناعي للعثور على التهديدات في أقل من ساعة.

5- الأدوات التقدمية لتحديد التهديد:

هناك عدة أنواع من التقنيات يمكن استخدامها كجزء من خطة شاملة ضد التهديدات الإلكترونية، وهي تشمل تقنيات الخداع الدفاعي، التي تحدد الهجمات في وقت مبكر وتنقل البيانات المهمة قبل الوصول إليها أو إتلافها. ويساعد استخدام الشراك الخداعية، فضلا عن جدران الحماية لتطبيقات الويب، ونظام منع الاختراق IPS، وحلول الخداع المستندة إلى الويب، في حماية البيانات من الهجمات.

ثالثاً : أبرز جهود المنظمات الدولية والإقليمية في مواجهة الإرهاب الإلكتروني

الإرهاب الإلكتروني إحدى الجرائم الدولية التي تتطلب الاهتمام والتعاون من قبل المنظمات الدولية والإقليمية لمكافحته، لذلك تعمل الدول على استخدام استراتيجيات تغطى تدابير الأمن الإلكتروني بما في ذلك الدفاع والردع الإلكتروني ، وعلى مدى خمسة عشر عاما أو أكثر بذلت المنظمات الدولية والإقليمية جهودا حثيثة للتصدي للإرهاب بمختلف أشكاله وصوره، ولعل أبرز تلك المنظمات التي يمكن أن نركز عليها ما يلي:

1- الأمم المتحدة والكيانات المرتبطة بها

يضع ميثاق الأمم المتحدة صون السلم والأمن الدوليين هدفا رئيساً للمنظمة، ويلزم الدول باتخاذ التدابير الجماعية المناسبة لمنع كل ما يهدد السلام من جانب وتعزيز حقوق الإنسان والتنمية بكل أبعادها من جانب آخر، ولأن الإرهاب بكل أشكاله التقليدية السيبراني والإلكترونية يمثل أحد أخطر مهددات السلم والأمن، فقد اتخذت الأمم المتحدة والكيانات المرتبطة بها مجموعة من التدابير لمكافحة الإرهاب، أبرزها:

أ ــ إستراتيجية مكافحة الإرهاب: تعد هذه الإستراتيجية التي اعتمدت بتوافق الآراء في عام ٢٠٠٦ أداة عالمية لتعزيز الجهود الوطنية، والإقليمية، والدولية لمكافحة الإرهاب، وقد اتفقت من خلالها جميع الدول الأعضاء في الأمم المتحدة لأول مرة على نهج إستراتيجي وتنفيذي مشترك لمكافحة الإرهاب، وترتكز الإستراتيجية على ركائز أساسية هي[19]:

1ـ معالجة الظروف المؤدية إلى انتشار الإرهاب وتدابير لمنعه ومكافحته.
2ـ تدابير لبناء قدرة الدول على منع الإرهاب ومكافحته .
3ـ تعزيز دور منظمة الأمم المتحدة في هذا الشأن.
4 ـ اتخاذ تدابير لضمان احترام حقوق الإنسان وسيادة القانون بوصفه الأساس لمكافحة الإرهاب.

وقد يبدو من ركائز هذه الإستراتيجية أن الإرهاب الإلكتروني قد تم دمجه ضمن المفهوم الواسع للإرهاب دون إشارة صريحة إليه، ولكن المراجعة الدورية للإستراتيجية، والتي تتم كل عامين، أسفرت في نسختها السادسة الصادرة في حزيران ٢٠١٨ عن إلقاء مزيد من الضوء على قلق الدول الأعضاء من تزايد استخدام الإرهابيين لتكنولوجيا المعلومات والاتصالات في ارتكاب الأعمال الإرهابية، أو التحريض عليها، أو التجنيد لها، أو تمويلها، أو التخطيط لها، الأمر الذي دفع مكتب الأمم المتحدة لمكافحة الإرهاب لاتخاذ عدة مبادرات في مجال التكنولوجيات الجديدة من أجل تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع إساءة استعمال الإرهابيين والمتطرفين للتطورات التكنولوجية .

ب ــ مجلس الأمن: فرض مجلس الأمن مجموعة من التدابير على الدول بهدف التضييق على الإرهاب الإلكتروني بموجب القرار ٢١٦١ لسنة ٢٠١٤ بشأن إنشاء لجان للعمل على الوقاية من التطرف وتقليص أثره على المجتمعات. وتبع هذا القرار مجموعة من المبادئ التوجيهية التي نصت عليها وثيقة مجلس الأمن رقم 939 لسنة ٢٠١٥، وسميت بمبادئ مدريد التوجيهية لوقف تدفق المقاتلين الإرهابيين الأجانب. وتضمنت

مواجهة الإرهاب الإلكتروني في البند السادس والعشرين الذي نص على : (أن تضطلع الدول الأعضاء ببناء القدرات وتكوين الخبرات في مجالي تكنولوجيا المعلومات أو نطاقها والاتصالات وعلم الأدلة الجنائية داخل الأجهزة الوطنية لإنفاذ القوانين وأن تعزز قدرتها على رصد محتوى وسائل التواصل الاجتماعي ذي الصلة بالإرهاب من أجل منع تدفق المقاتلين الإرهابيين الأجانب)[20].

ج ــ الاتحاد الدولي للاتصالات: وهي كالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات، وكانت مهمتها الرئيسة تتعلق بالاتصالات السلكية واللاسلكية، ويضطلع الاتحاد منذ القمة العالمية لمجتمع المعلومات التي عقدت عام ٢٠١٠ بدور أساسي يتمثل في بناء الثقة والأمن فيما يتعلق باستعمال تكنولوجيا المعلومات والاتصالات، وقد عنى الاتحاد بالتعاون مع مكتب الأمم المتحدة لمكافحة الإرهاب بوضع سياسات الأمن السيبراني، وتحفيز, الدول على التعاون من أجل بناء الثقة، ورفع درجة الحماية من الإرهاب الإلكتروني. ولعب الاتحاد دورا بارزا في السنوات الأخيرة في بناء قدرات الدول والمنظمات الإقليمية في مجال مكافحة الإرهاب الإلكتروني، إذ أطلق برنامج الأمن السيبراني العالمي كإطار للتعاون الدولي لتعزيز الثقة والأمن في مجتمع المعلومات منذ ٢٠٠٧ بالتعاون مع هيئة الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبرانى[21].

2 ــ الاتحاد الأوروبي

شهد التعاون الأوروبي في مكافحة الإرهاب تقدما ملحوظا على مدى العقدين الماضيين، الأمر الذي أدى إلى تعزيز قدرة الدول الأعضاء على حماية أمن وسلامة مواطنيها. وقد ساعدت قواعد بيانات الاتحاد الأوروبي في تدعيم التعاون الشرطي والقضائى بين دول الاتحاد، والربط بين النقاط الحدودية بشكل يحرم الإرهابيين من السفر لأغراض إرهابية. وفي تموز ٢٠٢٠، توجت جهود التعاون بين دول الاتحاد باعتماد المفوضية الأوروبية إستراتيجية جديدة للاتحاد الأمني للاتحاد الأوروبي للحقبة من ٢٠٢٠ إلى ٢٠٢٥ تسمح بمنع واكتشاف التهديدات وزيادة مرونة البنية التحتية الحيوية لتعزيز الأمن السيبراني وتعزيز البحث والابتكار. ودخلت الإستراتيجية الجديدة حيز التنفيذ في نيسان ٢٠٢١، بعد تبنى في البرلمان الأوروبي حزمة من القيود المشددة التي تفرض إزالة الرسائل والصور ومقاطع الفيديو ذات الطابع الإرهابي خلال ساعة من المنصات الإلكترونية بهدف منع الإرهابيين من استخدام الإنترنت للتطرف والتجنيد والتحريض على العنف، كما شجعت المفوضية التوقيع على مدونة الاتحاد الأوروبي لقواعد السلوك بشأن مكافحة خطاب الكراهية عبر الإنترنت عام ٢٠١٦، فضلا عن تقديم مبادرة لتوسيع قائمة الجرائم على مستوى الاتحاد الأوروبي لتشمل جرائم الكراهية[22].

3ــ الاتحاد الإفريقي

على الرغم من اعتماد الاتحاد الإفريقي لاتفاقيته بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي في ٢٠١٤، إلا أن الاتفاقية لم تدخل حيز التنفيذ إلى الآن بسبب عدم وصول عدد الدول الموقعة عليها للعدد المطلوب، إذ تحتاج الاتفاقية لتوقيع عشر دول إضافية بعد توقيع 19 دولة فقط من أصل 54

دولة وقد يرجع ضعف إقبال الدول الإفريقية على توقيع هذه الاتفاقية إلى عدم الشعور بخطورة الجرائم الإلكترونية في ظل ضعف استخدام الإنترنت في إفريقيا، إذ لم تتجاوز نسبة سكان القارة الإفريقية الذين يستخدمون الإنترنت ٢٨٪ بنهاية ٢٠١٩[23].

4- جامعة الدول العربية

اعتمدت جامعة الدول العربية عددا من الاتفاقيات لمكافحة الإرهاب بشكل عام منذ ١٩٩٨، والإرهاب الإلكتروني بشكل خاص الخصوص منذ ٢٠١٠، وبالرغم من اعتماد الإستراتيجية العربية لمكافحة الاتفاقية عام 1997، إلا أن التركيز على الإرهاب الإلكتروني بدا جليا في المراجعة السادسة لها بين عامى ٢٠١٣-٢٠١٥، إذ اتفقت الدول العربية على تفعيل دور الرقابة على وسائل الإعلام وعلى شبكة الإنترنت من قبل المكتب العربي للإعلام الأمني، وبذل جهود مكثفة لمنع استغلال مواقع التواصل الاجتماعي من قبل الإرهابيين، وسن التشريعات الخاصة بجرائم تقنية المعلومات عند الدول التي لا تمتلك مثل هذا التشريع، ولم تقتصر الجهود العربية في مكافحة الإرهاب الإلكتروني على اتفاقية مكافحة جرائم تقنية المعلومات، وإنما امتدت إلى إنشاء المركز الإقليمي للأمن الإلكتروني للمنطقة العربية الذي أنشئ بموجب الاتفاق مع الاتحاد الدولي للاتصالات في كانون الأول ٢٠١٢، ويتبنى المركز الأجندة العالمية للأمن الإلكتروني التي تنظم التعاملات الإلكترونية وتجرم الاستخدام غير المشروع للتكنولوجيا، وتهدف إلى تدريب وتأهيل وتنمية القدرات وتطويرها في مجال الأمن الإلكتروني[24] .

يتضح مما سبق أن الأمم المتحدة ووكالاتها المتخصصة المختلفة فضلا عن بعض المنظمات الإقليمية ترعى جهود أبرز القد المجتمع الدولي في وضع قانونية وتشريعية ذات صبغة عالمية لمنع الأعمال الإرهابية، ولكن إلى الآن لا توجد اتفاقية شاملة للأمم المتحدة بشأن الإرهاب تضم قائمة شاملة لكل أشكال الإرهاب بما فيها الإرهاب الإلكتروني، ولا تخضع الاتفاقيات القائمة الجرائم الإرهابية للقانون الدولي، وإنما تلزم الدول الأطراف في الاتفاقيات بتجريم الفعل المخالف في إطار قانونها الداخلي وتفتح المجال أمام التعاون الدولي بشكل يمكن الدول الأطراف من محاكمة المتهمين أو تسليمهم.

الخاتمة

لم تستخدم العناصر المتطرفة أحدث التكنولوجيا المتاحة دوما، ولكنها قامت بتكييف التكتولوجيا المتاحة للاستخدام الطبيعي بطرق غير تقليدية وغير متوقعة، ومن أجل توقع الهجمات المستقبلية، على رجال إنفاذ القانون التفكير في الكيفية التي يمكن من خلالها استخدام التكنولوجيا القائمة بطرق مختلفة عن استخداماتها المفترضة، والتحدي في التعلم من حقائق تطور علاقة التنظيمات المتطرفة والإرهابية بالتكنولوجيا، وفقا لمفهوم أكثر اتساعا لا يبدأ من ربط درجة التطور التقني بالاستهداف من قبل التنظيمات الإرهابية، ولكن من سؤال كيف يمكن توظيف هذا الغرض أو الأداة من أجل تحقيق أهداف تلك التنظيمات؟، وهو ما يحتاج إلى تجاوز حالة فشل الخيال أو عدم قدرة أجهزة إنفاذ القانون على إدراك تلك الحقائق كما في أحداث 11 سبتمبر وغيرها من العمليات الإرهابية التي تحولت فيها الأدوات العادية إلى قنبلة قاتلة أو وسيلة حشد وتعبئة مؤثرة.

ومن أجل المساعدة، وضع بعض الكتاب تصورات عن الاحتياجات التي تبحث عنها العناصر الإرهابية في الأدوات أو والتقنيات التي تتحول إلى أسلحة من أجل بناء تصورات والتنبؤ بما يمكن استخدامه ، ومن ضمن المميزات المطلوبة : سهولة الوصول والاستخدام، وانخفاض التكلفة، والقابلية للنقل، وإمكانية الإخفاء والفاعلية، وأن تكون الأسلحة مفيدة في سياقات متعددة، وأن تكون جزءا من تقنيات يمكن تضخيم آثارها، ولها صدى رمزى، ويكون لها استخدامات غير متوقعة ، ويمكن لأسلحة بمثل تلك المواصفات تمكين الأفراد والجماعات الصغيرة، ليس لأنها أكثر تفوقا عن التكنولوجيا الحديثة التي تملكها الدول، ولكن بسبب قدرتها على تجميع الأفراد، وتوسيع قدرة الوصول، التنظيم وتوفير إمكانيات القيادة والسيطرة. ومن خلال تلك الأفكار يمكن التركيز على كيفية استخدام التنظيمات الإرهابية للتكنولوجيا والجهود اللازمة في مجال الوقاية والمكافحة.

بدورها، ترتبط التكنولوجيا بالرغبة في تحقيق الأرباح، وهو ما يشير إلى استمرار جهود التطوير وفرص استغلال الإمكانيات في تكنولوجيا الإنترنت والذكاء الاصطناعي وغيرها من الأدوات التي تثير المخاوف في حالة استخدامها من قبل التنظيمات الإرهابية. ولهذا يتكرر الحديث عن ضرورة محاسبة الشركات والإنترت وعدها مسؤولة عن إخطار الجمهور بالمخاطر المرتبطة ببعض التقنيات، ووضع قواعد منظمة فيما يتعلق بمحاربة المحتوى الإرهابي والخطاب العنيف والعنصري، وتقييد فرص الوصول والتجنيد والتمويل، مع بذل المزيد من الجهد للكشف عن التنظيمات الإرهابية من قبل شركات التكنولوجيا.

ومع أهمية الذكاء الاصطناعي، والتكنولوجيا، والإنترنت، تظل المساحة مفتوحة للمنافسة بين جهود استخدام التكنولوجيا في سبيل العنف والإرهاب، وجهود تقليص فرص مثل هذا الاستخدام، وزيادة الإيجابيات المرتبطة باستخدام التكنولوجيا ما بين التقييد والمنع، والاستخدام والمواجهة، وإحلال السلام، إذ تدور معركة التكنولوجيا والإنترنت في قلبها من أجل منع الحرب المروعة التي يدفع إليها الإرهاب وتنظيماته.

المصادر

(1) إسحاف كافير ، دور التكنولوجيا في تمكين الإرهابيين وتطورهم، موقع عين أوروبية على التطرف ، 15أيلول 2021.

(2) T.X. Hammed (terror and technology from dynamite to drones September 4,2020 Texas National Security Review ،Book Review

(3) المصدر السابق.

(4) – أنتوني وود ، "رسالة مفتوحة تلتمس من الأمم المتحدة حظر التطورات المتعلقة بالجماعة آلمسلحة " ، نيو أطلس ، 27 أيلول2015.

(5) سعود الشرفات ،نجاح الجماعات الإرهابية في تبني واستخدام التكنولوجيا المتطورة ،على الرابط : www.mominoun.com

(6) سارة سمير،الذكاء الاصطناعي هل سينقذ العالم أم سيدمر الإنسان؟ ، صحيفة الرؤيا ، 22 شباط 2021، www.alroya.com

(7) ريتشارد غراي، كيف يساعدنا الذكاء الأصطناعي في مكافحة الأمراض والتصدي للعنف، 21أيلول 2017، على الرابط : www.bbc.com

(8) المصدر السابق.

(9) محمد الغباري ، قراءة في مفهوم الجيل الرابع من الحروب، السياسة الدولية، مركز الأهرام ، القاهرة ، 2019، ص244.

(10)مكافحة الإرهاب ..الذكاء الأصطناعي وكشف التهديدات الإرهابية، المرصد الأوروبي لمحاربة التطرف، 5تموز2020.

(11)أستخدام الأنترنت في أغراض إرهابية، مكتب الأمم المتحدة المعنى بالمخدرات والجريمة ، فيينا ،تموز 2021،ص37.

(12)عمرو عبد العاطى ، الثورة التكنولوجيا ومستقبل الحروب ،السياسة الدولية ،تحولات إستراتيجية ،مركز الأهرام ، العدد228،أبريل 2022.

(13)كريستين لاغارد ،العمل معاً لمكافحة غسل الأموال وتمويل الإرهاب،الاجتماع العام لمجموعة العمل المالي، صندوق النقد الدولي،2017 ،على الرابط: www.imf.org

(14)أستخدام الإرهاب .الذكاء الأصطناعي وكشف التهديدات الإرهابية، مصدر سبق ذكره.

(15)شبكة إنفاذ الجرائم المالية ، إتجاهات برامج الفدية في بيانات قانون السرية المصرفية ، وزارة الخزانة الأمريكية، الشؤون المالية،على الرابط www.state.gov

(16)عمرو عبد العاطي، الثورة التكنولوجية ومستقبل الحروب،مصدر سبق ذكره.

(17)كريستين لاغارد، العمل معاً لمكافحة غسل الأموال وتمويل الإرهاب، مصدر سبق ذكره.

(18)الأرهاب..الأساليب والدوافع والأموال..الردع والكشف والتعطيل ،www.interpol.int.

(19)محمد أحمد مرسي، المؤسسة الدولية والتعاون في مجال القضاء على التطرف والإرهاب، السياسة الدولية،مركز الأهرام،العدد226، القاهرة،اكتوبر 2021.

(20) الأمم المتحدة مكتب مكافحة الإرهاب، وثائق الجمعية العامة ومجلس الأمن الرئيسية،على الرابط:www.un.org.

(21)مجلس الأمن ،مبادئ مدريد التوجيهية لوقف تدفق المقاتلين الإرهابيين الأجانب،23ديسمبر2021، على الرابط:www.undocs.org.

(22)إستراتيجيات وتشريعات مكافحة الإرهاب داخل الاتحاد الاوروبي ، المركز الأوروبي لدراسات مكافحة الإرهاب والأستخبارات، اكتوبر2021.

(23)تقرير للإنتربول يحذر من أن الجريمة الإلكترونية في إفريقيا تشكل اشد خطرا من أي وقت مضى، موقع الإنتربول14أغسطس،2020، على الرابط: www.interpoi.int.

(24) جامعة الدول العربية ، أثر الإرهاب على الأمن السلم العالمي،مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال افريقيا في 28-29 تشرين الثاني 2017،www.unodc.org