آليات مواجهة الذكاء الاصطناعي المرتبط بالإرهاب/ الإرهاب الإلكتروني أنموذجًا

أ.م.د. سيف حيدر الحسيني

كلية العلوم السياسية/ جامعة الكوفة

تشكل التحدي الرقمي تحديًا كبيرًا للدول ولصانعي السياسات العامة من الناحية الأمنية، إذ يعدّ الذكاء الاصطناعي بوصفه واحدًا من منتجات ذلك التحول من أهم التحديات حديثًا، إذ إن هذا البعد يشكل تهديدًا خطيرًا للأمن القومي للدول، فبإمكان الجماعات الإرهابية توظيف هذا البعد لضرب أمن الدول، وتهديد حياة مجتمعاتها، وبذلك فالقيام بالعمليات الإرهابية بهذا الشكل يعدّ تحولًا خطيرًا وتحديًا كبيرًا للدول والمؤسسات الأمنية، فاستخدام الذكاء الاصطناعي سهّل كثيرًا للجماعات الإرهابية القيام بأعمالها، وبذلك انتقل الصراع من وصفه واقعيًا إلى صراع افتراضي، وهذا الأمر يضع على الدول مسؤوليات كبيرة جدًا تتمثل بضرورة مواكبة التطور التكنولوجي عبر إيجاد كفاءات إدارية وأمنية وعسكرية تأخذ على عاتقها مواجهة هذا التحدي، فضلًا عن الانتباه إلى البعد الدولي من خلال عقد شراكات إقليمية ودولية مع الدول المتقدمة بهذا المجال لإيجاد صيغ حديثة من شأنها تقويض هذا النوع من الإرهاب.

الكلمات المفتاحية: الذكاء الاصطناعي، الإرهاب، الإرهاب الإلكتروني، الأمن السيبراني.

Mechanisms to Confront Artificial Intelligence Linked to Terrorism: Cyber Terrorism as a Model

Asst. Prof. Dr. Saif Hayder Al-housaniy

College of Political Science/University of Kufa

The digital challenge has posed a major challenge to countries and public policy makers from a security standpoint. Artificial intelligence is one of the products of that transformation as it is considered one of the most important recent challenges, as this dimension constitutes a serious threat to the national security of countries. Terrorist groups can exploit this dimension to attack the security of countries and threaten the lives of their societies. Thus, carrying out terrorist operations in this manner is a dangerous transformation and a major challenge to countries and security institutions. The use of artificial intelligence has made it much easier for terrorist groups to carry out their work, and thus the conflict has moved from being realistic to a virtual conflict. This places on countries very great responsibilities represented by the need to keep pace with technological development by creating administrative, security and military competencies that will take it upon themselves to confront this challenge, as well as paying attention to the international dimension by concluding regional and international partnerships with developed countries in this field to find modern formulas that would undermine this type of terrorism.

Keywords: artificial intelligence, terrorism, electronic terrorism, cyber security.

الاستلام	الإرجاع	القبول
2025/8/22	2025/9/2	2025/9/11

المقدمة

إن التطور التقني الحديث وخاصة فيما يتعلق بمجال الذكاء الاصطناعي قد أسهم في تحقيق طفرة نوعية في أنماط الحياة المختلفة وفي المجالات كافة، فقد انبرت أغلب الدول المتقدمة والحكومات عبر مؤسساتها إلى توظيف الذكاء الاصطناعي لتقديم أفضل الخدمات وبسهولة فائقة، إلا أن هذا التقدم التكنولوجي له آثاره السلبية أيضا، وتتمظهر تلك الآثار على الصعيدين الأمني والاجتماعي والبنى التحتية، لا سيما فيما يتعلق بتوظيف الجماعات الإرهابية للذكاء الاصطناعي، وشكّل هذا التوظيف تحديا جديدا للدول للحفاظ على أمنها ونسيجها الاجتماعي، إذ عمدت بعض الجماعات الإرهابية إلى استخدام آليات جديدة لضرب الاستقرار الأمني والاجتماعي، وهذا الأمر يتطلب من الدول المؤسساتية تطوير منظومتها الأمنية تقنيا تماشيا مع التطور التكنولوجي، وذلك عبر فتح مسارات محلية ودولية تتعلق بالتدريب من أجل الوقاية والحماية من الهجمات الإرهابية الإلكترونية، إذ إن توفر بعض الأدوات الإلكترونية من شأنه أن يوجد قنوات عديدة لتنفيذ تلك الهجمات.

إزاء تلك التحديات الأمنية الخطيرة الخاصة بتوظيف الذكاء الاصطناعي من الجماعات الإرهابية للقيام بأعمال إرهابية أو التحريض على نشر ثقافة التطرف العنيف المؤدي إلى الإرهاب، لا بد من تشخيص هذه الأدوات، وإيجاد استراتيجيات وسياسات عامة واقعية تتضمن آليات واقعية من الممكن تطبيقها لمواجهة تلك الجماعات وهجماتها الإرهابية الإلكترونية.

إشكالية البحث

تتمثل إشكالية البحث في السؤال الرئيس الآتي:

ما آليات مواجهة الذكاء الاصطناعي بمختلف أنواعه المرتبط بالإرهاب؟

وثمة إشكالات فرعية تنطلق من السؤال الرئيس تتمثل بالآتي:

1. ما الذكاء الاصطناعي والإرهاب والإرهاب الإلكتروني؟
2. ما استخدامات الجماعات الإرهابية المرتبطة بالذكاء الاصطناعي؟
3. هل هناك آليات وخطط واقعية لمواجهة هذا التهديد؟

أهمية البحث

تنطلق الأهمية العلمية من كون أن ظاهرة الذكاء الاصطناعي أصبحت من أهم الظواهر في العصر الحالي، فضلاً عن خطورة توظيف هذه الظاهرة من الجماعات الإرهابية في القضايا الأمنية، التي تمس سلامة الدولة وتهدد مؤسساتها، يضاف لذلك تأثيرها في البعد الاجتماعي، ومحاولة تهديم النسيج الاجتماعي من خلال تبني وإثارة الفتن والنعرات الطائفية والقومية عبر تبني هجمات إلكترونية ذكية.

هدف البحث

يهدف البحث إلى ضرورة تنبيه صانع القرار والفاعليين الأمنيين والاجتماعيين على ضرورة التركيز على هذا التهديد الخطير للأمن القومي للدولة عبر تبني آليات واستراتيجيات من شأنها تدارك توظيف الذكاء الاصطناعي بمختلف أنواعه من أجل شن هجمات إرهابية إلكترونية.

فرضية البحث

ينطلق البحث من فرضية مفادها أن التطور التكنولوجي، وخاصة فيما يتعلق بالذكاء الاصطناعي وعملية توظيفه من الجماعات الإرهابية يشكّل تهديدا خطيرا على الأمن الإنساني، وإزاء ذلك التهديد لا بد للدول وصناع القرار من تبني آليات من أجل المواجهة، ومرتبطة بالمداخل السياسية، والأمنية، والاجتماعية، والثقافية، فضلاً عن التأكيد على أهمية الشراكات الدولية مع القطاعات ذات الاهتمام بهذا المجال.

منهجية البحث

لإثبات فرضية البحث، تم اعتماد منهج التحليل النظمي والمنهج الوصفي من أجل الوصل إلى نتائج علمية وموضوعية.

المحور الأول: الذكاء الاصطناعي والإرهاب الالكتروني (التأصيل النظري)

إن المتتبع لموضوع الذكاء الاصطناعي والإرهاب الإلكتروني يدرك تماما بعدم وجود تعريف جامع ومانع لهما، إذ إن التعريفات غالبا ما ترتبط بالمدارس الفكرية والتوجهات القيمية للمنظرين لها، ومن هنا منهجيا لا بد من إدراج بعض التعريفات العلمية الرصينة لهذين المفهومين كتأصيل نظري يسهل على الباحث إدراك المعنى لهذين المصطلحين، كما يعد الذكاء الاصطناعي تقنية سريعة التطور، ويمكن استخدامها لإنشاء هجمات إرهابية إلكترونية أكثر تعقيدا وقوة من الهجمات

التقليدية، مما يجعل من الصعب اكتشافها والتصدي لها، إذ يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل، فضلاً عن استهداف المؤسسات الأمنية والعسكرية.

المطلب الأول: الذكاء الاصطناعي

أولًا: ماهية الذكاء الاصطناعي

يعد الذكاء الاصطناعي الذي يعرف اختصارا (AI) نوعا جديدا من التفكير، إذ يعتمد على إشغال العقل الإلكتروني، وتفعيل قراراته بما يحاكي العقل البشري في تحديد أهداف وترتيب الأولويات، ووضع بدائل، واتخاذ قرارات، وذلك بوساطة خوارزميات تقوم بإنشائها الحواسيب الآلية وليس البشر.

يعرف الذكاء الاصطناعي بأنه "النشاط الذي يهدف إلى جعل الأجهزة ذكية، والذكاء يعني الجودة التي تمكن الكيان من العمل بشكل مناسب وبحكمة من خلال النظر إلى العواقب في بيئتها" [1].

وتم تعريفه على أنه "جزء من علم الحاسب الآلي الذي يهتم بأنظمة الحاسوب الذكية التي ترتبط خصائص مرتبطة بالذكاء، واتخاذ القرارات، وحل المشكلات، والتعلم والتفكير المشابهة لدرجة ما للسلوك البشري"[2].

وبالتالي فهو "فرع من فروع علم الحاسوب وهو عبارة عن سلوك وخصائص معينة تتبعها البرامج الحاسوبية، بحيث تصبح قادرة على محاكاة القدرات الذهنية الخاصة بالبشر في أنماط عملها المختلفة، ومن أهم هذه القدرات هي قدرة الآلة على التعلم، والاستنتاج، واتخاذ القرارات بالإضافة إلى القيام بالعديد من ردود الأفعال"[3].

وهناك تعريفات قانونية منها هو "مجموع الحلول التكنولوجية التي تسمح بتقليد الوظائف المعرفة للشخص، بما في ذلك التدريب الذاتي، وإيجاد خوارزميات محددة مسبقا، وتلقي النتائج القابلة للمقارنة على الأقل لنتائج الأنشطة الفكرية للشخص في حالة تحقق أهداف محددة"[4].

فيما يعرفه الباحث بأنه "عمليات حسابية رقمية تخضع لخوارزميات دقيقة تنتج قرارات تقترب من أو تشبه الذكاء البشري فيما يتعلق بالفعل أو رد الفعل إزاء مواقف معينة".

ثانياً: أنواع الذكاء الاصطناعي [5]

1. الذكاء الضعيف: يعد هذا النوع من الذكاء الاصطناعي مخصصا لأداء مهمة محدودة وبشكل متقن، على سبيل المثال نظام التوصيات على منصات البث الإلكتروني.
2. الذكاء القوي: يمثل هذا النوع من الذكاء الاصطناعي هدفاً يتمثل في إنشاء أنظمة قادرة على أداء مهام ذكية متنوعة بشكل مماثل للبشر، ويمثل هذا النوع من الذكاء كحد كبير في مجال البحث والتطوير، الذي بدأ اليوم يأخذ حيزا مهما لدى الباحثين والعلماء في مجال تطور العلوم.
3. الذكاء الاصطناعي المعزز: ويشير هذا النوع إلى التركيز على فكرة دمج القرارات البشرية مع التقنيات الذكية، ويحسن ويعزز قرارات الأفراد وأداء أفضل للمهام.
4. الذكاء الاصطناعي التفاعلي: يرتبط هذا النوع بالقدرة على التفاعل مع البشر والأنظمة البشرية بشكل طبيعي، ويعد هذا النوع من الذكاء هو الأكثر شيوعا لدى مستخدمي التقنيات الإلكترونية، وهذا الأمر مرتبط بطبيعة الاستخدامات الناشئة من المستفيدين، وإمكانية التفاعل ما بين الآلة والبشر وكذلك بين البشر أنفسهم.

ثالثاً: استخدامات الذكاء الاصطناعي

1. التنبؤ: واحدة من أهم مميزات الذكاء الاصطناعي هي إمكانية التنبؤ والتحديد المكاني والزماني للمستخدمين، وبالتالي يمكن توظيف هذا الاستخدام من المستخدمين سواء أكانوا مؤسسات رسمية أم أفرادا مدنيين أم جماعات إرهابية، فيمكن من خلال تطبيقات الذكاء الاصطناعي تصنيف المستخدمين سواء أكانوا مستهدفين من الجماعات الإرهابية أم يمكن للجهات الرسمية تصنيف الجماعات الإرهابية وتحديد أماكن تواجدهم وملاحقتهم[6].
2. تحليل البيانات والمعلومات: واحدة من أهم استخدامات الذكاء الاصطناعي هي إمكانية جمع البيانات، وتحليلها ومقاطعتها، وبذلك فإن هذه الميزة من الممكن أن يتم توظيفها لجمع البيانات ومقاطعتها بيانيا بشأن الأهداف التي من المحتمل استهدافها من الجماعات الإرهابية سواء كانت هذه الأهداف بشرية أم مادية، فضلاً عن إمكانية

استخدامها من الحكومات لتحليل السلوك البشري للجماعات المتطرفة، وتحليل فيما إذا كان في النية القيام بأي أعمال إرهابية مستقبلاً [7].

3. الاستجابة: تطورت تقنيات الذكاء الاصطناعي للاستجابة للتهديدات الإلكترونية الإرهابية بشكل كبير، إذ تتيح هذه التقنيات للدول والمؤسسات القيام باستخدام الذكاء الاصطناعي باستمرار من أجل اكتشاف الهجمات والتصدي لها في الوقت ذاته، ويمكن أيضا استخدام الذكاء الاصطناعي في أتمتة إنشاء رقعة افتراضية للتهديدات المكتشفة، فضلاً عن تطوير أدوات حماية جديدة، ويعمل الذكاء الاصطناعي أيضا على مساعدة الدول والمؤسسات العالمية على خفض التكلفة، وتوفير الوقت من أجل الاستجابة للتهديدات، ومواجهة الانتهاكات، بغض النظر عن شكل الأشكال والخصائص المحددة التي تستعمل فيها [8].

المطلب الثاني: مفهوم الارهاب والارهاب الالكتروني

يعد (Watson) أكثر الذين عرفوا الإرهاب بصورة دقيقة، إذ عرفه بأنه: "استراتيجية أو أسلوب يعتمد على الاستعمال المنظم للعنف في محاولة جماعية منظمة من أجل لفت الانتباه لأهدافها عن طريق فرض التنازلات لأغراضها"[9].

ويعرف (Thornton) الإرهاب بأنه "فعل رمزي يرمي إلى إحداث تأثير بوسائل غير عادية إما باستعمال العنف أو التهديد"[10].

كما توصل (جولي تلورج) في كتابه (A Challenge to the State terrors) الصادر عن جامعة أكسفورد عام 1982 إلى تعريف الإرهاب بأنه "التهديد أو استخدام العنف السياسي عندما يهدف هذا العمل إلى التأثير في موقف أو سلوك مجموعة أوسع من الضحايا المباشرين، أو عندما تتعدى عواقبه الحدود الوطنية"[11].

وتعد محاولة (Schmid) صاحب كتاب (الإرهاب السياسي) من أهم المحاولات التي جرت لوضع تعريف شامل لمصطلح (الإرهاب) إذ عرفه بأنه "أسلوب من أساليب الصراع الذي تقع فيه الضحايا كهدف عنف فعال، تشترك هذه الضحايا الفعالة في خصائصها مع جماعة أو طبقة أخرى مما تشكل أساسا لانتقائها من أجل التضحية بها،..."[12].

وقد وصف الإرهاب أيضا بأنه: "إثارة العنف والرعب والفزع أو التهديد باستخدام شتى الوسائل التي تتباين وفقاً للمصلحة أو التهديد باستخدام شتى الوسائل التي تتباين وفقاً للمصلحة أو الهدف المراد تحقيقه سياسيا سواء بطريقة الاغتيالات أو بتفجير القنابل في الأماكن العامة، والهجوم المسلح على المنشآت والأفراد، واختطاف الأشخاص، أما معنيين أو مستهدفين من العصابات الإرهابية أو لتحقيق غرض سياسي متخذين من عملية الاختطاف كوسيلة أو كرهائن للوصول إلى مبتغاهم"[13].

أما الإرهاب الالكتروني فيمكن تعريفه على أنه "هو عمل إجرامي والسلاح المستخدم فيه هو وسائل الاتصال والذي ينتج عنه عنف وتدمير أو بث الخوف تجاه المستهدف سواء أكان فردا أم مؤسسة أم دولة والهدف منه التأثير على الحكومات والسكان، وعادة ما يمثل أجندات سياسية أو اجتماعية أو فكرية معينة"[14].

كذلك يعرف الإرهاب بأنه "الاستخدام العدائي غير المشروع للإنترنت بهدف ترويع الحكومة والمدنيين أو قسم منهم في إطار السعي إلى تحقيق أهداف سياسية أو اجتماعية"[15].

وكذلك عرفه بعض فقهاء القانون بأنه "خرق قانون يقدم عليه فرد من الأفراد أو تنظيم جماعي بهدف إلى إثارة أضرار خطيرة في النظام العام عن طريق شبكة المعلومات"[16].

وأيضا عرف بأنه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية أو الوسائل الإلكترونية، بشتى صنوف العدوان".

إذن الإرهاب الإلكتروني يعتمد على استغلال الإمكانات العلمية والتقنية واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الأخرين، وإلحاق الضرر بهم، أو تهديدهم، وبالتالي فإن الإنترنت والإرهاب لهما طريقتان مترابطتان وهما[17]:

أولاً: ممارسة الأعمال التخريبية لشبكات الحاسوب والإنترنت.

ثانيا: إن الإنترنت أصبح منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف.

ومن ذلك فإن الإرهاب الإلكتروني يمثل عملية تحول رقمية من الواقع الفعلي أي الانتقال من تنفيذ الأعمال الإرهابية ميدانيا والتحول بعنصر الجذب من الواقع إلى المواقع الإلكترونية؛ لذا فهو يمثل التحول الفعلي للإرهاب وكما يلي[18]:

أ. بنية هيكل الإرهاب الإلكتروني: يكمن في وجود جماعة منظمة تعمل بشكل منهجي لارتكاب عدد غير محدد من الجرائم، على هذا الأساس يعد الإرهاب الإلكتروني إرهابا من حيث الهيكل لاشتماله على وجود عدد غير محدد من الأعضاء، والوصول إلى الموارد والتمويل، والقدرة على التخطيط المستدام للعمليات وتنفيذها بمرور الوقت، فهي جرائم إلكترونية منظمة، لأن أعضاء الخلية على تواصل وتنسيق مستمر لتنفيذ هجمات إلكترونية محددة ضد مؤسسات الدولة.

ب. مبدأ الضرر: قد لا يهاجم الإرهاب الإلكتروني المصالح الفردية؛ لأن غايته إظهار الوقع الحقيقي في نفوس المواطنين بالعموم واستشعارهم بقوة الكيان الإرهابي، أي زرع الخوف في نفوس أكبر عدد ممكن من الأفراد؛ لذلك يعمل على استهداف جماعي لمصلحة جماعية هجوما مباشرا لمصالح وطنية ومؤسسية للدولة والمجتمع.

ج. العناصر: يتكون هذ الإرهاب من عنصرين إلغائي ووسائلي: إلغائي أي ارتكاب جرائم ذات دوافع سياسية دائما عبر تغيير النظم السياسية، والإطاحة بالحكومات المنتخبة شرعيا، أما الوسائل فهي تنفيذ الأعمال الإرهابية بطريقة مناسبة لغرس الإرهاب في نفوس المواطنين مع استخدام الوسائل المناسبة لترويع وبث الرعب العام عبر استخدام الأدوات الرقمية الفايروسات الدودية والهجمات البرامجية الخبيثة لحجب الخدمات.

مما تقدم يعرف الباحث الإرهاب الإلكتروني على أنه "التوظيف العلمي والعملي للأدوات الرقمية الحديثة من الجماعات المتطرفة بغية التهديد أو إيقاع الضرر القصدي على المؤسسات الرسمية أو الجماعات المدنية".

المحور الثاني: توظيف الذكاء الاصطناعي في العمليات الارهابية

تتعرض الكثير من الدول للعديد من التهديدات الإلكترونية المحتملة، ويمثل التهديد الخطر المحتمل الذي يمكن أن يتعرض له أمن الدولة ومجتمعها بتوظيف البعد الرقمي في تبني هجمات إلكترونية إرهابية، وقد يكون القائم بتلك الأعمال الإجرامية جماعات إرهابية أو قد يكون شخصا كالمتجسس أو المجرم المحترف أو الهاكرز المخترق بهدف إثارة الرعب وخرق الأمن عبر تبني هجمات إرهابية أو أعمال أخرى مثل الحريق، أو قطع التيار الكهربائي، وإزاء تلك التهديدات لا بد من تبني آليات أو استراتيجيات أو سياسات عامة من شأنها أن تواجه تلك التحديات الخطيرة.

المطلب الأول: التهديدات الإلكترونية الذكية المرتبطة بالإرهاب

1. الإنترنت ومواقع التواصل الاجتماعي

ثبتت جدوى الإنترنت منذ أواخر الثمانينيات بوصفها وسيلة اتصال شديدة الحيوية، لها القدرة على الوصول إلى الجمهور في كل أنحاء العالم، واقد أدى استحداث تكنولوجيات تتطور باستمرار كشبات التواصل الاجتماعي (فيسبوك، وتويتر، وإنستكرام، وتيليجرام...إلخ) والمواقع الأخرى (المنتديات الشبكة وتطبيقات الاتصال المشفرة، والمدونات، ومواقع عرض الفيديو كاليوتيوب)، قلّت العوائق أمام الدخول إليها نسبيا، وقد جعلت تكنولوجيا التوسع الإلكتروني من السهل على الفرد أن يتواصل عبر الحدود، بسرعة وفاعلية، ومع إمكانية عدم الكشف عن هويته إلى حد ما، مع عدد يكاد يكون غير محدود من الأشخاص[19]، فقد شهدت السنوات العشر 2006–2016 طفرة هائلة في وسائل التكنولوجيا الحديثة، وعلى رأسها الإنترنت الذي بلغ عدد مستخدميه (3.5) مليار شخص مع نهاية العام 2016، وهو ما يمثل (47%) من إجمالي سكان العالم، وإذا كان (91) بلدا في العالم يزيد عدد السكان الذين يستعملون فيه الإنترنت على (50%)، فإن هذه النسبة تتفاوت في البلدان العربية، التي وصل عدد مستخدمي الإنترنت فيها إلى نحو (226) مليون مستخدم في نهاية العام 2018، ليصبح الإنترنت وما يرتبط به من مواقع التواصل الاجتماعي جزءا أساسيا من الحياة اليومية للفرد، ومثلما استخدمته كبريات الشركات والمؤسسات من أجل عرض منتجاتها والإعلان عن خدماتها، فقد سخَّرته مختلف التنظيمات المتطرفة أيضا لأغراضها الدعائية.

وصارت وسائل التواصل الاجتماعي الوسيلة المستعملة عند تجنيد الفئات المختلفة من أجل الانخراط في الجماعات الإرهابية، وذلك عند مراحل العملية الإرهابية جميعا ابتداء من التخطيط وصولاً إلى التنفيذ، بطرائق وسبل مختلفة، منها تقديم النصائح والإرشادات، ونشر الفكر المتطرف، وتوزيع المهام، وتعليم صناعة العبوات الناسفة والمتفجرات المختلفة.

2. برامج التجسس

ساعد التطور التكنولوجي والطفرات النوعية التي حدثت فيه إلى انتشار ظاهرة البرامج التجسسية، والتي تم توظيفها لتحقيق أغراض سياسية أو اجتماعية أو فكرية أو أمنية وعسكرية، وبالتالي فيمكن توظيفها لإحداث أعمال إرهابية هدفها قد يكون فردي أو جماعي أو مؤسساتي قائم

على فكرة التخريب، إذ من خلالها يتمكن المجرمون من زراعة هذه البرامج بطرائق مختلفة تمكنهم من الوصول إلى المعلومات التي تخص كيان الجماعات والمؤسسات وبالتالي السيطرة عليها والكشف عن الأسرار، التي قد تكون عسكرية أو أمنية أو سرقة ملكات فكرية أو اختراعات[20].

3. تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف والبيانات الإلكترونية والنظم المعلوماتية الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالبا، وهي الأهداف العسكرية، والسياسية، والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها، وعلى رأسها مراكز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية، والمقصود بالتدمير هنا، الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي (PC–Server) أو مجموعة نظم مترابطة بهدف تخريب نقطة الاتصال أو النظام[21].

وإزاء ذلك لا بد من توفير ما يعرف بأمن البنية التحتية، ويتمثل بوصفه إجراء أمنيا يعمل على حماية البنية التحتية الحيوية للدولة، مثل اتصالات الشبكة، أو مركز البيانات، أو الخادم وغيرها من مفاصل تكنولوجيا المعلومات، ويهدف هذا النوع من الأمن إلى الحد من نقاط ضعف الأنظمة السيبرانية وحمايتها من التخريب أو الإرهاب.

4. التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية إلى تدريب خاص، ويعد التدريب من أهم هواجس التنظيمات الإرهابية، وقد أنشأت معسكرات تدريبية سرية، لكن مشكلة معسكرات تدريب الإرهابيين أنها دائما معرضة للخطر، ويمكن اكتشافها ومداهمتها في أي وقت؛ ولذا فإن الشبكة المعلوماتية بما تحويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي، كما قامت بها الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم[22].

5. التهديد الإرهابي الإلكتروني الاقتصادي

يمكن توظيف الذكاء الاصطناعي لتنفيذ جرائم وعمليات إرهابية تتعلق بالبعد الاقتصادي للدول، وذلك من خلال قدرة الجماعات الإرهابية على اختراق النظام المصرفي، وإلحاق الضرر بالبنوك وأسواق المال العالمية، وتعطيل عمليات التحويل المالي، وهذا الأمر ينعكس سلبيا على عدم الاستقرار، مما تنعكس آثاره السلبية على الاستثمار العالمي، فضلاً عن إلحاق الأذى بالاقتصاد الوطني، وقد تستغل الجماعات الإرهابية الذكاء الاصطناعي لتحويل الأموال من أجل تمويل العمليات الإجرامية، فضلاً عن سرقة البيانات الخاصة ببطاقة الائتمان[23].

6. التهديد الإرهابي الإلكتروني الاجتماعي

تمارس الجماعات الإرهابية –عبر توظيف الذكاء الاصطناعي– بعض الأدوار التي من شأنها ترويع المواطنين المدنيين، وإثارة الرعب والخوف فيهم، وهذا الأمر يعد واحدا من أساليب الحرب النفسية، وهي بذلك تستغل البعد الإلكتروني من خلال إنتاج بعض المواد الفلمية المصورة، ونشرها على الإعلام أو مواقع التواصل الاجتماعي، ما يؤثر في المدنيين، فضلاً عن ذلك قد تتبنى الجماعات الإرهابية أدوارا تتعلق باختراق الأنظمة الخاصة بالأدوية أو مصانع الغذاء الخاصة بالأطفال، وتعمد على تغيير النسب العلمية للأدوية أو الغذاء مما يؤدي ذلك إلى قتل العديد من المواطنين، مع إمكانية استغلال ضرب القطاع الخاص بتزويد بالمياه أو الطاقة الكهربائية.

7. هجمات اختراق التحكم في الطائرات المسيرة

أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها، فضلاً عن توظيفها لشن هجمات إرهابية، فهي وبمساعدة الذكاء الاصطناعي تتمكن من اختراق الأجواء، وتنفيذ الهدف بدقة عالية جدا، وبذلك أصبحت واحدة من أدوات الحروب والهجمات الإجرامية الحديثة[24].

• العمليات التخريبية التي أصابت بعض المواقع الحكومية • تزايد صناعة الجريمة السيبرانية • الممارسات الاحتيالية • وقوع الاستغلال عبر الإنترنت من شريحة الشباب من السكان • إساءة استخدام وسائل الإعلام ومواقع التواصل الاجتماعي لشن حملات خبيثة ضد الدولة • الصراع والعنف المستمر من خلال الإنترنت • التخريب الاقتصادي من خلال حرمان المواطنين من الوصول إلى الخدمات الإلكترونية الحكومية وغير الحكومية	• التجسس الإلكتروني المنسق • التدخل الخبيث في أنظمة الكمبيوتر والأجهزة الرقمية الأخرى • القرصنة الإلكترونية • سرقة الأصول الفكرية • الإرهاب الإلكتروني • الجرائم المالية عبر الإنترنت • غسل الأموال

شكل رقم (1): تهديدات الأمن السيبراني (نقلاً عن [25]).

المطلب الثاني: آليات مواجهة خطر الذكاء الاصطناعي المرتبط بالإرهاب الإلكتروني

1. مكافحة الأمية الإلكترونية

إن هنالك عددا من المواطنين الذين لا يتاح لهم التعامل مع الكمبيوتر أو الدخول على شبكة الإنترنت لأسباب تعليمية أو اقتصادية، وهو ما يسمى بالفجوة الرقمية، وللتغلب على هذا العائق ينبغي إدخال مادة الكمبيوتر ضمن منهاج التعليم العام، وإتاحة فرص الحصول على أجهزة كمبيوتر منخفضة لتكون في متناول عامة الناس، ومكافحة أمية الإنترنت، وتدريب الشباب الخريجين على استخدام الكمبيوتر [26].

2. دور وسائل الإعلام

يسهم الإعلام الجديد والتقليدي بدور كبير جدا في تعزيز الوعي الرقمي لدى المتلقين، لا سيما الشباب منهم، بوصفهم الفئة الاجتماعية الأكثر استخداما له في وقتنا الراهن، وظهور ما يعرف بالإعلام الرقمي الذي استطاع أن يجذب أعدادا كبيرة من جانب الشباب، من خلال العالم الافتراضي الذي يمتاز بسهولة الوصول للمعلومة، وسهولة الوصول للمتلقي، فضلاً عن وجود

عنصر التفاعل بين المرسل والمتلقي، بوصفه عابرا للحدود، وإزاء تلك التحديات لا بد من توظيف هذا البعد من الجهات والمؤسسات الحكومية وغير الحكومية، فضلاً عن الفاعلين في بيئة هذا الإعلام لتنشئة المتلقين، وتدريبهم، وتزويدهم بالمعلومات والخبرات، التي تمكنهم من الابتعاد عن التفاعل مع الدعوات والنشاطات، التي تحمل بعدا طائفيا أو إرهابيا، ما يقلل من خطورة توظيف الذكاء الاصطناعي من الجماعات الإرهابية والمتطرفة لغرض التأثير في المواطنين وبالتحديد فئة الشباب[27].

3. الدور القانوني

تقع مسؤولية تفعيل هذا الدور على السلطة التشريعية، والمنظمات المدنية الفاعلة المرتبطة بالثقافة القانونية، إذ لا بد من تشريع قوانين من شأنها أن تضبط الواقع الافتراضي، وتحدد العقوبات الرادعة لمن يوظف أو يتفاعل مع المواقع أو الحسابات الرقمية التي تحمل دلالات التطرف والإرهاب وضرورة وضع أساس تشريعي للجرائم الحديثة، التي كان سببها العالم الرقمي مثل جرائم التحريض، والتجنيد، والتدريب الإرهابي، وعمليات السرقة والنصب والاحتيال والتزوير في البيانات، وحماية الملكية الفكرية، إذ إن التشريعات القانونية قد لا تتلاءم مع التطور الرقمي الحديث ومتطلبات العالم الافتراضي، وبذلك يتم خلق بيئة إلكترونية نظيفة، ذلك أن المستخدم لشبكات الإنترنت سيتفهم حدود حريته، وهذا الأمر سيحد من توظيف البيئة الإلكترونية للعمليات الإرهابية كون من يستخدمها يعرف أن هناك قوانين وتشريعات رادعة، وعلى ضوء ذلك يجب أن يتبنى المشرع دورا تشريعيا يستند إلى الخبرات الأكاديمية ومنظمات المجتمع المدني المختصة لإنجاز هذا الدور على أتم وجه، بحيث لا يتنافى مع حقوق الإنسان في حرية الرأي والتعبير، وإنما يركز على إيقاع العقوبة على من يوظف الذكاء الاصطناعي لأغراض من شأنها أن تهدد الأمن والسلم المجتمعي[28].

4. تفعيل وسائل مراقبة الاستخدام وتتبع سجلات النفاذ أو الأداء (الاستخدام)

هي عبارة عن مجموعة من التقنيات، التي تستخدم من الجهات الأمنية المختصة لمراقبة العاملين على توظيف الذكاء الاصطناعي في العمليات الإرهابية أو نشر الأفكار المتطرفة، التي تهدد أمن المواطنين والتماسك الاجتماعي لتحديد الشخص الذي قام بالعمل المعين في وقت معين،

وتشمل أنواع البرمجيات والسجلات الإلكترونية كافة التي تحدد الاستخدام، وهذا الأمر يسهم في تعقب المنفذين للهجمات الإرهابية الإلكترونية في وقت حدوث الفعل أو بعده، وتحديد أماكن تواجدهم عبر استخدام تقنيات التعقب الذكية، وبذلك يسهل عملية الوصول إليهم، وإلقاء القبض عليهم.

وقد يصل الأمر إلى التنبؤ بالهجمات والعمليات الإرهابية الإلكترونية قبل وقوعها، إذ أصبح الذكاء الاصطناعي جزءا لا يتجزأ من الأمن السيبراني، لدرجة أن يصعب الفصل بينهما، وذلك لقدرة أنظمة الذكاء الاصطناعي التي توجد في الحاسوب على إظهار التهديدات، ومن ثم التصدي بسرعة عالية، وذلك في حالة توظيفها بشكل صحيح ضمن منظومة الأمن السيبراني، لا سيما أن الأمن السيبراني وتقنيات الذكاء الاصطناعي ترتبط بصورة مباشرة أو غير مباشرة بخصوصية الأفراد التي تعد واجبة الحماية، وهذه المعلومات يمكن اختراقها، ومن ثم إساءة استخدامها من خلال العمل على اختراق الأمن السيبراني للدول والأشخاص وانتهاك خصوصية بياناتهم[29].

وأعلنت شركة تريند مايكرو العالمية الرائدة في مجال الأمن السيبراني في 2023/7/17 عن نتائج تقريرها السنوي للأمن السيبراني، الذي كشف عن زيادة ملحوظة بنسبة 55٪ في عمليات اكتشاف التهديدات العالمية، وزيادة هائلة على مستوى الملفات الخبيثة المحظورة بلغت نسبة 242٪ في عام 2022، وقدر تعلق الأمر بالعراق نجحت حلول الشركة باكتشاف وحظر أكثر من 15 مليون تهديد عبر البريد الإلكتروني، وقامت بحماية أكثر من 400 ألف مستخدم من التضرر من روابط خبيثة قاموا بالضغط عليها، كما استطاعت تحديد وإيقاف أكثر من نصف مليون هجوم لبرمجيات خبيثة في الدولة، وهذا يكشف لنا حجم التهديدات الإلكترونية[30].

فضلًا عن ذلك، ففي عام 2014 تمكنت شركات أمنية مختصة بالأمن السيبراني من مراقبة ورصد حركات تنظيم داعش الإرهابي عن طريق الأقمار الاصطناعية وأجهزة GPS، ومراقبة استعمالهم لمواقع التواصل الاجتماعي عند القيام بعمليات تجنيد المزيد من الإرهابين والدعاية للتنظيم، ونلاحظ استعمال الجماعات الإرهابية أحدث التقنيات التكنولوجية الرقمية للحصول على الدعم اللوجستي، واستعمال الأسلحة المتطورة الذكية الأمنية والعسكرية في أغلب الأعمال الإرهابية لزعزعة الأمن القومي العراقي، وهنا جاء دور محللي الأمن السيبراني في رصد

تحركات تنظيم داعش الإرهابي بشن هجمات عبر الإنترنت، ومعرفة أماكن تواجدهم والعمل على اختراق منظومتهم الأمنية وتفكيكها للقضاء تدريجيا على التنظيم[31].

5. تعزيز التعاون الدولي والإقليمي والدخول في المعاهدات والاتفاقيات متعددة الجنسيات المتعلقة بالأمن السيبراني

إن لهذا البعد أمرا بالغ الأهمية، إذ تشكل محركاً لتنمية القدرات؛ لذا يجب على العراق أن يعمل ويتعاون مع الدول والهيئات الدولية على تبادل المعلومات لمواجهة التحديات السيبرانية، التي تتعرض لها المؤسسات، فإقليميا عن طريق التعاون مع عدد من الدول الإقليمية ذات التجارب الناجحة في تحقيق الأمن السيبراني، ومثال على ذلك المملكة العربية السعودية التي عملت على حماية أمنها السيبراني عبر إنشاء (الهيئة السعودية للأمن السيبراني)، التي جعلت من البلاد أن تحتل المرتبة (13) عالميا في مؤشر الأمن السيبراني لعام (٢٠١٨)، المرتبة (2) عالميا ضمن تقرير عام (2023) الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا (IMD)، الهادف إلى تحليل وترتيب قدرة الدول على إيجاد بيئة داعمة ومحفزة للتنافسية والمحافظة عليها وتطويرها،ومن بين هذه الهيئات هو (الاتحاد الدولي للاتصالات) الذي يخصص جزءا رئيسا من برامجه وخطط عمله لتحقيق الأمن السيبراني، وكذلك يمكن للعراق التعاون مع (المجلس الأوروبي)، الذي أقر معاهدة مكافحة الجريمة السيبرانية، التي دخلت حيز التنفيذ عام (٢٠٠٤)، داعيا الدول جميعا إلى التوقيع عليها، منذ تأريخ إقرارها في العام (٢٠٠١)، وتعد أحكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة السيبرانية، لا سيما أنها تطلب من الدول الأعضاء، إنشاء مراكز اتصال، تعمل بحسب مبدأ استمرارية الخدمة، أي بمعنى تأمين متابعة على مدار الساعات، إذ تكون دائمة الاستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، وللتعاون مع القوات المعنية بمكافحة الجريمة، بسرعة وفاعلية عالية[32].

6. البعد الأمني

تطبيق السياسات الأمنية اللازمة، التي يتم وضعها من مختصين بهذا المجال، إذ إن العمل على ذلك يتضمن وضع سياسات وإجراءات أمنية صارمة وتنفيذها لضمان الامتثال القانوني والتنظيمي والتصدي للتهديدات السيبرانية، وضرورة اعتماد مبدأ (أقل الامتياز) وفقاً لهذا المبدأ، يجب أن يتم منح الوصول إلى الموارد السيبرانية والبيانات فقط للأشخاص الذين يحتاجون إليها

لأداء مهامهم، وهذا يقلل من فرص الوصول غير المصرح به، ويقيد نطاق الأضرار في حالة التعرض إلى هجوم[33].

شكل رقم (2): ركائز الأمن السيبراني في مواجهة التهديدات (نقلاً عن [34]).

الخاتمة

شكّل التحدي الرقمي تحديا كبيرا للدول ولصانعي السياسات العامة من الناحية الأمنية، إذ يعد الذكاء الاصطناعي بوصفه واحدا من منتجات ذلك التحول من أهم التحديات حديثاً، إذ إن هذا البعد يشكل تهديدا خطيرا للأمن القومي للدول، فبإمكان الجماعات الإرهابية توظيف هذا البعد لضرب أمن الدول، وتهديد حياة مجتمعاتها، وبذلك فالقيام بالعمليات الإرهابية بهذا الشكل يعد تحولاً خطيرا وتحديا كبيرا للدول والمؤسسات الأمنية، فاستخدام الذكاء الاصطناعي سهل كثيرا للجماعات الإرهابية القيام بأعمالها، وبذلك انتقل الصراع من وصفه واقعيا إلى صراع افتراضي، وهذا الأمر يضع على الدول مسؤوليات كبيرة جدا تتمثل بضرورة مواكبة التطور التكنلوجي عبر إيجاد كفاءات إدارية وأمنية وعسكرية تأخذ على عاتقها مواجهة هذا التحدي، فضلاً عن الانتباه

إلى البعد الدولي من خلال عقد شراكات إقليمية ودولية مع الدول المتقدمة بهذا المجال لإيجاد صيغ حديثة من شأنها تقويض هذا النوع من الإرهاب.

ونتيجة لذلك، فإن إعادة تشكيل النهج التعاوني والشراكة بين الإنسان والآلة يعد أمرا حيويا للاستفادة الكاملة من إمكانات الذكاء الاصطناعي في تحديد مخابئ الأسلحة والإرهابيين، إذ ينبغي أن يشكل النهج التعاوني هذا جسرا يجمع بين قدرات البشر والقوة التحليلية للذكاء الاصطناعي، ولا يستبدل الذكاء الاصطناعي الخبرة البشرية والحكم عبر تبني علاقة تكافلية، فيمكن تحسين تعزيز فاعلية العمليات الأمنية والعسكرية من خلال استعمال مسؤول وفعال للذكاء الاصطناعي في هذا السياق، ومن هنا يتضح لنا أن للذكاء الاصطناعي وجهين، فيمكن توظيفه من الجماعات الإرهابية لشن هجماتها الإجرامية، كما يمكن توظيفه من الدول ومؤسساتها لضرب وتقويض تلك الجماعات من أجل الوصول إلى بيئة آمنة ومستدامة.

الاستنتاجات

1. إن التوظيف التكنولوجي الحديث سلاح ذو حدين، إذ يمكن استخدام الذكاء الاصطناعي لأغراض علمية وإنسانية من شأنها أن تخدم البشرية والتقدم العلمي، فضلاً عن إمكانية توظيفه واستخدامه لأغراض سلبية من جهات وجماعات متطرفة من شأنها أن تهدد الأمن والسلم المجتمعي.
2. إن الجماعات الإرهابية عملت وبشكل ملحوظ، وخاصة بعد دحرها ميدانيا وانكماشها إلى اللجوء لتوظيف الذكاء الاصطناعي المرتبط بالإرهاب، وعملت على تطوير إمكاناتها المادية ومواردها البشرية لغرض ضرب وإحداث زعزعة أمنية في مناطق وجودها وغيرها.
3. إن خطورة توظيف الذكاء الاصطناعي ترتبط بإمكانية عمل هجمات إرهابية على المؤسسات الأمنية والعسكرية والخدمية وحتى الأهداف المدنية، وذلك يكون بشكل عابر للحدود، وهذا الأمر يشكل واحدا من أوجه الصعوبات من مكافحة هذا الفعل الإجرامي.
4. إن التطور التكنولوجي يسهم بتعدد وتنوع طبيعة الهجمات الإرهابية الإلكترونية، إذ وفرت البيئة التقنية أساليب متنوعة لتلك الجماعات، وبإمكانها أن تستهدف الجماعات الاجتماعية، لا سيما شريحة الشباب بوصفهم أكثر الجماعات استخداما للتقنيات البرمجية، وصولاً إلى إمكانية

استهداف المؤسسات الحكومية والمدنية؛ لذا فإن خطورة الإرهاب الإلكتروني تمتد إلى البعدين الاجتماعي والعسكري والأمني وحتى البعد الاقتصادي ليس ببعيد عنها.

5. إن آليات المواجهة المتبعة وخاصة في البلدان التي في طور النمو لا زالت متخلفة وبحاجة إلى تحديث لمواجهة هذا الخطر المتنامي، إذ ما يلاحظ أن استراتيجيات المواجهة ضعيفة وبدائية، وهذا الأمر يخل بموازنة المجابهة، ويجعل من تلك الدول أرضا رخوة لتلقي الهجمات الإرهابية الإلكترونية.

التوصيات

1. ضرورة تبني استراتيجيات وطنية مستدامة قائمة على الكفاءة والخبرة الأمنية والعسكرية والتقنية من أجل وضع خطط تقنية هجومية ودفاعية للحد من الهجمات الإرهابية الإلكترونية.
2. ضرورة انتقال الحكومات وصانع القرار من الاعتماد الذاتي في المجابهة إلى الشراكة المستدامة مع القطاع الخاص، لا سيما ضرورة الانتباه إلى القطاع الأكاديمي المتخصص بهذا الجانب.
3. ضرورة عقد اتفاقيات ومعاهدات وشراكات مع المنظمات الدولية وحكومات الدول المتقدمة بهذا الجانب لفتح آفاق التعاون الأمني لمواجهة خطر الإرهاب الإلكتروني.
4. ضرورة انتباه صانع القرار إلى تحديث المنظومة التشريعية التي تخص الجريمة الإلكترونية والعمل على استحداث تشريعات صارمة من شأنها مواجهة ومعاقبة ومحاسبة مرتكبي هذه الجرائم.
5. ضرورة أن تتبنى المؤسسة الأمنية والعسكرية خططاً واضحة وعلمية قائمة على تحديث منظومة الأدوات التقنية تتماشى مع قيم العصر التكنولوجي لمواجهة الهجمات الإرهابية الإلكترونية.

المصادر

(1) بونيه الآن (1993): الذكاء الاصطناعي واقعه ومستقبله، ترجمة: علي صبري، المجلس الثقافي الكويتي، الكويت، العدد 172.

(2) سيف المنصور شيخة والطحيطاح علي ناصر (2021): دور الذكاء الاصطناعي في اتخاذ القرارات، مجلة كلية المعارف الجامعة، العدد 3، ص68.

(3) حسان نورهان سليمان (2020): تكنلوجيا الإعلام المتخصص: ديناميات مستقبلية، مؤسسة حورس الدولية، الإسكندرية، ص65.

(4) البياتي مصطفى عماد محمد (2022) حدود الذكاء الاصطناعي والمسؤولية الناشئة عنه على الصعيد الدولي، مجلة القادسية للقانون والعلوم السياسية، مجلد13، العدد 2، ص271.

(5) راشد سامح (2022): الذكاء الاصطناعي في مواجهة الإرهاب: فرص وتحديات، مجلة الأهرام للشؤون الدولية والإقليمية، القاهرة، العدد 75، ص2.

(6) جيركي ماركو (2014) فهم الجريمة السيبرانية: الظاهرة والتحديات والجريمة القانونية، الاتحاد الدولي للاتصالات، جينيف، ص114.

(7) راشد سامح (2022): مصدر سابق، ص7.

(8) ايسيني ألبانا (2022): الذكاء الاصطناعي والأمن السيبراني: دراسة فيما يخبئه المستقبل، ترجمة: باسم علي خريسان، بغداد، مركز البيان للدراسات والتخطيط.

(9) حسين سعد علي (2004): الولايات المتحدة وسبل مكافحة الإرهاب الدولي، مجلة الدراسات الدولية، مركز الدراسات الدولية، جامعة بغداد، العدد 20، ص95.

(10) صادق يوسف محمد (2007): الإرهاب والصراع الدولي، رسالة ماجستير غير منشورة، كلية العلوم السياسية، جامعة النهرين، بغداد، ص10.

(11) صادق يوسف محمد (2007): المصدر نفسه، ص46.

(12) شكري محمد عزيز (1991): الإرهاب الدولي، بيروت، دار العلم للملايين، 1991، ص46.

(13) شكري محمد عزيز (1991): المصدر نفسه، ص50.

(14) عبد الصادق عادل (2019): الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ص107.

(15) البشري محمد الأمين (1422 ه): التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، الرياض، ص22.

(16) منشاوي محمد عبد الله (1433): جرائم الإنترنت من منظور شرعي وقانوني، مطبعة جامعة الملك فهد، الرياض، ص11.

(17) القرعان محمود أحمد محمد (2017): الجرائم الإلكترونية، دار وائل، عمان، ص176.

(18) بولمكاحل إبراهيم (2021): تجليات الإرهاب السيبراني: داعش ونهج الخلافة الرقمية، في عبد القادر دندن محررًا، العلاقات الدولي في عصر التكنولوجيا الرقمية: تحولات عميقة ومسارات جديدة، مركز الكتاب الأكاديمي، الجزائر، ص141-142.

(19) مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC (2013): استخدام الإنترنت في أغراض إرهابية، مكتب الأمم المتحدة، فيينا، ص3.

(20) منيخر حازم جري (2020) توظيف القوة السيبرانية في استراتيجيات الدول الكبرى، أطروحة دكتوراه، جامعة النهرين، كلية العلوم السياسية، بغداد، ص23.

(21) عواد منى جلال (2020): مقاربات تحليلية لظاهرة الإرهاب الإلكتروني، مجلة تكريت للعلوم السياسية، جامعة تكريت، كلية العلوم السياسية، العدد 19، ص44.

(22) المسند عبد الرحمن (2002): وسائل الإرهاب الإلكترونية: حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الأول، الرياض، ص127.

[23] خليل رؤى خليل سعيد (2018): الإرهاب الإلكتروني وأثره في أمن الدول: السعودية أنموذجًا، مجلة حمورابي، مركز حمورابي للدراسات الاستراتيجية، العدد 25-26، ص60.
[24] الحسين ياسمين وعمروش (2021): التهديدات الإلكترونية والأمن السيبراني في الوطن العربي، مجلة نوميروس الأكاديمية، الجزائر، العدد 2، ص165.
[25] موسى حازم حمد (2023): قراءة تحليلية لاستراتيجية الأمن السيبراني العراقي، مجلة فرسان الرد السريع للدراسات الأمنية، وزارة الداخلية، قيادة الرد السريع، بغداد، العدد 2، ص193.
[26] القدوة محمود (2017): الحكومة الإلكترونية والإدارة المُعاصِرة، دار أسامة للنشر والتوزيع، عمان، ص195.
[27] عبد السلام وفاء حافظ (2012): الانعكاسات الاجتماعية للإنترنت كأحد أشكال التكنولوجيا الرقمية، دراسة وصفية مطبقة على عينة من طلاب جامعة القاهرة، المؤتمر الدولي الخامس والعشرين لكلية الخدمة الاجتماعية في جامعة حلوان، مصر، ص365.
[28] المعمري سعيد بن علي بن حسن ورضوان أحمد الحاف (2022): مبدأ الأمن القانوني ومقومات الجودة التشريعية - مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، ص233.
[29] خلف حسام عبد الأمير، حمزة وهج علي (2023): مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي، مجلة جامعة الأنبار للعلوم القانونية والسياسية، جامعة الأنبار المجلد، 13، العدد 2، ص655-656.
[30] موقع شفق نيوز، 20 مليون تهديد في العراق: تقرير الأمن السيبراني يكشف حصيلة 2022، 2023/3/17، شبكة المعلومات الدولية-إنترنت- https://shafaq.com.
[31] الشمري مصطفى إبراهيم سلمان (2021): الجرائم الإلكترونية وتأثيرها في العراق، وقائع المؤتمر العلمي الدولي التاسع، "العراق بعد عام ٢٠٠٣ الدولة، المجتمع، الاقتصاد، القانون، العلاقات الخارجية: التحديات والفرص"، مركز الدراسات الإقليمية جامعة الموصل، تحرير: لقمان عمر محمود النعيمي، دار نون للطباعة والنشر والتوزيع، ص173.
[32] جبور منى الأشقر (2012) الأمن السيبراني: التحديات ومستلزمات المواجهة، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، القاهرة، ص7-8.
[33] بطو أحمد (2022): عناصر الأمن السيبراني، على الرابط: https://cyberone.co.
[34] عودة زمن ماجد (2023): الأمن السيبراني وإدارة المخاطر العراق أنموذجًا، مجلة فرسان الرد السريع للدراسات الأمنية، وزارة الداخلية، قيادة الرد السريع، بغداد، العدد 2، ص211.