قضايا سياسية

اسم المقال: مكافحة الإرهاب الالكتروني: تحليل التهديدات وتعزيز القدرات الدفاعية
اسم الكاتب: م.م. سحر عبد السادة دريعي
رابط ثابت: https://political-encyclopedia.org/index.php/library/7537
تاريخ الاسترداد: 2026/11/02 17:24 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهرين ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

مكافحة الإرهاب الالكتروني: تحليل التهديدات وتعزيز القدرات الدفاعية▽

Electronic counterterrorism: Threats analysis and defensive capabilities enhancement

م.م. سحر عبد السادة دريعي*
Sahar AbdulSada Duraye

الملخص:

تعّد مكافحة الإرهاب الإلكتروني من أهم التحديات التي تواجه المجتمع الدولي في الوقت الحالي، إذ يتم استعمال التكنولوجيا والإنترنت لتنظيم وتنفيذ الأعمال الإرهابية؛ وتشمل هذه التهديدات الإلكترونية الهجمات على البنية التحتية للإنترنت والتجسس الإلكتروني والاحتيال الإلكتروني واختراق الأنظمة الإلكترونية والاعتداء على بيانات المستخدمين، وغيرها من الأنشطة الإلكترونية الخبيثة، وبالتالي فإن تحليل التهديدات الإلكترونية وتعزيز القدرات الدفاعية ضد هذه التهديدات يعّدان من أهم الأولويات للحفاظ على الأمن والاستقرار العام.

تسعى الدراسة إلى تحليل التهديدات الإلكترونية التي يمكن استعمالها في أعمال الإرهاب وتحديد الأساليب والتقنيات اللازمة لتعزيز القدرات الدفاعية ضد هذه التهديدات، بما في ذلك تحسين الأمان الإلكتروني وتدريب الموظفين وتطوير الأدوات الأمنية المتطورة، ويتم تقديم هذه النتائج والإجراءات كمساهمة في مكافحة الإرهاب الإلكتروني وتعزيز الأمن الإلكتروني في المؤسسات والمنظمات المختلفة.

الكلمات المفتاحية: الارهاب، التهديدات الالكترونية ، الهجمات الالكترونية، الحماية الالكترونية.

Abstract:

Cyberterrorism is one of the most important challenges facing the international community today, as technology and the internet are used to organize and carry out terrorist activities. These electronic threats include attacks on internet infrastructure, electronic espionage, electronic fraud, system penetration, attacks on user data, and other malicious electronic activities. Therefore, analyzing electronic threats and enhancing defensive capabilities

▽ تاريخ التقديم : 2023/7/18 تاريخ القبول: 2023/8/16 تاريخ النشر: 2023/9/31
* الجامعة المستنصرية/ كلية العلوم السياسية. E-mail/ ad30sahar@gmail.com

against these threats are among the top priorities for maintaining general security and stability.
This study aims to analyze electronic threats that could be used in terrorist activities and identify the necessary methods and techniques to enhance defensive capabilities against these threats, including improving electronic security, training employees, and developing advanced security tools. The results and measures presented in this study are offered as a contribution to the fight against cyberterrorism and the enhancement of electronic security in various institutions and organizations.

Key Words: Terrorism, Electronic Threats, Cyber Attacks, Electronic Protection.

المقدمة:

يشهد العالم تحولات كبيرة ومن بين هذه التحولات، الثورة التكنولوجية الهائلة، والتي أثرت على تطور المفاهيم المختلفة، إذ تم تشكيل مفاهيم جديدة تتلاءم مع هذا العصر من بينها ظهور مفهوم الإرهاب الإلكتروني كشكل جديد من أشكال الإرهاب، يعتمد على توظيف التقنيات الرقمية الحديثة لنشر الخوف والرعب لأغراض مختلفة، كما يمكن عده جريمة إلكترونية عابرة للحدود تهدد أمن الدول، خاصة الدول المتقدمة التي تعتمد تكنولوجيا المعلومات والاتصال في مختلف المجالات.

يختص الإرهاب الإلكتروني بمجموعة من الخصائص التي تميزه عن غيره من أشكال الإرهاب، كونه يستعمل تقنيات نظم المعلومات كأساس لتنفيذ أعماله، ويتميز بسرية هوية المستخدم، وعدم ترك آثار كبيرة، فضلًا عن قدرته على تجاوز القيود الإقليمية والدولية، كما تسبب الهجمات الإلكترونية الإرهابية أضرارًا كبيرة وتؤثر على عدد كبير من الضحايا، وأنها تُنفذ بسرعة وسهولة وباستعمال موارد بسيطة قد تكون جهاز محمول او حاسب آلي وشبكة أنترنت.

تهدف الهجمات الإرهابية الإلكترونية إلى تحقيق أهداف خبيثة، بما في ذلك الإخلال بالأمن العام وزعزعة استقرار المجتمعات، وتمويل التنظيمات الإرهابية والعمليات الإرهابية، ونشر أفكار مغلوطة، وتجنيد اعضاء جدد، ونشر الرعب والخوف بين الناس، كما تستهدف الهجمات الإرهابية الإلكترونية وسائل الاتصالات والبنية التحتية المعلوماتية، ويشترك الإرهاب الإلكتروني والإرهاب التقليدي في أهدافهما

السياسية، حيث يسعى كل منهما إلى تحقيق أهداف سياسية بغض النظر عن التبريرات الاجتماعية أو العرقية أو الدينية المستعملة.

تشمل مكافحة الإرهاب الإلكتروني تحليل التهديدات الإلكترونية، والتعرف على الأساليب المستعملة في الهجمات الإرهابية الإلكترونية، وتطوير القدرات الدفاعية للحد من هذه المخاطر، ويتطلب تحليل التهديدات الإلكترونية دراسة متعمقة للأساليب التي يستعملها المجرمون والإرهابيون في الهجمات الإلكترونية، بما في ذلك البرامج الضارة والتصيد الاحتيالي والهجمات الموزعة على الخدمة.

تستلزم مكافحة الارهاب الالكتروني أن تكون القضايا القانونية والتشريعية مواكبة للتطورات السريعة في مجال مكافحة الإرهاب الإلكتروني، وتحديد المسؤوليات والواجبات والحقوق المتعلقة بمكافحة الجرائم الإلكترونية والإرهاب، كما ينبغي أن تتضمن هذه الجهود قوانين وتشريعات تحظر وتعاقب على الجرائم الإلكترونية وتحمي حقوق الأفراد والمؤسسات.

أهمية البحث : تزداد أهمية دراسة مكافحة الإرهاب الإلكتروني في العصر الحديث نظراً لارتفاع تهديد الإرهاب الإلكتروني وتأثيره السلبي على الأفراد والمجتمعات، كما يعّد مكافحة الإرهاب الإلكتروني جزءًا هامًا من الأمن الإلكتروني، إذ يسعى الخبراء إلى حماية أنظمة المعلومات وبنية الإنترنت من الهجمات الإلكترونية للإرهابيين، فضلا عن حماية المعلومات الحساسة، ومكافحة الأفكار المتطرفة على الإنترنت، ورفع الوعي العام حول خطر الإرهاب الإلكتروني وكيفية الوقاية منه، من خلال توعية الأفراد والمجتمعات حول أساليب الهجمات والتحذير من مخاطر الانتماء لجماعات إرهابية عبر الإنترنت، وتطوير حلول تقنية مبتكرة للكشف والوقاية والاستجابة لهذه التهديدات، وتحديد أفضل الممارسات والسياسات الأمنية والتشريعية للحد من هذه التهديدات.

هدف البحث : يهدف البحث إلى تحسين الأمن السيبراني وتعزيز القدرات الدفاعية ضد التهديدات الإلكترونية المرتبطة بالإرهاب، ويتم ذلك من خلال إجراء تحليل شامل للتهديدات الإلكترونية المختلفة وتطوير الأدوات والتقنيات اللازمة للكشف والوقاية والاستجابة لهذه التهديدات.

ومن بين الأهداف الرئيسة للبحث في مجال مكافحة الإرهاب الإلكتروني، هو تحديد الاتجاهات الحالية والمستقبلية للتهديدات الإلكترونية، وتحديد أفضل الممارسات والسياسات الأمنية والتشريعية للحد من هذه التهديدات وتعزيز الأمن السيبراني، فضلًا عن توفير بيئة محفزة للابتكار والتطوير في هذا المجال،

ويمكن أيضًا لنتائج البحث أن تساعد الجهات المعنية في اتخاذ القرارات الأمنية والإدارية اللازمة للحد من التهديدات الإلكترونية وتعزيز الأمن السيبراني.

مشكلة البحث : تتمثل مشكلة البحث في التحديات الكبيرة التي تواجه الأمن السيبراني والتهديدات الإلكترونية المرتبطة بالإرهاب، وتشمل هذه التحديات التطور المستمر للتهديدات الإلكترونية، وتعقيد الأمن السيبراني والتهديدات المتعّددة الأطراف، وارتفاع تكلفة الحماية السيبرانية والتدريب اللازم لذلك، لذا جاء هذا البحث ليجيب على تساؤل مهم ورئيس هو :

– ما هي مجالات مكافحة الإرهاب الإلكتروني، وكيفية تعزيز القدرات الدفاعية؟

يتفرع عن هذا التساؤل عدة تساؤلات فرعية هي:

1. ما هو الإرهاب الإلكتروني؟
2. ما هي الأدوات المستعملة في مكافحة الإرهاب الإلكتروني؟
3. ما هي التحديات التي تواجه مكافحة الإرهاب الإلكتروني؟
4. كيف يمكن للحكومات والمؤسسات التعاون في تحسين القدرات الدفاعية ضد الإرهاب الإلكتروني؟
5. ما هي أفضل الممارسات التي يمكن اتباعها لحماية البنية التحتية الرقمية من الهجمات الإلكترونية الإرهابية؟
6. كيف تتعامل الحكومات مع قضية الخصوصية في إطار مكافحة الإرهاب الإلكتروني؟

فرضية البحث : ينطلق البحث من فرضية مفادها (أن تحليل تهديدات الارهاب الالكتروني وتحسين القدرات الدفاعية للمؤسسات الحكومية والشركات والأفراد يساعد على تقليل الأضرار الناجمة عن هذه التهديدات وتحسين الأمن السيبراني بشكل عام).

منهجية البحث:

يرتكز البحث على المنهج الوصفي الذي يرمي إلى وصف وتحليل الظواهر والعمليات المتعلقة بمكافحة الإرهاب الإلكتروني، ويساهم في توفير صورة شاملة للمفاهيم والممارسات والتحديات التي تواجه مجال مكافحة الإرهاب الإلكتروني.

اولًا:- الاطار النظري لمفاهيم الدراسة

أن تحديد المفاهيم يعّد من الاشكاليات التقليدية في الدراسات الانسانية، لاسيما في حقل العلوم السياسية، ولغرض تغطية جوانب الموضوع بشيء من التفصيل، فضلا عن محاولة توضيح رأي المختصين حول التأصيل النظري لمفهوم الارهاب الالكتروني، لابد من البحث في مفهوم الارهاب والارهاب الالكتروني وخصائصه.

1. مفهوم الإرهاب:

لا يوجد مفهوم جامع وموحد لمصطلح الإرهاب (Terrorism)، وهذا يعّد أمراً ملحاً إذ تتطلب الحاجة إلى تعريف دقيق لهذا المصطلح لوضع الأمور في نصابها الصحيح، فالتعريف الدقيق للإرهاب يساعد في فهم طبيعته وأبعاده المختلفة، ويمكن من خلاله تطوير الإجراءات الوقائية والتدابير الأمنية المناسبة للحد من هذه الظاهرة الخطيرة.

ترد كلمة الإرهاب على المستوى اللغوي من كلمة (رَهِبَ) بمعنى خاف [1]، أما معجم مصطلحات العلوم الاجتماعية فقد عرف الارهاب بأنه "بث الرعب الذى يثير الخوف، اوالفعل بأي طريقة تحاول بها جماعة منظمة أو حزب أن يحقق أهدافه عن طريق استعمال العنف، وتوجه الأعمال الارهابية ضد الأشخاص سواء كانوا أفراداً أو ممثلين للسلطة مما يعارضون أهداف هذه الجماعة" [2]، كما تم تعريف مصطلح الإرهاب في القاموس السياسي على (أنه استعمال الذعر والفزع لأغراض سياسية، وأنه يمكن استعماله كوسيلة من قبل حكومة استبدادية لإجبار الشعب على الخضوع له)، ومن جانبه يعني مصطلح الإرهاب وفقًا لقاموس أكسفورد (استعمال العنف والتخويف أو الرعب، وخاصة لأغراض سياسية) [3].

يشير مصطلح الإرهاب إلى سلوكيات عنيفة ومنظمة تستهدف إشاعة حالة من الرعب وعدم الاستقرار في المجتمعات، وتشمل ذلك الاغتيالات والتفجيرات والهجمات المسلحة على المنشآت والأفراد والممتلكات، وكذلك أعمال القرصنة واختطاف الرهائن وإشعال الحرائق وغيرها من الأعمال التي تستهدف المصالح

---

[1] ابو الفضل جمال الدين، لسان العرب، بيروت، دار صادر، 1955، ج8، ص337.

[2] حيدر علي نوري، الجريمة الارهابية دراسة في ضوء قانون مكافحة الارهاب، لبنان، مكتبة زين الحقوقية، 2012، ص56.

[3] احمد عطية، القاموس السياسي، القاهرة، دار النهضة العربية، 1975، ص45.

الأجنبية، يتم تنفيذ هذه الأعمال من قِبَل جماعات منظمة تهدف إلى تحقيق أهداف سياسية، وتترتب على هذه الأعمال زعزعة الاستقرار الداخلي في الدول المستهدفة وإثارة النزاعات الدولية، وقد يؤدي ذلك إلى تبرير التدخل العسكري للدول الأجنبية [1].

وتم تعريف الارهاب في الاتفاقية العربية لمكافحة الإرهاب التي صدرت عن مجلسي وزراء الداخلية والعدل العرب في عام 1998، على (أنه كل فعل من أفعال العنف أو التهديد به، سواء كان منفذًا بشكل فردي أو جماعي، ويهدف إلى خلق الرعب والترويع بين الناس، وإيذاءهم، وتعريض حياتهم وحريتهم وأمنهم للخطر، وإلحاق الضرر بالبيئة والمرافق العامة والخاصة، واختلاسها، والاستيلاء عليها، وتعريض الموارد الوطنية للخطر)، هذا التعريف يساعد على فهم طبيعة الإرهاب وتحديد الأعمال التي تشكل عملًا إرهابيًا ووضع استراتيجيات فعالة لمكافحته وتحقيق الأمن والسلم الدوليين [2].

تختلف وتتضارب آراء الباحثين في الفقه الغربي حول تعريف مصطلح الإرهاب نظراً لاختلاف المعايير التي يستعملونها لتحديد مفهوم العمل الإرهابي، ويمكن أن نعزو هذا التباين إلى الأفكار المسبقة والأولويات المختلفة التي يحملها كل باحث، ومن خلال استعراض مجمل الآراء التي ظهرت في هذا الخصوص، يمكن تحديد بعض الاتجاهات الرئيسية التي اتبعت لتحديد مفهوم العمل الإرهابي في الفقه الغربي، وتشمل [3]:

-الاتجاه الأول: يعرف الإرهاب بأنه عمل عنف إيديولوجي يرتبط بأهداف سياسية، أو كل نشاط إجرامي يستعمل العنف لتحقيق أهداف سياسية، ويعرف الجريمة الإرهابية بأنها كل جناية أو جنحة سياسية تنتج عنها الخوف العام.

-الاتجاه الثاني: يضفي هذا الاتجاه صفة العشوائية على العمل الإرهابي، إذ يعرف الإرهاب بأنه عمل عنف عشوائي يهدف إلى إحداث آثار غير تمييزية.

---

[1] عبد السلام زكريا، الإرهاب بين الأمس واليوم، بيروت، دار غريب، د.ت، ص 15.

[2] اسراء فهمي ناجي، مفهوم الارهاب في الشريعة والقانون، مجلة العلوم القانونية والسياسية، عدد خاص بالمؤتمر العلمي الدولي الثاني للكلية، جامعة ديالى/ كلية القانون والعلوم السياسية، 2013، ص 423.

[3] إريك موريس وألان هو، الإرهاب.. التهديد والرد عليه، ترجمة د. أحمد حمدى محمود، القاهرة،الهيئة المصرية العامة للكتاب، ١٩٩١م، ص ١٦٣.

– الاتجاه الثالث: يتميز هذا الاتجاه بالتركيز على شدة العنف التي تتضمنها الأعمال الإرهابية، إذ يعرف الإرهاب بأنه عمل عنف ذو جسامة غير عادية يرتكبه الإرهابيون بهدف تحقيق أهداف سياسية.

لا يخضع الإرهاب للنطاق الجغرافي، بل أصبح مشكلة عالمية تتطلب جهودًا دولية في مجالات الأمن والاقتصاد والاجتماع والسياسة، ولمواجهته لا يكفي دور الحكومات فحسب، بل يشترك فيه مختلف المؤسسات وقطاعات الأعمال والأفراد في ميدان مكافحة الإرهاب، وبالتالي يتوجب على المجتمع الدولي العمل بتعاون شامل وتنسيق فعال لمكافحة هذه الظاهرة وتعزيز الشفافية والمساءلة وحقوق الضحايا والمجتمعات المتضررة، وأن الإرهاب ظاهرة عالمية تقوم على استعمال العنف أو التهديد به، ويؤدي تعريف مفهوم الإرهاب إلى تحديد المسؤوليات والالتزامات القانونية للدول والأفراد والمجتمعات في مواجهة هذه الظاهرة.

2. مفهوم الإرهاب الالكتروني:

يعتمد الإرهاب الإلكتروني على استغلال الإمكانيات العلمية والتقنية، واستعمال وسائل الاتصالات والشبكات المعلوماتية لتحقيق أهدافه؛ ويهدف الإرهاب الإلكتروني إلى ترويع الآخرين وإلحاق الضرر بهم، وذلك من خلال استعمال البيانات والأساليب الإلكترونية المختلفة، ويتمثل الهدف الرئيسي للإرهاب الإلكتروني في تحقيق الأهداف السياسية أو الشخصية، ويمكن أن يتسبب في الأضرار المادية والبشرية.

يمكن تناول مفهوم الإرهاب الإلكتروني على انه استعمال الفضاء الإلكتروني لتنفيذ أنشطة إرهابية أو حربية، والتي تهدف إلى التأثير على القرارات الحكومية والرأي العام العالمي. ويستعمل الإرهاب الإلكتروني البنية التحتية للإنترنت كوسيلة للتواصل والتنفيذ، ويستعمل البيانات والأساليب الإلكترونية للتحريض ونشر الكراهية الدينية وحروب الأفكار، يمكن أن يؤدي الإرهاب الإلكتروني إلى الأضرار المادية والبشرية، إذ يمكن استعمال الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في فضاء الإنترنت، وقد يتعّدى تأثيرها الرقمي لتصل إلى الأهداف المادية [1].

يشير بعض الباحثين إلى أن الإرهاب الالكتروني هو نوعاً جديداً من أنواع القوة الناعمة الجديدة، فلم تعّد القوة قاصرة على القوة الصلبة، سواء كانت عسكرية أو اقتصادية، والتي كانت محتكرة من قبل الدول

[1] عادل عبد الصادق، هل يمثل الارهاب الالكتروني شكلا جديدا من اشكال الصراع الدولي، الاهرام الاستراتيجي،العدد 156، مركز الدراسات السياسية والاستراتيجية ، 2007، ص18.

الكبرى فقط، إذ أدى ظهور القوة الافتراضية إلى انتهاء احتكار القوة التقليدية، وأصبح كل من لديه معرفة تكنولوجية وقدرة على استعمالها يمتلك القدرة على التأثير في النظام العالمي، ويعّد الإرهاب الإلكتروني من أهم أدوات هذه القوة الناعمة الجديدة، إذ يمكن استعماله لتحقيق أهداف سياسية واجتماعية واقتصادية، ويمكن أن يتسبب في الأضرار المادية والبشرية [1].

يمكن تعريف الإرهاب الإلكتروني على أنه " عمل اجرامي يتم التحضير له عن طريق استعمال أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف ارباك وزرع الشك لدى الافراد وذلك بهدف التأثير على الحكومة أو الافراد لخدمة أجندة سياسية أو اجتماعية أو ايديولوجية، من خلال هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً من أجل الانتقام أو الابتزاز أو اجبار الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية" [2].

بناء على ما سبق، يمكن القول إن الإرهاب الإلكتروني يمثل تهديداً خطيراً في الوقت الحاضر واكثر خطورة في المستقبل، نظراً لتعّدد أشكاله وتنوع أساليبه، وإمكانية استهداف مجموعة واسعة من الأهداف باستعمال وسائل الاتصالات وتقنية المعلومات في بيئة هادئة وآمنة، مما يوفر للإرهابيين قدراً كبيراً من السرية والأمان، لذلك يستلزم أن يكون هناك تعاون دولي وجهود مشتركة لمواجهة هذا التهديد الجديد والمتزايد، وتعزيز الحماية الأمنية للأفراد والمؤسسات ضد هذه الأنشطة الإرهابية.

3. خصائص الإرهاب الالكتروني

أهم ما يميز الإرهاب الالكتروني عن غيره، هو استعماله لكل الوسائل التقنية الحديثة في تنفيذ مخططاته وتدويلها سواء فيما يتعلق بالتخطيط أو التمويل أو التبرير أو التنفيذ، وتلجأ الجماعات الارهابية لاستعمال شبكات التواصل الاجتماعي للترويج لأفكارها وتجنيد الشباب والشابات من مختلف جنسيات العالم، ويتسم الإرهاب الالكتروني بعدة خصائص أهمها [3]:

---

[1] جمال علي الدهشان، الإرهاب في العصر الرقمي (الإرهاب الإلكتروني) صوره، مخاطره، آليات مواجهته، المجلة الدولية للبحوث في العلوم التربوية، العدد 3، مصر، 2018، ص92.

[2] جمال علي الدهشان، المصدر السابق، 94.

[3] المصدر نفسه, ص94- ص97.

أ. يعتمد على التقنيات الحديثة: يتميز الإرهاب الإلكتروني بالاستفادة من الموارد المعلوماتية والوسائل الإلكترونية المتاحة، إذ يختلف عن الإرهاب التقليدي بطريقة عمله، كونه يستند إلى التقنيات الحديثة في مجال المعلوماتية والاتصالات، ويستغل الإمكانات العلمية والتقنية المتاحة لتنفيذ جرائمه، ويتضمن ذلك استعمال وسائل الاتصال والإنترنت وتقنيات مثل أنظمة تحديد المواقع عبر الأقمار الصناعية (GPS)، والهواتف الجوالة وبرامج الكمبيوتر للتعرف على الأصوات باللغات المختلفة، إلى غير ذلك، ما هي إلا أساليب تكنولوجية حديثة في العصر الرقمي، قد يساء استعمالها من قبل البعض في تحقيق أهداف واعتداءات إجرامية وإرهابية.

ب. الكلفة المنخفضة: يتميز الإرهاب الإلكتروني بأنه عنصر جاذب للجماعات الإرهابية، إذ يتطلب إيجاد بعض المعلومات لاختراق الحواجز الإلكترونية، ولا يحتاج لأسلحة ومدرعات وقنابل أو تحركات سرية مكلفة في الإرهاب الفعلي، وبسبب هذا الاختلاف يمكن للإرهاب الإلكتروني أن يكون أقل تكلفة وأكثر فاعلية في تحقيق أهدافه، ومن المهم مراقبة هذا النوع من التهديدات وتحديد الإجراءات الوقائية والاستباقية اللازمة لمنع حدوثها، وحماية الأنظمة الإلكترونية والمعلومات الحيوية من الاختراقات والاعتداءات.

ج. الإرهاب الإلكتروني يتنوع في أشكاله وأساليبه، ويشمل التجسس والاختراق والقرصنة والتجنيد الإلكتروني والتهديد والترويع، ويستعمل الفيروسات والتجسس وتجنيد الإرهابيين وجمع الأموال وحروب الدعاية للأفكار المتطرفة والهدامة وغيرها كأدوات.

د. الإرهاب الإلكتروني يتجاوز الحدود ويؤثر على العالم بأسره، ويستعمله الإرهابيون للتأثير في الرأي العام وتجنيد أعضاء جدد وجمع الأموال ونشر رسالتهم وشن حرب نفسية والدعاية للتنظيم.

هـ. تتميز جرائم الإرهاب الإلكتروني بصعوبة إثباتها، وذلك بسبب قدرة المهاجمين على التخفي وتجهيل مصادر المعلومات، وبخلاف الهجمات التقليدية، لا توجد أدلة مادية واضحة، ويرجع ذلك إلى العديد من الأسباب، مثل كفاءة المهاجمين، وارتفاع درجة الخداع والتضليل، واختلاف الزمان والمكان والقانون المطبق في الدولة التي ارتكبت فيها الجريمة، وعند نسب هجوم إلكتروني إلى جهة معينة، فإنه يمكن رفض هذه التهمة بسبب تحدي "الإنكار المقبول"، وبسبب إمكانية إخفاء الهوية التي يتيحها الفضاء السيبراني.

تشكل صعوبة إثبات جرائم الإرهاب الإلكتروني والجرائم الأخرى في الفضاء الإلكتروني عائقاً حقيقياً أمام مهمة المحققين، إذ يصعب الوصول إلى الدليل الرقمي اللازم لإثبات وإدانة الجناة، وذلك بسبب تخفي

المهاجمين وعدم وجود أدلة مادية واضحة، وتعّد هذه الجرائم بيئة افتراضية عابرة للحدود، الامر الذي يجعلها صعبة التعقب والكشف عنها، وقد يوصف بعض الجرائم الإلكترونية بأنها "تخيلية"، مثل جرائم النصب والاحتيال والسطو على أموال الآخرين، والتشهير والتحريض على تعاطي الرذيلة، وتصعب إثباتها في أغلب الحالات، نظراً لسهولة التخلص وإتلاف الأدلة المادية، وترتبط غالباً بالخصوصية والحرية الشخصية، وبالتالي، يتم الكشف عن معظم هذه الجرائم بطريقة عرضية، وليس بسبب الكشف الفعال عنها من قبل الجهات الرسمية، وتعّد هذه التحديات تتعّدى حدود الدول وتتطلب التنسيق الدولي والتعاون لمواجهة هذه الجرائم [1].

وتأسيسًا على ماتقدم؛ فأن خطورة الإرهاب الإلكتروني تزداد مع زيادة استعمال الجماعات الإرهابية للتقنية، وتتركز هذه الخطورة في الدول المتقدمة التي تستخدم بنية تحتية تقنية متطورة، ويمكن للجماعات الإرهابية من خلال الإنترنت الهجوم على البنية التحتية وتدميرها بشكل أسرع وأكثر فعالية، وذلك بشكل يفوق مثيلته في استعمال المتفجرات، كما ويمكن للجماعات الإرهابية شن هجمات إلكترونية لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات.

ثانيًا:- مخاطر الإرهاب الالكتروني

يشكل الإرهاب الإلكتروني تهديدًا جديدًا للأمن السيبراني والاقتصادي والسياسي والاجتماعي، وتشمل مخاطره اختراق البيانات الحساسة والهجوم على البنية التحتية التقنية والقرصنة الإلكترونية والإرهاب النفسي والاحتيال الإلكتروني، ويتطلب تحديد مخاطر الإرهاب الإلكتروني توضيح الأدوات التي يستعملها المهاجمون، فضلاً عن الأضرار التي يسببونها وكيفية استعمالهم لوسائل الإعلام الرقمية في تحقيق أهدافهم.

1. أدوات الإرهاب الالكتروني:

أ. انشاء المواقع الالكترونية: صار تصميم المواقع جزءًا هامًا في نشر الأفكار (الجهادية)، إذ يستعمل الإرهابيون شبكة الإنترنت لنشر أفكارهم عبر آلاف المواقع والمنتديات (الجهادية)، ويعود سبب أهمية الإنترنت في ذلك إلى سهولة استعماله وتوفره وسرعته وأمانه، إذ يمكنهم من خلال تصميم مواقع ومنتديات وغرف دردشة أن يتواصلوا ويتجمعوا لتبادل المعلومات وجذب إرهابيين جدد وتدريبهم على الهجمات

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، الاسكندرية، منشأة المعارف، 2009، ص ١٥٦.

الإرهابية، وتستخدم بعض المنظمات الإرهابية آلاف المواقع لتوسيع انتشار أفكارهم، وبالتالي فأن هذه المواقع تصير ملجأً آمنًا ومناسبًا لعقد الاجتماعات والتواصل بين الأعضاء على المستوى العالمي [1].

ب. الاختراق: يمكن لعملية الاختراق الإلكتروني أن تتم من أي مكان في العالم دون الحاجة إلى تواجد القراصنة في الدولة التي يتم اختراق موقعها، وتهدف عمليات الاختراق إلى إفساد وظائف أنظمة المعلومات وتدمير الأصول الافتراضية والمادية وحجب المواقع الإلكترونية وتعطيل الحياة اليومية باستهداف البنية التحتية التي تُدار بأجهزة حاسوبية كالمرافق الطبية والبورصات والنقل والأنظمة المالية وغيرها [2]. ومن الامثلة على ذلك قيام (داعش) بعدة عمليات اختراق مثل اختراق القمر الصناعي المصري نايل سات وبث قناة تابعة للتنظيم واختراق قناة (TV5) الفرنسية ومواقعها وحساباتها على مواقع التواصل الاجتماعي، واختراق بعض المواقع والشبكات لتشويهها ونشر الدعاية المتطرفة كما حدث مع مواقع وزارة الصحة البريطانية والشرطة الماليزية الملكية والخطوط الجوية الماليزية، ولايمكن على الشركات التعامل مع مثل هذه الهجمات الا من خلال اتباع نظام التشويش أو الانتظار لمخاطبة إدارة تلك الأقمار لمنع محتواها من الوصول [3].

ج. التجسس: يقوم المتشددون بعمليات التجسس على الأفراد والدول والمنظمات والهيئات الدولية والوطنية، وتتميز عمليات التجسس الإلكتروني بالاعتماد على الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وتهدف عمليات التجسس الإرهابي في عصر المعلومات إلى ثلاثة أهداف رئيسية وهي: التجسس العسكري والتجسس السياسي والتجسس الاقتصادي، ومن المتوقع أن تزداد الطرق الفنية للتجسس المعلوماتي استعمالاً في المستقبل من قبل التنظيمات الإرهابية، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية [4].

---

[1] حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، جامعة ديالى، 2013، ص331.

[2] سعد عطوة الزنط، الارهاب الالكتروني واعادة صياغة استراتيجيات الامن القومي، مصر، المركز القومي للبحوث الاجتماعية والجنائية، 2010، ص4.

[3] جمال علي الدهشان، المصدر السابق، ص97.

[4] هشام بشير، الإرهاب الالكتروني في ظل ثورة المعلومات، 2012، على الرابط:
https://araa.sa/index.php?option=com_content&view=article&id

د. تطبيق (تليجرام): اعتمدت الجماعات الارهابية على استعمال تطبيقات دردشة مشفرة مثل (تليجرام) لتحقيق أهدافه الإرهابية، وقد قام (جيش الخلافة الرقمي) بتدريب كوادره على فن اخفاء الهوية الرقمية على الإنترنت، وقد أدى هذا التحول في الاستراتيجية العسكرية ل(داعش) إلى تغيير في أساليبها وأدواتها المستعملة، وتعّد تطبيقات مثل(تليجرام) قوية التأمين، إذ يتم تنفيذ التشفير مباشرة على الهواتف المحمولة دون الحاجة إلى خادم أو وسيط، الامر الذي يجعلها أكثر أماناً وصعوبة في التجسس عليها من قبل الشركات المطورة للتطبيقات. ويتميز تطبيق تليجرام بميزات مثل إمكانية تدمير الرسائل تلقائياً بعد فترة زمنية محددة [1].

هـ. الإنترنت المظلم (The Dark Web) : تعرف بأنها "أرض الخدمات المخفية"، إذ يتم الحفاظ على سرية هوية المستخدمين وعدم ترك آثار على الإنترنت، وذلك بعيداً عن مراقبة الحكومات واستخباراتها، ويتمكن القائمون على التنظيمات الإرهابية من التواصل بسرية تامة من خلال الإنترنت المظلم، إذ يتم حماية المعلومات وصعوبة تتبع النشاط الإلكتروني من قبل مزود الخدمة أو الحكومة، ولذا يعّد الإنترنت المظلم هو المكان الأمثل للتخفي بعيداً عن أعين المراقبين، ويمكن الوصول إلى الإنترنت المظلم من خلال خدمات مثل تور (Tor)، وتُعتبر الشبكة المظلمة سوقاً غير تقليدية تقدم مجموعة مقلقة من المنتجات والخدمات غير المشروعة، مثل شراء العقاقير غير المشروعة والأسلحة والسلع المقلدة وبطاقات الائتمان المسروقة والبيانات المخترقة، وكذلك العملات الرقمية والبرامج الضارة وبطاقات الهوية الوطنية وجوازات السفر، وفي الوقت الحالي، تستخدم الجماعات الإرهابية هذه الخدمات لممارسة أنشطتها بشكل سري وغير مراقب [2].

2. اضرار الإرهاب الالكتروني:

يشكل الإرهاب الإلكتروني تهديدًا خطيرًا (للأمن السيبراني)* والاستقرار العام، إذ يمكن أن يؤدي إلى حدوث أضرار جسيمة في البنية التحتية الإلكترونية للدول، وتترتب عليه أيضًا تأثيرات سلبية على الاقتصاد

---

(1) المستقبل للابحاث والدراسات المتقدمة، لماذا تلجأ التنظيمات الإرهابية لاستعمال "تليجرام"؟، 2018، على الرابط:
https://futureuae.com/ar-AE/Mainpage/Item/3610

(2) Darren Guccione, What is the dark web? How to access it and what you'll find, 2021, on:
https://www.csoonline.com/article/564313

* يرجع أصل مصطلح الأمن السيبراني إلى لفظ (Cyber) اللاتينية والتي تعني الفضاء المعلوماتي، وأن الامن السيبراني هو أمن الفضاء المعلوماتي، وهو تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات وآليات وتطبيقات

والمجتمعات، وتشمل هذه الأضرار فقدان البيانات الحساسة، وتعريض الأمن القومي للخطر، والإضرار بالاقتصاد والتجارة الإلكترونية، والإضرار بالأمن الصحي والبيئي، والتأثير على الحريات الفردية وحقوق الخصوصية، كما يمكن للإرهاب الإلكتروني أن يتسبب في التحريض على العنف والكراهية والتمييز، ويؤدي إلى تفاقم الصراعات والنزاعات في أنحاء مختلفة من العالم.

تتمثل أضرار الإرهاب الإلكتروني، في شل أنظمة القيادة والسيطرة والاتصالات، وقطع شبكة الاتصال بين الوحدات والقيادات المركزية، وتعطيل أنظمة الدفاع الجوي، والتحكم في خطوط الملاحة الجوية والبحرية والخطوط البرية، واختراق النظام المصرفي وإلحاق الأضرار بأعمال البنوك وأسواق المال العالمية.، ويتم استعمال تقنية المعلومات لإصابة المرافق الحيوية ومن ثم فإن الأهداف التي تتعرض للتهديد تخزين المعلومات عمليات إدخال المعلومات ارسال واستقبال الرسائل، استهداف البنية التحتية للمعلومات وخاصة في قطاعات الكهرباء والاتصالات والكمبيوتر والتي تعّد وبحق ركائز الأمن القومي الجديد، فضلًا عن تقديم الوصفات الجاهزة لصناعة القنابل، ومهاجمة نظم التحكم الوطني في الطيران لإحداث تصادم بين الطائرات، ومهاجمة نظم التحكم الوطني في قطارات السكك الحديدية لإحداث تصادم بين القطارات، مما يُلْحِقُ الأذى بالاستثمار الأجنبي، وبالثقة بالاستثمار عامة، وإلحاق الأذى بالاقتصاد الوطني، وتعّديل كل من ضغط الغاز عن بعد في أنابيب الغاز لتفجيرها، ونظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، وأيضاً الدخول عن بعد لنظام التحكم في علاج المرضى في المستشفيات بهدف قتل المرضى، وفي مصانع غذاء الأطفال لتغيير مستويات نسب المواد الغذائية، إذ تمكن بعض القراصنة من اختراق مجموعة (سيتي جروب) الأمريكية، وسرقة عشرات الملايين من الدولارات، مما أصاب النظام الاقتصادي الأمريكي بخسائر فادحة، وهذا الفعل تبين بعد ذلك أنه تم بالتنسيق بين مجموعة من القراصنة الأمريكيين بعصابة روسية من خلال شبكة الإنترنت، أيضاً في عام ٢٠١٠م عقب ما عُرف بإعصار ويكيليكس (Wikileaks Storm) الذي تضمن أخطر قضايا القرصنة المعلوماتية في القرن الواحد والعشرين، إذ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم[1].

تقنيات المعلومات والحاسب الالي، والترابط فيما بينها من خلال شبكات الانترنت. انظر: حيدر علي حسين، سياسة الولايات المتحدة الامريكية ومستقبل النظام الدولي، بغداد، دار الكتب العلمية للطباعة والنشر والتوزيع، 2017، ص279.

[1] جمال علي الدهشان، المصدر السابق، ص97.

3. توظيف (الإعلام الرقمي)*:

احتلت الحملات الاعلامية للجماعات الإرهابية، وتحديدًا (داعش)، مساحات واسعة في مواقع التواصل الاجتماعي، إذ استعملت صفحات خاصة بها لنشر حملات إعلامية منظمة ومتزايدة مع التوسع والتقدم الميداني، وقد استعملت الجماعة أساليب متطورة للترويج الإعلامي الإلكتروني، ومن بينها بث رسائل عن طريق وسوم (هاشتاغ) يطلقها التنظيم عنواناً رئيساً لكل حملة يقوم بها، منذ بدء الهجوم على مدينة الموصل في محافظة نينوى العراقية في عام 2014م، كما استعمل التنظيم أدوات الإعلام الاجتماعي الحديثة بشكل شامل، ووظف كل ما يمكن من أدوات الإنترنت في خدمة خطته الإعلامية التي يديرها، وتفوق القائمون على (داعش) في الترويج الخطابي والفكري وصناعة الدعاية الإعلامية، سواءً كان بالتغرير أو بالترهيب، ويبدو هذا واضحاً في الغزو المعلوماتي الفكري لوسائل التواصل الاجتماعي، وخاصةً "تويتر" التي باتت ميداناً إضافياً من ميادين المعارك التي يخوضوها، وقد نجحت الجماعة في التواصل مع المجتمعات المختلفة، وبلغات عدة، عبر مئات الحسابات والصفحات التي خاطبتها، ولا يمكن تجاهل أعداد المتابعين لها على "تويتر"، الذين يصل عددهم حسب(Brookings Institution–USD) إلى ما لا يقل عن (46) ألف حساب[1].

اعتمد تنظيم (داعش) بشكل كبير على وسائل الإعلام الرقمي منذ احتلاله للعراق والشام، وفي دراسة نشرتها قناة العربية عام 2015م، تبين أن التنظيم يمتلك سبعة أذرع إعلامية يستعمل من خلالها العنف والإرهاب للتأثير على العالم، وهي: "أجناد الفرقان، الاعتصام، الحياة، مكاتب الولايات، إذاعة البيان، مجلة وموقع دابق، و (90) ألف صفحة على مواقع التواصل الاجتماعي فيسبوك وتويتر، وتعّد هذه القنوات وسيلة تسويق لأفكار التنظيم في مختلف دول العالم، إذ يمكن تجنيد أكبر عدد من المواطنين وتأكيد مفهوم الخلافة، والتحضير لغزو أمريكا وأوروبا خلال الفترة المقبلة [2].

---

* مجموعة من الاساليب والانشطة الرقمية التي تنتج محتوى اعلامي بمختلف اشكاله من خلال توظيف شبكة الانترنت، واستعمال مواقع التواصل الاجتماعي، في عملية تفاعلية بين المرسل والمستقبل. انظر: انتصار محمد القحطاني، الاعلام الرقمي، المجلة الالكترونية الشاملة، عدد2، 2019، على الرابط:

https://www.eimj.org.

[1] فيصل ارشد، كيف يستعمل "((داعش))" الانترنت في الترويج لنفسه؟، 2014، على الرابط:

https://www.bbc.com/arabic/middleeast/2014/06/140619_isis_internet_campaign.amp

[2] أشرف عبد الحميد، ((داعش)) يمتلك 7 قنوات و90 ألف حساب إلكتروني، 2015، على الرابط:

كما اعتمدت سياسة (داعش) الإلكترونية على نشر كم هائل من المحتوى، من أجل جذب شريحة كبيرة من المتعاطفين معهم من مختلف مناطق العالم، وحثهم على الجهاد لقيام الدولة المزعومة من خلال وجود التنظيم في الفضاء الإلكتروني، ويعبر عن هذا الأمر الباحث في قضايا الإرهاب(J. M. Berger) الذي تعقب نحو ثلاث ملايين تغريدة ل(داعش) على تويتر، فوجد أن التنظيم يدير أكثر من (7500) حساب يستعمل في ذلك هاشتاغات جهادية [1].

سخر (داعش) أدواته في الترويج لأفكاره ومشروعه، من خلال مواد إعلامية دعائية تشمل ما يأتي [2]:

1. الإصدار المرئي كالأفلام الطويلة والقصيرة، الميدانية والتوجيهية، المتسلسلة والمتفرقة الوثائقية وغيرها، وهي أهم أنواع الإصدارات وأكثرها انتشارا في وسائل التواصل الاجتماعي والمواقع التابعة للتنظيم.

2. الإصدار الصوتي، وهو كل ما يصدره التنظيم من تسجيلات صوتية، وأناشيد مؤثرة في الشباب.

ويصدر تنظيم (داعش) مجلة دابق الاحترافية باللغة الإنجليزية (Dabiq)، ولها ثلاثة أعداد مترجمة للغة العربية، وهدفها استهداف المتحدثين باللغة الإنجليزية، وتتميز المجلة بالإخراج والتصميم والجودة، وتعّد مؤسسة الفرقان للإنتاج الإعلامي المؤسسة الرئيسية لتنظيم الدولة، فضلًا عن ذلك، يحتل مركز الحياة للإنتاج الإعلامي مكانة بارزة بين المراكز الإعلامية في التنظيم، وذلك لأنه يتخصص في التواصل مع الشباب المسلم في الدول الغربية بلغات مختلفة، والتأثير عليهم، وقد ظهرت مؤسسات إعلامية عديدة تابعة لتنظيم (داعش) مؤخراً، مثل مؤسسة الاعتصام، ومركز الحياة، ومؤسسة أعماق، ومؤسسة البتار، ومؤسسة دابق الإعلامية، ومؤسسة الخلافة، ومؤسسة أجناد للإنتاج الإعلامي، ومؤسسة الغرباء للإعلام، ومؤسسة الإسراء للإنتاج الإعلامي، ومؤسسة الصقيل، ومؤسسة الوفاء، ومؤسسة نسائم للإنتاج الصوتي، فضلًا عن مجموعة من الوكالات التي تتبع الولايات والمناطق التي يسيطر عليها التنظيم، مثل وكالة أنباء البركة، والخير، وغيرها [3].

---

https://www.alarabiya.net/amp/arab-and-world/egypt//10/03/2015

[1] محمد سليمان ابو رمان، سر الجاذبية: ((داعش))، الدعاية والتجنيد، عمان، مؤسسة فريدريش ايبرت، 2016، ص50.

[2] وليد عبد الرحمن، صراع القاعدة و((داعش)) ينتقل للإصدارات المرئية، صحيفة الشرق الاوسط، 2019، على الرابط: https://aawsat.com/home/article/1719561/

[3] اشرف عبد الحميد، المصدر السابق.

نستخلص مما تقدم، أن استعمال الجماعات الإرهابية لوسائل الإعلام الرقمي يشكل عدة مخاطر في مجال مكافحة الإرهاب الإلكتروني، فمن خلال استعمالها للإعلام الرقمي، تتمكن هذه الجماعات من توصيل رسائلها وأفكارها بشكل واسع وسريع، الامر الذي يؤدي إلى تأثير كبير في الجمهور وزيادة نفوذها، كما يسهل استعمال الإعلام الرقمي التواصل بين أفراد الجماعات الإرهابية وتنظيم أنشطتهم وتنسيقها بشكل أفضل، كما يشكل استعمال الجماعات الإرهابية للإعلام الرقمي تحديًا كبيرًا للأجهزة الأمنية والمخابراتية، إذ يصعب تتبع ومراقبة الأنشطة الإلكترونية لهذه الجماعات.

ثالثًا:- آليات مكافحة الارهاب الالكتروني

يشكل الإرهاب الإلكتروني تهديدًا خطيرًا على الأمن الدولي، إذ يستعمل الإرهابيون وسائل التكنولوجيا الحديثة والإنترنت للتخطيط وتنفيذ هجمات إرهابية، ولمواجهة هذا التهديد، تعمل الدول والمؤسسات الأمنية على تطوير استراتيجيات وآليات لمكافحة الإرهاب الإلكتروني، ولأن الكثير من الحكومات ادركت بالفعل خطورة الارهاب الالكتروني وعمليات التجنيد التي تتم عبر شبكات التواصل الاجتماعي، لذلك سعت جاهدة ألى شن (حرب الكترونية)* مضادة من خلال عمليات معقدة تبدأ بالرصد والمتابعة والمراقبة وتنتهي باتخاذ إجراءات عملية وقائية [1]، وتشمل هذه الاجراءات استراتيجيات تعزيز التعاون الدولي وتشديد التشريعات القانونية وتطوير التكنولوجيا الأمنية والأمن الإلكتروني، فضلًا عن التوعية العامة والتثقيف حول خطر الإرهاب الإلكتروني.

1. تحسين القدرات الدفاعية:

أ. جمع المعلومات:

يعّد جمع المعلومات الاستخباراتية أساسيًا في مكافحة الإرهاب الالكتروني، إذ تساعد هذه المعلومات في التحقيق مع المشتبه بهم وتستخدم كدليل في المحاكمة، بعد الحصول عليها من خلال القنوات المختلفة

* سلسلة هجمات تستهدف الانظمة المعلوماتية للدول والجهات المعادية عبر الفضاء الالكتروني، والتي غيرت طبيعة الحرب، فهي لا تستهدف تدمير المعدات العسكرية ولا القوات البشرية للعدو، ولا تهدف للاستيلاء على ارض العدو، وانما الحاق الضرر البالغ ببناه التحتية بأقل تكلفة. انظر : صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، عمان- الاردن، جامعة الشرق الاوسط، 2021، ص22.

[1] عادل عبد القادر المكينزي، الاعلام الرقمي وسبل مواجهة الارهاب، الرياض، دار جامعة الملك سعود للنشر، 2019، ص65.

مثل شبكة الإنترنت والمواقع الإلكترونية وغرف الدردشة ونشرات الإنترنت. وتعّد بيانات قادة الحركات الإرهابية مصدرًا مهمًا لتحليل المعلومات الاستخباراتية، وقد يعطي تحليل محتوى هذه البيانات بعض النوايا والمعلومات القيمة، ولإنجاح هذه العملية، يتطلب الأمر تدريب وتخصيص وحدات مكافحة الإرهاب لجمع المعلومات الاستخباراتية، وكذلك التقييم والتحليل لتطوير الإستراتيجيات الفعالة لمواجهة التهديد الإرهابي، ومع ذلك، ينبغي تجنب التضارب في المسؤوليات والأهداف بين وكالات الاستخبارات الوطنية، إذ يمكن أن يؤدي هذا إلى عرقلة التنسيق وترجمة المعلومات الاستخباراتية إلى خطط عملياتية فعالة، كما يتطلب مراعاة أن يكون تحليل المعلومات الاستخباراتية قائمًا على الدقة في جمع المعلومات [1].

ويمكن لتحليل السياق أن يساعد في تحديد ما يريد الشخص الذي يدلي بالبيانات أن يسمعه جمهوره، ويمكن استعمال هذا التحليل لقياس بعض اتجاهات الشارع. وبالتالي، يمكن أن يكون هذا التحليل مفيدًا للمؤسسات الاستخباراتية في تحديد تركيز جمع المعلومات التكتيكية. ومن المهم أن يتم إيلاء اهتمام خاص للغة وتركيز وتصميم المواقع (الجهادية)، إذ يمكن أن تكشف اللغات المستعملة عن جمهور (الجهاديين) ومن المستهدفين لتجنيدهم. وفي بعض الحالات، يمكن أن يشير هذا الأمر إلى نقاط الضعف الملحوظة بين المجموعة المستهدفة، والملفت أن هذا التحليل يمكن أن يساعد أيضًا في تحديد الأشخاص الذين يرغب الجهاديون في جندهم، ومن هم الأكثر استعمالا لهم [2].

فضلًا عن ذلك تصميم المواقع والصور تلعب دورًا حيويًا في توجيه رسالة الجماعات الإرهابية وجذب المؤيدين والمجندين المحتملين، وغالبًا ما يتم تصميم هذه المواقع والصور من قبل أفراد متطرفين ماهرين في استعمال التقنيات الحديثة، ومن المهم أن يتم التركيز على هذه الجوانب في الحملات الوقائية ومكافحة الإرهاب، ويمكن استغلال خبرات الجماعات المكافحة للإرهاب وتوظيف مصممي الويب لبناء حملات مضادة، ويمكن أن يتم تحقيق النجاح في هذا النوع من الحملات المضادة من خلال العمل على تعزيز القدرات والتوعية في القواعد الشعبية على مستوى المجتمعات المحلية، إذ يتم التعاون مع الأفراد المستهدفين والذين يمكن اختيارهم للتجنيد من قبل الجماعات الإرهابية، يصبح المجتمع المكافح للإرهاب شريكًا رئيسيًا

---

[1] قوادرة حسين، كحلوش منى، دور الاستخبارات الالكترونية في مكافحة الارهاب السيبراني، الجزائر، مجلة الابحاث القانونية والسياسية، العدد1، 2021، ص 120.

[2] المصدر السابق، ص121.

في هذا العمل، إذ يجب أن يكون الهدف هو المنافسة على نفس الجمهور مع الجماعات الإرهابية في توجيه رسالة تعزز الأمن والسلم والتعايش السلمي [1].

يعّد جمع المعلومات أحد الأدوات الرئيسة في مكافحة الإرهاب الإلكتروني، كون الجماعات الإرهابية تستخدم وسائل الاتصال الحديثة والتقنيات الرقمية لتوجيه رسائلها وجذب المؤيدين والمجندين المحتملين، ومن خلال جمع المعلومات، يمكن لمؤسسات مكافحة الإرهاب تحليل هذه الرسائل والتنبؤ بالأنشطة الإرهابية المحتملة وتحديد الأهداف المحتملة والجماعات المتطرفة، كما تعّد جمع المعلومات أيضًا مهمًا في تحديد الأشخاص الذين يرغب (الجهاديون) في جندهم، والأكثر استعمالا لهم، وذلك من خلال تحليل اللغات المستعملة في المواقع الجهادية وتصميمها، وبالتالي، يمكن توظيف مصممي الويب والمجتمعات المحلية في بناء حملات مضادة تستهدف هذه الأهداف وتحقق النجاح في مكافحة الإرهاب الإلكتروني.

ب. سن التشريعات والقوانين

تزايد النشاط الإرهابي التكنولوجي يشكل تحديًا كبيرًا، إذ توجد عناصر إجرامية محترفة تنتشر في جميع أنحاء العالم، ويرتبط هذا النشاط بشبكة المعلومات الدولية. ولمواجهة هذا التحدي، قامت الامم المتحدة بمجموعة من المبادرات في مجال التكنولوجيا الحديثة من خلال مكتبها لمكافحة الإرهاب، ومن ضمن هذه المبادارت (برنامج أمن الفضاء الإلكتروني والتكنولوجيات الجديدة)، والذي يهدف إلى تعزيز قدرات الدول الأعضاء والمنظمات الخاصة في منع استغلال الإرهابيين والمتطرفين للتطورات التكنولوجية، وتخفيف آثار سوء استعمال هذه التكنولوجيات، ويتضمن ذلك؛ التصدي لخطر الهجمات الإلكترونية التي يشنها الجماعات الإرهابية على البنى التحتية الحيوية، فضلًا عن تطوير استعمال وسائل التواصل الاجتماعي لجمع المعلومات من مصادر مفتوحة والأدلة الرقمية لمكافحة الإرهاب والتطرف العنيف على الإنترنت، مع احترام حقوق الإنسان[2].

طلب مجلس الأمن من الدول الأعضاء في القرار (2341) عام 2017م إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع أصحاب المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على البنية التحتية الحيوية وحمايتها وتخفيف آثارها

---

[1] قوادرة حسين، كحلوش منى، المصدر السابق ، ص121.

[2] الامم المتحدة، مكتب مكافحة الارهاب، على الرابط:
https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity

والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك من خلال التدريب المشترك واستخدام أو إنشاء شبكات اتصال وإنذار مناسبة في حالات الطوارئ[1].

تهدف الجهود الحالية إلى وضع قوانين وتشريعات جديدة تتناسب مع الطبيعة المتغيرة للجرائم الإلكترونية والإرهاب الإلكتروني. ويتم ذلك من خلال تجريم أي استعمال غير آمن لتكنولوجيا المعلومات والاتصالات، وإصدار قوانين جديدة مثل قانون التوقيع الإلكتروني والمعاملات الالكترونية رقم (78) لسنة 2012م في العراق، وقانون مكافحة الإرهاب العراقي رقم (13) لسنة 2005م، اما فيما يتعلق بإصدار التشريعات المتعلقة بمكافحة الجرائم المعلوماتية في العراق، لا يزال البلد لم يتوصل إلى إصدار قانون مكافحة الجرائم المعلوماتية حتى الآن. إذ في عام 2011م فشل مجلس النواب في تمرير مسودة القانون، وتمت إعادة عرضها في عام 2019م، ولكن المجلس لم يفلح في تمريرها. كما تمت مناقشة المسودة في تشرين الثاني من عام 2020م بحضور عدد من رؤساء المنظمات وسفراء الدول والمختصين، فقد واجهت المسودة اعتراضات وانتقادات من بعض النواب، فضلًا عن الهجمة الإعلامية الشديدة ضدها، كون المسودة عدت تقييد لحقوق وحريات المواطنين المنصوص عليها في الباب الثاني من الدستور، وتم تأجيل تقديم المسودة لجلسة أخرى، ولكن انتهت دورة مجلس النواب دون أن تُعرض المسودة قبل انتهاء الدورة[2].

وعلى الرغم من عدم تمكن العراق من إصدار قانون مكافحة الجرائم المعلوماتية حتى الآن، إلا أن الموضوع ما زال قيد النقاش والمناقشة، ومن المحتمل أن يتم تقديم المسودة مرة أخرى في المستقبل للنظر فيها واتخاذ الإجراءات المناسبة.

تتطلب مكافحة الإرهاب الإلكتروني ضرورة إقرار جميع الحكومات والدول لقوانين وعقوبات صارمة لمرتكبي الجرائم الإلكترونية، ودعم الجهود التشريعية والأمنية في هذا الصدد، كما تتطلب هذه المكافحة تخصيص دوائر قضائية متخصصة للنظر في الجرائم الإلكترونية، والاستفادة من التشريعات الجنائية التي اعتمدها الاتحاد الأوروبي والدول الأخرى في هذا المجال [3].

---

[1] الامم المتحدة، مكتب مكافحة الارهاب، المصدر السابق.

[2] سعيد النعمان، مخاطر الجريمة الالكترونية، المنتدى العراقي للنخب والكفاءات، على الرابط:
https://iraqi-forum2014.com/%D8%A7%D9%84%D9/

[3] وادرة حسين، كحلوش منى، المصدر السابق، ص109.

استنادا لما تقدم يمكن القول أن المعركة ضد انتشار التطرف والإرهاب عبر شبكة الإنترنت تعتمد بشكل أساسي على ضرورة "تجريم" تلك الممارسات، من خلال سن قوانين خاصة تشمل السلوك على الإنترنت، وتضمن إجراء التحقيقات وإقامة الدعاوي القضائية بشكل فعال، ويتطلب ذلك التعاون الدولي ومواءمة التشريعات الوطنية، ويمكن تحقيق ذلك من خلال تبني نهجين على المستوى العالمي: الأول يتعلق بمكافحة الجرائم الإلكترونية، والثاني يتعلق بمكافحة الإرهاب، بشكل يضمن إجراء التحقيقات وإقامة الدعاوي القضائية بشكل فعال، وتجرم الممارسات الإرهابية عبر الإنترنت، وتتضمن التدابير المتخذة لمكافحة الإرهاب عبر الإنترنت، إنشاء دوائر قضائية مختصة بالجرائم الإلكترونية، وتبادل المعلومات والخبرات الأمنية والفنية بين الدول.

جـ . حفظ بيانات الانترنت: تم إجبار مقدمي خدمات الاتصالات الإلكترونية في بعض الدول على جمع بيانات الاتصالات الخاصة بمستعملي خدمات الاتصالات وأرشفتها، وتعود هذه الضرورة إلى عدة أسباب، من بينها الهجمات الإرهابية التي شهدتها مدريد في عام ٢٠٠٤م ولندن في عام ٢٠٠٥م، ولحماية المواطنين، فقد اتخذ الاتحاد الأوروبي توجيهًا في عام ٢٠٠٦م يفرض الاحتفاظ الإلزامي ببيانات حركة الاتصالات التي تنشأ أو تتم معالجتها في إطار تقديم خدمات الاتصالات الإلكترونية للجمهور أو شبكات الاتصالات العامة، ويهدف هذا التوجيه إلى تحقيق التوافق بين الدول الأعضاء في الاتحاد الأوروبي بشأن الالتزامات الدنيا المفروضة على مقدمي خدمات الاتصالات الإلكترونية، وذلك لغرض منع الأنشطة الجنائية والتحقيق فيها وكشفها ومساءلة مرتكبيها [1].

يتوجب على مقدمي خدمات الاتصالات الإلكترونية الاحتفاظ ببعض البيانات المتعلقة بحركة الاتصالات لمدة تتراوح بين ستة أشهر وسنتين، وذلك لغرض التحقق من هوية المرسل والمستقبل لرسائل البريد الإلكتروني والاتصالات الهاتفية، والحصول على معلومات حول توقيت وتاريخ ومدة هذه الاتصالات، ومع الأخذ في الاعتبار أهمية حماية الخصوصية، فإن هذه البيانات لا تتضمن محتوى الاتصالات الإلكترونية، ومن الضروري أن يتم توفير هذه البيانات لسلطات إنفاذ القانون الوطنية والأجنبية في الدول الأعضاء في الاتحاد الأوروبي، وذلك في إطار التحقيق في الجرائم الخطيرة والكشف عنها وملاحقة الجناة[2].

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استعمال الأنترنت في أغراض إرهابية، نيويورك، 2013، ص125.

[2] المصدر السابق، ص125.

ومن الممكن على سبيل المثال، بعد إدخال التوجيه في التشريعات المحلية وتلبية المتطلبات الإجرائية المناسبة، أن تطلب سلطات إنفاذ القانون الوطنية من مقدمي الخدمات الوصول إلى البيانات اللازمة للكشف عن هويات المشتركين الذين يستعملون عنوان محدد في بروتوكول الإنترنت، والجهات التي كانوا يتصلون بها خلال فترة محددة من الزمن، كما يمكن الاعتماد على بيانات يخزنها مقدمي الخدمات لفترة زمنية محددة للتحقيق في الأعمال الإرهابية، مثل فترة التخطيط للعمل الإرهابي، للكشف عن الأنماط السلوكية الإجرامية والعلاقات بين المشتبه بهم والمؤامرين، ولإثبات القصد الجنائي [1].

في العديد من الدول تتحكم جهات غير حكومية في قدرة المستخدمين على الوصول إلى الإنترنت، مثل مقدمي خدمات الاتصالات في القطاع الخاص الذين يملكون أو يديرون البنية التحتية الشبكية، وقد يكون هؤلاء المقدمون في موقع يمكنهم فيه مساعدة أجهزة إنفاذ القانون والعدالة الجنائية والاستخبارات في الحصول على بيانات الاتصالات أو الكشف عنها، حسب الاقتضاء، لدعم تحقيقات محددة تتعلق بأنشطة إرهابية محتملة، وقد تشكل بيانات الاتصالات التي يحتفظ بها مقدمو خدمات الإنترنت أدلة رئيسية في قضايا الجرائم المتعلقة بالإنترنت، وقد تؤدي إلى الوصول إلى أدلة إضافية أو شركاء جناة علها تفيد في التحقيق [2].

من الممكن أن يُطلب من مستعملوا الإنترنت تقديم معلومات تثبت هويتهم قبل الوصول إلى محتويات وخدمات الإنترنت، بما في ذلك من قِبَل مقدمي خدمات الإنترنت، ويمكن للحصول على معلومات إثبات الهوية وحفظها أن يؤدي دوراً مهماً في إجراءات التحقيق والملاحقة القضائية، ويشار بشكل خاص إلى أن اشتراط التسجيل لاستعمال شبكات الإنترنت اللاسلكية (واي فاي) أو مقاهي الإنترنت يمكن أن يوفر مصدرًا مهمًا للبيانات في التحقيقات الجنائية، وتشترط بعض البلدان، مثل مصر، توثيق هوية المستخدمين لدى مقدمي خدمات الإنترنت قبل السماح لهم بالوصول إلى الإنترنت، ويمكن لمقدمي خدمات الإنترنت تنفيذ تدابير من هذا النوع طوعًا [3].

د. تفعيل التعاون الدولي: يتم التعاون الدولي في العديد من دول العالم من خلال الاتفاقيات الدولية لضبط وتسليم المجرمين، بالإضافة إلى التعاون والتنسيق الدائم مع الإنتربول الدولي في مجال تبادل

---

[1] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، المصدر السابق، ص126.

[2] المصدر السابق، ص122.

[3] المصدر نفسه، ص123.

المعلومات والخبرات الأمنية والفنية في رصد ومتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايده المستمر من خلال عناصره الإجرامية المحترفة والمنتشرة في جميع أنحاء العالم، وارتباط هذا النشاط بشبكة المعلومات الدولية، وذلك لأن الفضاء الإلكتروني بات يشكل بيئة استراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع، ولظهور فاعلين جدد على الساحة الدولية [1].

وعلى الرغم من الوعي المتزايد بالتداعيات السياسية والاقتصادية والاجتماعية للحوادث السيبرانية، وأهمية وضرورة وجود أعراف مشتركة تسهل الوصول إلى تفاهم بين الدول، فإنه لا يزال هناك الكثير مما ينبغي القيام به لوضع معايير دولية محددة وقانون دولي قابل للتطبيق وبدون ثغرات في الفضاء الالكتروني، وإن وضع معايير ملزمة من الناحية السياسية هي الطريقة الأفضل لتحقيق اتفاق مبدئي مشترك بين الدول، وذلك قبل الشروع في بلورة مبادئ قانونية دولية واضحة حول العالم الالكتروني [2].

كما إن وضع قوانين ومعايير قابلة للتطبيق على الفضاء الالكتروني سيكون بدون شك عملية لا تخلو من بطء وتعثر من الناحية التنظيمية، فإن الموافقة عليها أي فهم طريقة تطبيقها وقبولها وتعزيزها كلها من طرف الدول ما تزال تسير بإيقاع بطيء، وهو ما يرجع إلى التحديات المرتبطة بتحديد المسؤوليات والتعاريف المتناقضة حول المعنى الحقيقي للأنشطة الارهابية في الفضاء الالكتروني، فضلا عن إن التوجهات السيبرانية تتطور بوتيرة أسرع بكثير مقارنة بالسياسات المتخذة للتصدي لها، الأمر الذي يضع صناع القرار في جميع أنحاء العالم أمام مجموعة كبيرة من التحديات التي لم يعّد من الممكن لهم تأجيل التعاطي معها.

2. توصيات ومقترحات: هناك عدة توصيات ومقترحات يمكن تقديمها بعد دراسة الإرهاب الإلكتروني وتحديد مخاطره، وتتضمن هذه المقترحات ما يأتي:

1 .تطوير القدرات الفنية والتكنولوجية: ينبغي على مؤسسات مكافحة الإرهاب تطوير القدرات الفنية والتكنولوجية للتعامل مع التحديات الناشئة في مجال الإرهاب الإلكتروني، ويشمل ذلك الاستثمار في تقنيات جديدة وأنظمة الأمان والحماية من الهجمات الإلكترونية، فضلا عن توظيف التقنيات الذكية والتعلم الالي والتحليل الضخم للبيانات.

---

[1] جمال علي الدهشان، المصدر السابق، ص111.

[2] المصدر السابق، ص112.

2 .تكثيف التعاون الدولي: من بين أهم الاجراءات التي تحد من الارهاب الالكتروني هو التعاون بين الدول في مكافحة الإرهاب الإلكتروني وتبادل المعلومات والخبرات والتجارب الناجحة في هذا المجال، وذلك من خلال تعزيز الشراكات الدولية وتبادل الخبرات والتقنيات الحديثة.

3 .توعية الجمهور: الخطوة الاخرى هي نشر الوعي بمخاطر الانترنت، ويستلزم ذلك قيام مؤسسات مكافحة الإرهاب التوعية بأخطار الإرهاب الإلكتروني وكيفية التعامل معها، وذلك من خلال تحسين الوعي العام بالأمور المتعلقة بالأمن السيبراني والإرشادات الأمنية.

4 .تحسين التعاون مع المجتمعات المحلية: ينبغي على مؤسسات مكافحة الإرهاب تحسين التعاون مع المجتمعات المحلية والشباب والمؤسسات ذات الصلة، وذلك من خلال التعاون في تطوير حملات التوعية والتثقيف والتدريب وتقديم الدعم الفني والتقني.

5 .تحليل البيانات والمعلومات: يتوجب على مؤسسات مكافحة الإرهاب تحليل البيانات والمعلومات والتحقق من صحتها واستعمالها لتحديد الأنشطة الإرهابية المحتملة وتحديد الأهداف المحتملة والجماعات المتطرفة وتصميم حملات مضادة تواجه تحديات الجماعات الإرهابية وتحقق النجاح في المكافحة.

6 .العمل على تشجيع الإبلاغ: على مؤسسات مكافحة الإرهاب العمل على تشجيع الإبلاغ عن الأنشطة الإرهابية المحتملة وتوفير آليات تحفيزية للإبلاغ والتعاون مع المجتمعات المحلية في هذا الصدد.

7 .العمل على تطوير القوانين واللوائح: على الحكومات والمؤسسات الدولية العمل على تطوير القوانين واللوائح المتعلقة بمكافحة الإرهاب الإلكتروني، وضمان التزام الجميع بها، وتوفير الدعم القانوني والتقني اللازم لمؤسسات مكافحة الإرهاب لضمان فعالية الجهود المبذولة في هذا المجال.

الخاتمة:

قدمَ الإنترنت خدمة للجماعات الإرهابية من إذ تضخيم الصورة الذهنية لقوة وحجم تلك المجاميع التي تمتلك عدداً قليلاً من الأفراد لديهم، أو لدى أحدهم خبرة بالإنترنت لبث رسائل إعلامية ترفد أهدافهم لشن حرب نفسية ضد مستهدفيها والدعاية لأهدافها وأنشطتها، بعيداً عن وسائل الإعلام التقليدية.

يتضح مما تقدم أن العالم بأسره يواجه تحديًا كبيرًا بسبب انتشار الإرهاب الإلكتروني، فأن التهديدات الإلكترونية لم تعّد تقتصر فقط على الهجمات الإلكترونية، بل تمتد إلى استعمال وسائل التواصل الاجتماعي

والمدونات وتطبيقات الدردشة لإساءة الاستعمال ونشر الأفكار المتطرفة، وللأسف، فإن هذه التهديدات سوف تزداد تعقيدًا وخطورة في المستقبل، كما يعمل الإنترنت على تحقيق الترابط التنظيمي بين الجماعات الإرهابية والخلايا، ويتيح لهم تبادل المعلومات والخبرات والمقترحات حول كيفية تنفيذ الأعمال الإرهابية والتخطيط والتنسيق، كما قد يتمكن الارهابيين من استعمال الإنترنت لتدمير مواقع الإنترنت المضادة واختراق مؤسسات حيوية وتعطيل خدماتها الإلكترونية.

أن مكافحة الإرهاب الإلكتروني تشكل تحدي مستمر يتطلب جهودًا مشتركة من جميع الأطراف المعنية، وحتى الآن توصلت العديد من الدراسات العلمية إلى أن التهديدات الإلكترونية المتعلقة بالإرهاب تزداد بشكل مستمر، مما يؤكد ضرورة تحليل التهديدات وتطوير القدرات الدفاعية لمواجهة هذا التحدي، وأن على الجميع العمل بشكل مشترك لتحديد النقاط الضعيفة في الأنظمة والشبكات الحيوية، وتطوير الإجراءات الأمنية والتقنيات الأمنية لتعزيز الحماية الأمنية للشبكات والأنظمة، ومن المهم أيضًا توفير التدريب والتحضير للمؤسسات والأفراد للتعامل مع التهديدات الإلكترونية، وتحسين التعاون الدولي وتبادل المعلومات والخبرات بين الدول والجهات الأمنية والمخابراتية.

كما تستلزم مكافحة الارهاب الالكتروني استعمال التقنيات المتطورة مثل الذكاء الاصطناعي والتحليل الضخم للبيانات والكشف عن الأنشطة الإرهابية، وتنفيذ التفتيش الإلكتروني لمراقبة البيانات والاتصالات الإلكترونية، مع ضرورة إنشاء آليات فعالة للتنسيق الفوري والاستجابة السريعة للهجمات الإلكترونية.

Reference:

- Dictionaries and glossaries:

1. Abu al-Fadl Jamal al-Din, Lisan al-Arab, Beirut, Dar Sader, 1955, vol. 8.

2. Ahmed Attia, The Political Dictionary, Cairo, Dar Al-Nahda Al-Arabiya, 1975.

- Books:

3. Haider Ali Hussein, US policy and the future of the international system, Baghdad, Dar Al-Kutub Al-Ilmiyya for Printing, Publishing and Distribution, 2017.

4. Adel Abdul Qadir Al-Mukinzi, Digital Media and Ways to Confront Terrorism, Riyadh, King Saud University Publishing House, 2019.

5. Abdel Salam Zakaria, Terrorism between Yesterday and Today, Dar Ghraib, Beirut, ed.

6. Abdel Fattah Bayoumi Hegazy, Criminal Evidence and Forgery in Computer and Internet Crimes, Alexandria, Al-Ma'arif Establishment, 2009.

7. Muhammad Suleiman Abu Rumman, The Secret of Attraction: (ISIS), Propaganda and Recruitment, Amman, Friedrich-Ebert-Stiftung, 2016.

8. United Nations Office on Drugs and Crime, Use of the Internet for Terrorist Purposes, New York, 2013.

9. Eric Morris and Alan Ho, Terrorism: The Threat and the Response to It, translated by Dr. Ahmed Hamdy Mahmoud, Cairo, Egyptian General Book Authority, 1991 AD.

Master's theses:

10. Salah Haider Abdel Wahed, Cyber Wars: A Study of their Concept, Characteristics, and Ways to Confront them, Master's Thesis, Amman-Jordan, Middle East University, 2021.

- Research:

11. Israa Fahmi Naji, The Concept of Terrorism in Sharia and Law, Journal of Legal and Political Sciences, a special issue of the Second International Scientific Conference of the College, University of Diyala/College of Law and Political Science, 2013.

12. Jamal Ali Al-Dahshan, Terrorism in the Digital Age (Electronic Terrorism): Its Images, Risks, and Confronting Mechanisms, International Journal of Research in Educational Sciences, Issue 3, Egypt, 2018.

13. Hassan Turki Omair, Salam Jassim Abdullah, Electronic Terrorism and its Risks in the Current Era, Journal of Legal and Political Sciences, Special Issue, University of Diyala, 2013.

14. Haider Ali Nouri, The Terrorist Crime: A Study in Light of the Anti-Terrorism Law, Lebanon, Zein Law Library, 2012.

15. Saad Atwa Al-Zant, Electronic Terrorism and Reformulating National Security Strategies, Egypt, National Center for Social and Criminological Research, 2010.

16. Adel Abdel-Sadiq, Does cyber terrorism represent a new form of international conflict, Al-Ahram Strategic, Issue 156, Center for Political and Strategic Studies, 2007.

17. Qawadra Hussein, Kahloush Mona, the role of electronic intelligence in combating cyberterrorism, Algeria, Journal of Legal and Political Research, Issue 1, 2021.