

التطرف والارهاب عبر الانترنت

¹ زينه محمد سعدون*

¹ جامعة تكريت، كلية العلوم الإسلامية، صلاح الدين (العراق)

Extremism and terrorism online

¹ Zeina Muhammad Saadoun *

¹ <https://orcid.org/0000-0002-2096-4152>

¹ Tikrit University, College of Islamic Sciences, Salah (Iraq), zinah.m.saadoun@tu.edu.iq

تاريخ الاستلام: 2025/ 01 / 31 تاريخ القبول: 2025 / 02 / 28 تاريخ النشر: 2025 / 03 / 01

الملخص:

تطورت الظاهرة الإرهابية بشتى صورها واساليبها بشكل أكثر ضراوة عما كان في الماضي، فبعدها كانت العمليات الإرهابية تتم بطرق واساليب تقليدية بحسب المتاح من أدوات للأجرام في ذلك الوقت، وأدت تلك العمليات إلى سقوط ضحايا وخسائر محدودة في الأفراد والأغراض الإنشائية والصناعية والمباني. ولكن مع التطور في المعدات والاسلحة ووسائل التكنولوجيا والتقدم العلمي في كافة هذه الوسائل أصبحت تتم بطرق بالغة الدقة والتطور مستفيدة من التكنولوجيا الحديثة، وأضحت تلك العمليات يترتب عنها خسائر جسيمة تكاد تعادل خسائر الحروب النظامية بين الدول، سواء في الأرواح أو العتاد أو الممتلكات والمنشآت، هدفت الدراسة الى بيان مفهوم الإرهاب والتطرف وتوضيح الفرق بين مفهوم الإرهاب والتطرف وتحديد الأسباب التي أدت إلى ولادة الإرهاب والتطرف. وتوصلنا الى نتائج منها على سبيل المثال أن الإرهاب لا دين له ولا وطن، ولا انتماء حقيقي للعقائد الدينية والقيم الروحية والمشاعر الانسانية. أن الدين الإسلامي والأديان والشرائع السماوية بريئة من هذه الظاهرة الإرهابية الإجرامية الشنعاء. يعد الإرهاب بحق هو أخطر عدو يواجهه العالم اليوم والبشرية جمعاء. كلمات مفتاحية: الحروب الدولية الحديثة، الارهاب والتطرف، عبر الانترنت، المعلوماتية.

Abstract:

The terrorist phenomenon, in all its forms and methods, has developed in a more ferocious manner than it was in the past. Terrorist operations were carried out in traditional ways and methods according to the criminal tools available at that time. These operations led to casualties and limited losses in individuals, constructional and industrial objects, and buildings. But with the development of equipment, weapons, means of technology, and scientific progress in all of these means, they have become carried out in very precise and sophisticated ways, taking advantage of modern technology, and these operations have begun to result in huge losses that are almost equivalent to the losses of regular wars between countries, whether in lives, equipment, property, or installations. The study aimed to explain the concept of terrorism and extremism, clarify the difference between the concept of terrorism and extremism, and identify the

* المؤلف المرسل.

* Corresponding author.

reasons that led to the birth of terrorism and extremism. We reached conclusions, including, for example, that terrorism has no religion, no homeland, and no true affiliation to religious beliefs, spiritual values, and human feelings. The Islamic religion, religions, and divine laws are innocent of this heinous criminal terrorist phenomenon. Terrorism is truly the most dangerous enemy facing the world and all of humanity today.

Keywords: modern international wars; terrorism and extremism; via the Internet; informatics.

مقدمة:

تطورت الظاهرة الإرهابية بشتى صورها واساليبها بشكل أكثر ضراوة عما كان في الماضي، فبعدها كانت العمليات الإرهابية تتم بطرق واساليب تقليدية بحسب المتاح من أدوات للأجرام في ذلك الوقت، وأدت تلك العمليات إلى سقوط ضحايا وخسائر محدودة في الأفراد والأغراض الإنشائية والصناعية والمباني. ولكن مع التطور في المعدات والاسلحة ووسائل التكنولوجيا والتقدم العلمي في كافة هذه الوسائل أصبحت تتم بطرق بالغة الدقة والتطور مستفيدة من التكنولوجيا الحديثة، وأضحت تلك العمليات يترتب عنها خسائر جسيمة تكاد تعادل خسائر الحروب النظامية بين الدول، سواء في الأرواح أو العتاد أو الممتلكات والمنشآت، فقد قيل بحق حديثاً " أن شبكات الإنترنت هي خير مثال في الزمن المعاصر، يوضح لنا كيف يمكن للإرهابيين استخدامها في إدارة عملياتهم الإرهابية المختلفة، ويمارسوا أنشطتهم الإجرامية ، على نحو عابر للحدود والقارات، ولذلك يجب على جميع دول العالم أن يتصدوا متضامين لهذه المخاطر العابرة للحدود أيضاً. (1)

يعد الفضاء الإلكتروني عنصر جذب مهماً للتنظيمات الإرهابية على اختلاف أنواعها وتباين أفكارها، نظراً لما يتيح لها من وسيلة إعلام عالمية هي في الوقت نفسه سلاح خطير، وتقوم هذه التنظيمات باستخدام الفضاء الإلكتروني في الدعاية والتجنيد والتمويل، وجمع المعلومات، وتنسيق الهجمات الإرهابية، وحشد المتعاطفين من مختلف دول العالم (2).

ويلاحظ أنه من خلال هذا المظهر الجديد لهذه العمليات الإرهابية، فقد تطور شكله ونمطه في عمليات أخرى ترتبط بالتطور التكنولوجي وتنقية المعلومات، فأخذ أيضاً نمط تدمير المعلومات من خلال شبكات الاتصال الدولية، فقد أصبح بإمكان جماعات أو أشخاص تحركهم دوافع سياسية وحتى شخصية، بل وبإمكان مراهقين تحركهم اندفاعهم وفضولهم وهم داخل غرفهم ومكاتبهم وأمام حواسيبهم، تدمير معلومات وبرامج ضخمة لكبريات الشركات والمؤسسات الوطنية والدولية البعيدة عنهم كل البعد.

مشكلة البحث وأسئلته:

تعتبر مشكلة التطرف والإرهاب من أكثر القضايا إثارة للجدل والاهتمام من قبل النخب الفكرية ان نمو مثل هذه الظواهر بين المجتمعات وانتقالها إلى أطوار وأشكال جديدة لم تكن موجودة من قبل يدعونا إلى قراءة أكثر تعمقاً، بعيداً عن التبسيط الذي قد يخل بالتحليل الدقيق لتلك الظواهر. إذ أن اختلاف الناس في فهم مدلول هذا المصطلح ما بين غالي متشدد ومتوسط ومفرط متساهل، فكل شخص يفسر هذا المصطلح على حسب مدرسته الفكرية وميوله وهواه ومبادئه وأهدافه وما يرمي إليه من إطلاق هذه العبارة حتى أنك بعد التأمل تجد تفاوتاً كبيراً بين المثقفين والمتخصصين في معنى والمدلول وأسباب الذي تم وضعه للتطرف والإرهاب، وعليه ستقوم الدراسة بالإجابة عن التساؤلات الآتية:

1. لماذا شبح الإرهاب هو أخطر عدو يواجهه العالم اليوم؟
2. لماذا الإرهاب؟ ومن المستفيد منه؟ ومن يقف وراءه؟ وماهي أسبابه وأشكاله؟

3. ما هي التحديات التي تواجه الأمن حيال العمليات الإرهابية ومواجهتها والتي تحدث من أن للآخر؟
4. هل الإجراءات الأمنية التي أقرتها الجهات المعنية لمكافحة الإرهاب بالمنظمات الدولية والدول بالوقت الحالي كافية لمنع الأعمال الإرهابية؟
5. هل تمكنت العصابات والجماعات الإرهابية من رصد نقاط الضعف الأمنية، وتبنوا تكتيكات جديدة أكثر تعقيداً لتحقيق أهدافهم الإرهابية؟
6. ما هي الأسباب التي أدت إلى ولادة الإرهاب؟
7. ما هي طرق مكافحة وعلاج ظاهرة الإرهاب والتطرف؟

أهمية البحث:

تكمن أهمية هذا البحث من أهمية الموضوع الذي يتناوله وهو ظاهرة الإرهاب والتطرف في المجتمع، إذ أن ظاهرة التطرف والإرهاب من أكثر القضايا الراهنة التي حظيت باهتمام الشعوب والحد منها ومكافحتها، إذ أن خطورتها أصبحت شديدة، ولها تجاذبات داخلية وخارجية، عربية وإقليمية ودولية، لأن التطرف أصبح كونياً، إذ أنه موجود في مجتمعات متعددة ولا ينحصر في دين أو دولة أو شعب أو لغة أو ثقافة أو هوية، وإن اختلفت الأسباب باختلاف الظروف والأوضاع، ومن هنا جاء هذا البحث لتسليط الضوء بشكل مختصر على ظاهرة التطرف والإرهاب في المجتمع، كما تكمن أهمية البحث مما يلي:

- تنبثق أهمية بحث ظاهرة الإرهاب بالدراسة الوصفية والتحليلية، بمحاولة إلقاء الضوء على مدى خطورة الإرهاب على أمن البلاد واستقراره بصفة عامة في شتى أنحاء المعمورة، وعلى أمن المجتمع بكل مقوماته بصفة خاصة وتقدير مدى ما يفرضه الإرهاب على الساحة السياسية والأمنية على المستوى الوطني والإقليمي والدولي.
- وكذلك تسليط الضوء على الجهود الكبيرة التي تبذل من الجهات وأجهزة الأمنية والشرطية لمواجهة الأعمال الإرهابية في الزمن المعاصر.

أهداف البحث:

تتمثل أهداف البحث فيما يلي:

- بيان مفهوم الإرهاب والتطرف.
- توضيح الفرق بين مفهوم الإرهاب والتطرف.
- تحديد الأسباب التي أدت إلى ولادة الإرهاب والتطرف.
- تحديد وسائل ارتكاب جريمة الإرهاب الإلكتروني.
- إلقاء الضوء على ملامح الإستراتيجية الأمنية لمواجهة مثل هذه العمليات الإرهابية.

منهج البحث المستخدم (المنهجية البحثية):

اعتمدت خطة البحث على الدراسة الوصفية التحليلية بشأن إبراز أوجه مواجهة العمليات الإرهابية، وانتهاج المنهج الوصفي الذي يسعى أساساً إلى توضيح ووصف وتشخيص العمليات الإرهابية.

المبحث الأول

مفهوم الإرهاب الإلكتروني

إنَّ أبرز أشكال الإرهاب المعاصرة، هو الإرهاب الإلكتروني أو ما يسمى الإرهاب المعلوماتي، أو الإرهاب عبر الإنترنت، والذي يرتبط بالمستوى المتقدم للغاية الذي باتت وسائل الاتصالات وتقنية المعلومات تلعبه في جميع مجالات الحياة في العالم بأسره، ومن خلال الأنظمة الإلكترونية والشبكات المعلوماتية اتخذ الإرهاب أبعاداً جديدة، وازدادت خطورته على المجتمعات الدولية (3)، وينطلق الإرهاب الإلكتروني من عالمين، العالم المادي (Physical world)، والعالم الافتراضي (Virtual World)، والذي من خلاله تتم عمليات الإرهاب الإلكتروني والتدمير والتخريب، ويشير العالم المادي إلى قضايا وظواهر متعددة مثل: الطاقة، والضوء والظلام، والبرودة والحرارة، وجميع الأمور المادية والحيز الذي يعيش فيه المجتمع، ويمارس الوظائف والأدوار من خلاله، أما العالم الافتراضي فيشير إلى التمثيل الرمزي والمجازي للمعلومات، وهو المكان الذي تعمل به البرامج والأنظمة الإلكترونية وتنقل فيه البيانات . (4) ولتوضيح هذا الشكل الجديد من الإرهاب لا بد أولاً من تعريفه وبيان خصائصه وأهدافه، وذلك على النحو الآتي:

المطلب الأول: تعريف الإرهاب الإلكتروني.

إذا كان الإرهاب بمفهومه التقليدي يعني قيام بعض الأشخاص سواء أكانوا أفراد أم جماعات باغتيال شخصيات مهمة وبارزة في المجتمع أو الاستيلاء على طائرة أو سفينة بوجه غير قانوني أو تفجير قنبلة في مكان ما ، فإن الإرهاب المعلوماتي وبفضل التقدم العلمي الذي تحقق ومازال يتطور في مجال تقنية المعلومات يقصد به استخدام نظام المعلومات والشبكات المعلوماتية للقيام بأعمال إرهابية، حيث تستفيد الجماعات الإرهابية من الخدمات التي تقدمها شبكة الإنترنت لتنفيذ عملياتهم الإرهابية التي تستهدف إلحاق الضرر بالبنية الأساسية للدولة وتدمير أنظمة الاتصالات والطيران ومحطات الطاقة..... إلخ، لذلك سارعت الجماعات الإرهابية إلى استخدام هذه التقنية الحديثة فبادرت إلى إنشاء المواقع الإلكترونية والمنتديات التحوارية وما يسمى بالكليات الإلكترونية المفتوحة وهي مواقع الكترونية تقوم الجماعات الإرهابية من خلالها بنشر المعلومات المتعلقة بكيفية صنع المتفجرات والعبوات الناسفة وطرق تنفيذ الاغتيالات وحرب العصابات فضلاً عن تقنيات الإرهاب المعلوماتي كطرق اقتحام المواقع الإلكترونية للجهات المعادية وتدميرها وكذلك التسلسل داخل شبكة الإنترنت وسرقة البريد الإلكتروني ويتم ذلك عن طريق نشر محاضرات ودروس في مواقع خاصة للجماعات الإرهابية لشرح كيفية القيام بهذه العمليات وتوضيحها، فضلاً عن نشر كتب باللغتين العربية والإنكليزية عن أنواع الأسلحة كافة (5).

إنَّ أول من انتبه إلى ظاهرة الإرهاب الإلكتروني هم الأمريكيون فقد أمر الرئيس الأمريكي الأسبق بيل كلينتون عام 1996 بتشكيل لجنة خاصة هدفها حماية البنية التحتية للولايات المتحدة الأمريكية للحيلولة دون تعرضها لهجمات إرهابية محتملة (6)، كما أصدر الرئيس الأمريكي الأسبق بوش في 16 - تشرين الأول - 2001 قراراً يتضمن تأسيس مجلس لحماية البنية الأساسية الحيوية كالسدود والجسور والأنفاق ومصادر الطاقة الخ ويقوم رئيس المجلس بتقديم تقارير إلى مساعد الرئيس لشؤون الأمن القومي ومساعد الرئيس لشؤون الأمن الداخلي، كما أنشأت وكالة الاستخبارات المركزية مركزاً يتكون من ألف خبير لتشكيل قوة ضاربة لمواجهة الإرهاب الإلكتروني (7).

كما قسم الإرهاب الإلكتروني لثلاثة أنواع: إرهاب الكتروني ضد الأفراد، وإرهاب الكتروني ضد المؤسسات، وإرهاب إلكتروني ضد الدول ويعرفه بأنه "إمكانية النفاذ إلى شبكات التحكم في المرافق العامة مما يتسبب في الشلل التام للبنى التحتية الأساسية بل واحتمال تدميرها بالكامل (8)، ونجد أن هذا التعريف غير جامع مانع وذلك لأن الإرهاب الإلكتروني لا

يقتصر على الدخول أو النفاذ لشبكات المرافق العامة للدولة وإنما يتعدى ذلك بكثير. وهناك آخر يطلق على الإرهاب الإلكتروني (الإرهاب عبر الإنترنت).

المطلب الثاني: الإرهاب الإلكتروني (أنواعه، أسبابه، خصائصه).

أصبح الإرهاب الإلكتروني خطراً يهدد العالم بأسره، إذ أنّ خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق (9). ومع هذا الانتشار الكبير للجرائم الإرهابية المعلوماتية فإن ظهرت بأشكال متنوعة ومختلفة، ولها أسبابها الخاصة وخصائصها التي تتميز بها عن الإرهاب التقليدي، ومن خلال هذا المطلب سيتم توضيح هذه الجوانب على النحو الآتي:

الفرع الأول: أنواع الإرهاب الإلكتروني

اختلفت التقسيمات التي وضعها فقهاء القانون لأنواع الإرهاب وذلك لأسباب عديدة أهمها اختلاف انتماءاتهم واختلاف أفكارهم ووجهات نظرهم، لكن الإرهاب الإلكتروني يمكن تقسيمه على طريقة مغايرة وذلك استناداً إلى معيارين موضوعيين، وهما: الأول: من حيث الأشخاص الذين يمارسون الإرهاب المعلوماتي وهم إما أفراد أو جماعات أو دول، والمعيار الثاني هو من حيث المضمون، وعلى ذلك يمكن توضيح هذه الأنواع وفقاً للمعيارين السابقين على النحو الآتي:

أولاً: الإرهاب الإلكتروني من حيث مرتكبيه.

من الواضح أن الإرهاب المعلوماتي أما يقوم به فرد أو جماعة أو دولة، وعلى ذلك يكون التقسيم وفق هذا المعيار على النحو الآتي:

- 1- الإرهاب الإلكتروني الفردي: وهو الذي يرتكبه فرد تحقيقاً لأهداف محددة، ويمكن أن يقع من فرد واحد، وهذا ما أشار له قانون منع الإرهاب الأردني من خلال المادة (1/3) بأنه: " تحظر الأعمال الإرهابية ويعتبر في حكمها الأعمال التالية: أ- القيام بأي وسيلة مباشرة أو غير مباشرة بتقديم الأموال أو جمعها أو تدبيرها بقصد استخدامها لارتكاب عمل إرهابي أو تمويل الإرهابيين سواء وقع العمل أو لم يقع داخل المملكة أو خارجها متعلق بمواطنيها أو مصالحها في الخارج". حيث يمكن عن طريق الوسائل الإلكترونية تقديم الدعم المالي أو جمعه أو حث مجموعة من الأفراد على القيام بأعمال إرهابية داخل المملكة أو خارجها.
- 2- الإرهاب الإلكتروني الجماعي: وهو الذي ترتكبه جمعة تحقيقاً لأهداف محددة وهو ما نصت عليه كذلك المادة (3/ج) من قانون منع الإرهاب الأردني بأنه: "تحظر الأعمال الإرهابية ويعتبر في حكمها الأعمال التالية: ج- تأسيس أي جماعة أو تنظيم أو جمعية أو الانتساب إليها بقصد ارتكاب أعمال إرهابية في المملكة أو ضد مواطنيها أو مصالحها في الخارج". حيث يمكن القيام بهذه الأعمال بواسطة الوسائل الإلكترونية.
- 3- الإرهاب الإلكتروني الدولي: وهو الذي تنفذه دولة أو أكثر ضد مواطنيها أو ضد دولة أخرى وهذا النوع يدخل فيه العنصر الدولي(10).

ثانياً: الإرهاب الإلكتروني من حيث موضوعه.

يتفرع الإرهاب الإلكتروني من حيث موضوعه إلى عدة أنواع منها:

- 1- الإرهاب الإلكتروني الفكري: حيث تعد الشبكات الإلكترونية الملاذ الآمن للإرهابيين، حيث تشكل شبكة الإنترنت أيضاً الملتقى الحر لهم، فأخذ الإرهابيون ينشرون مبادئهم وأفكارهم الضالة والهدامة عبر هذه الشبكة وبوساطة

غرف المحادثة لكسب أكبر عدد ممكن من الناس المتعاطفين معهم ولتجنيدهم في جماعاتهم ومنظماتهم الإرهابية (11).

2- الإرهاب الإلكتروني الديني: لما كان الدين عقيدة يعنقها الناس فلا شك أن هناك من يؤيدها على الطرف الآخر من يعارضها، وقد استغل الإرهابيون شبكات الإنترنت ومواقع التواصل الاجتماعي كميدان افتراضي لنشر أفكارهم الدينية المتطرفة والدعوة للانتقام من يحارب أو يعارض هذه الأفكار. (12)

الفرع الثاني: الأسباب الخاصة للإرهاب الإلكتروني.

كما أشرنا سابقاً أن الإرهاب التقليدي له أسباب متعددة ومتنوعة ومتشابكة، وهي عينها أسباب ظاهرة الإرهاب عموماً حيث تتداخل الدوافع الشخصية مع الدوافع الفكرية والسياسية والاقتصادية والاجتماعية، أما الإرهاب الإلكتروني فله أسباب خاصة، يمكن تلخيصها على النحو الآتي:

1. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق؛ حيث إن شبكات المعلومات مصممة بحسب الأصل بشكل مفتوح دون حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين. ويمكن للمنظمات الإرهابية استغلال الثغرات المتواجدة في الأنظمة الإلكترونية والشبكات المعلوماتية، في التسلسل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية.
2. عدم وضوح الهوية الرقمية للمستخدم يجعل الفرصة سانحة للإرهابيين، حيث يستطيع محترف الحاسوب أن يتخفى تحت شخصية وهمية، ويشن بالتالي هجومه الإلكتروني بعيداً عن مراقبة السلطات العامة.
3. سهولة استخدام شبكة المعلومات وقلة التكلفة مما هيا للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون حاجة إلى مصادر تمويل. فشن هجوم إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة، فصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب الإرهاب الإلكتروني، لأنها تساعد المجرم على الإفلات من العقوبة.
4. صعوبة اكتشاف وإثبات الجريمة الإرهابية، خاصة في مجال جرائم الاختراق، مما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته.
5. غياب السيطرة والرقابة على الشبكات المعلوماتية. ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى (13).

الفرع الثالث: خصائص الإرهاب الإلكتروني وأهدافه.

الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي تميزه عن الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق بعض الأغراض غير المشروعة، وذلك على النحو التالي:

أولاً: خصائص الإرهاب الإلكتروني التي تميزه عن الإرهاب العادي:

هناك مجموعة من الخصائص التي ينفرد بها الإرهاب الإلكتروني تميزه عن الإرهاب التقليدي، ويمكن تلخيص أهم هذه الخصائص على النحو الآتي:

1. لا يحتاج الإرهاب الإلكتروني في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية فقط ومزود ببعض البرامج اللازمة.

2. يتسم الإرهاب الإلكتروني بأنه عابر للدول والقارات، وغير خاضع لدولة معينة، إضافة لصعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الجهات الأمنية والقضائية في التعامل مع مثل ذلك النوع من الجرائم.
3. صعوبة إثبات جرائم الإرهاب الإلكتروني، لغياب الدليل الرقمي من ناحية، وسهولة إتلافه وتدميره من ناحية أخرى.
4. أن مرتكب الإرهاب الإلكتروني يكون في العادة من المتخصصين في مجال تقنية المعلومات، أو لديه - على الأقل - قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية (14).

ثانياً: أهداف الإرهاب الإلكتروني هي:

ما يميز الإرهاب الإلكتروني بأنه يسعى الإرهابيون من خلاله إلى تحقيق جملة من الأهداف مستغلين في ذلك سهولة استخدام مواقع الإنترنت ومواقع التواصل الإجتماعية التي أصبحت هدفاً لهم في تنفيذ عملياتهم الإرهابية، حيث تكمن أهم أهدافهم بما يلي:

1. نشر الخوف والرعب بين الأشخاص والدول، وتعريض سلامة المجتمع وأمنه للخطر.
2. الإخلال بالأمن المعلوماتي وزعزعة الطمأنينة.
3. تدمير البنى التحتية المعلوماتية، والإضرار بوسائل الاتصالات وتقنية المعلومات.
4. الاستيلاء على الأموال (15).

المبحث الثاني

وسائل ارتكاب جريمة الإرهاب الإلكتروني

لبيان أبرز وأهم مظاهر الإرهاب الإلكتروني وأشكاله فإنه من المناسب أن نقسم هذا المبحث إلى خمسة مطالب، حيث تناولنا في المطلب الأول تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، وفي المطلب الثاني إنشاء المواقع الإرهابية الإلكترونية، وفي المطلب الثالث تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وفي المطلب الرابع التهديد والترويع الإلكتروني، وأخيراً وفي المطلب الخامس التجسس الإلكتروني، وذلك على النحو الآتي:

المطلب الأول: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية.

إن كثيراً من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناولها بين القائمين بالعمليات الإرهابية والمخططين لها، ويقوم الإرهابيون كذلك باستغلال البريد الإلكتروني والاستفادة منه في نشر أفكارهم والترويع لها، والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية (16) وعليه من أبرز الوسائل ما يلي:

أولاً: الاتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم، نظراً لقلّة تكاليف الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال والتخفي، وذلك عن طريق البريد الإلكتروني أو المواقع والمنتديات وغرف الحوار الإلكتروني، حيث يمكن وضع رسائل مشفرة تأخذ طابعا لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته، كما لا تترك أثرا واضحا يمكن أن يدل عليه (17).

ثانياً: جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما انها تعتبر موسوعة إلكترونية شاملة متعددة الثقافات، ومتنوعة المصادر، وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية، والمعلومات المختصة بسبل مكافحة الإرهاب، ونحو ذلك من المعلومات التي تعتبر بمثابة الكنز الثمين بالنسبة للإرهابيين؛ نظرا لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية (18).

ثالثاً: التخطيط والتنسيق للعمليات الإرهابية

العمليات الإرهابية عمل على مستوى عالي من التعقيد والصعوبة، فهي تحتاج إلى تخطيط محكم، وتنسيق شامل، وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية؛ حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيدا عن أعين الناظرين، مما يسهل على الإرهابيين ترتيب تحركاتهم، وتوقيت هجماتهم. (19)

رابعاً: الحصول على التمويل

ومن خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية، من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة، والقلوب الرحيم ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة رسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية، بطريقة ذكية وأسلوب مخادع، بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية (20).

خامساً: التعبئة وتجنيد الإرهابيين

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي بها، كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها. ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدى من لديهم ميول واستعداد للانخراط في

الأعمال التدميرية والتخريبية، مما يوفر لديها قاعدة ممن تجمعهم نفس الأفكار والتوجهات، فيسهل تجنيدهم لتنفيذ هجمات إرهابية في المستقبل (21). إن استقدام عناصر جديدة داخل التنظيمات الإرهابية، يحافظ على بقائها واستمرارها؛ لذا فإن الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي، وعبارات حماسية براقية، وذلك من خلال غرف الحوار والمنتديات والمواقع الإلكترونية.

سادساً: التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية إلى تدريب خاص، ويعد التدريب من أهم هواجس التنظيمات الإرهابية. وقد أنشئت معسكرات تدريبية سرية - كما ظهر بعضها في وسائل الإعلام - لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر، ويمكن اكتشافها ومداهمتها في أي وقت، لذا فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي، كما قامت بعض 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). وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة المدمرة.

سابعاً: إصدار البيانات الإلكترونية

تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة، وذلك عن طريق المواقع الإلكترونية أو بواسطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وساحاته، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات، ووصولها إلى مختلف فئات المجتمع ((23). وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة، فتارة ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي، وأحياناً تكون للتهديد والوعيد بشأن هجمات إرهابية معينة، في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار أو تصريحات صادرة من جهات أخرى (24).

المطلب الثاني: إنشاء المواقع الإرهابية الإلكترونية.

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات (Internet) ليث أفكارهم الضالة، والدعوة إلى مبادئهم المنحرفة، وإبراز قوة التنظيم الإرهابي، وللتعبئة الفكرية وتجنيدهم إرهابيين جدد، ولإعطاء التعليمات والتلقين الإلكتروني، وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشأن هجمات إرهابية، فقد أنشئت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية الفتاكة، ولشرح طرق اختراق البريد الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات، ونحو ذلك (25).

إذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالفنونات التلفزيونية والإذاعية صعبا بالنسبة للإرهابيين، فإن إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات (Internet)، لخدمة أهدافهم وترويج أفكارهم الضالة أصبح سهلا وممكنا، ولذا فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية، وهي بمثابة المقر الافتراضي لها (26) إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الإلكتروني غدا، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمنوا انتشاراً أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت بعضها للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها (27).

المطلب الثالث: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية.

تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالباً، 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 (28). والمقصود بالتدمير هنا الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي (Server - PC)، أو مجموعة نظم مترابطة شبكية (Intranet)، بهدف تخريب نقطة الاتصال أو النظام. وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراقها بشكل دائم، فالمتغيرات التقنية، وإمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (source open)، سواء كان ذلك في مكونات نقطة الاتصال أو في النظم أو في الشبكة أو في البرمجة، جعلت الحيلولة دون الاختراقات صعباً جداً، بالإضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الامكانيات والقدرات ما ليس لدى الأفراد (29).

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية، ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسبة الإلكترونية والشبكات المعلوماتية (30). كما يمكن تصور هجومات إلكترونية على أحد المواقع الإلكترونية بقصد الاستيلاء على محتوياتها، كما لو قامت إحدى التعليمات الإرهابية بشن هجومات إرهابية عن طريق الشبكة المعلوماتية على أحد البنوك والمصارف المالية بقصد السرقة والاستيلاء على الأموال وذلك من أجل تمويل ذلك التنظيم الإرهابي.

ومن المتصور قيام أحد التنظيمات الإرهابية باختراق مواقع معينة بقصد السيطرة والتحكم فيها، وقد هيمن الذعر على المختصين بمكافحة الإرهاب الإلكتروني عندما تمكن أحد الأشخاص من السيطرة على نظام الحاسبة الإلكترونية في أحد المطارات الأمريكية الصغيرة، وقام بإطفاء مصابيح إضاءة ممرات هبوط الطائرات. ومن المتصور شن هجومات إلكترونية على البنية التحتية للشبكة المعلوماتية بقصد تدميرها وتوقفها عن العمل، مما يحدث أثارا مادية اقتصادية وسياسية

وثقافية خطيرة، لأن توقف الشبكة المعلوماتية يعني توقف القطاعات والمرافق الحيوية عن العمل، بالإضافة إلى توقف الحكومات الإلكترونية عن عملها، وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية (31). وفي الواقع إن هناك أسبابا لوقوع عملية تدمير المواقع ومن هذه الأسباب ما يأتي: (32)

1. ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسر وتخمين الكلمات السرية من المخترق.
2. عدم وضع برامج حماية كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق للموقع.
3. استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج وأنظمة غير موثوقة أمنيا ولا يتم تحديثها باستمرار.
4. عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية. تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.
5. عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة فيه، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها، ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في الآونة الأخيرة، ويعد عام 2002م من أكثر الأعوام اختراقا، فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات.(33).

المطلب الرابع: التهديد والترويع الإلكتروني.

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، ومن خلال الشبكة العالمية للمعلومات (Internet)، وتتعدد أساليب التهديد وتتنوع طرقه، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي وإبراز قوة التنظيم الإرهابي من ناحية أخرى (34). والمقصود بالتهديد: الوعيد بشر، وزرع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضررا ما سيلحقه أو سيلحق أشخاصا أو أشياء له بها صلة، فقد يلجأ إرهابي الإرهاب الإلكتروني إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية؛ بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد (E-mails-)، وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية (35). ولقد تعددت الأساليب الإرهابية في التهديد، فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، ونحو ذلك.

المطلب الخامس: التجسس الإلكتروني

أصبح التجسس في العصر الحالي شاملاً لمختلف المجالات فلم يعد يقتصر على النواحي العسكرية والحربية، وإن كان هذا النوع من التجسس يمثل أهم أنواع التجسس وأخطرها، إلا أن المعلومة المطلوبة الآن تختلف عنها في الماضي، فلم تعد أعداد الجيوش وتجهيزاتها التقليدية من الأمور السرية، ولكن هناك تجسس عسكري يكون بصورة عميقة خصوصاً بين الدول الكبرى، فتسعى هذه الدول للحصول على أسرار حربية تكنولوجية، كي تقف على مدى التقدم الذي وصلت إليه غيرها من الدول، خاصة بأن تلك الدول يوجد بينها سباق في التسليح المتقدم النووي والكيمياوي والإشعاعي(36)، وتكمن أهم صور التجسس بشكل عام في النقاط التالية:

1. التجسس السياسي: قد يكون التجسس سياسياً لمعرفة المواقف السياسية لصناع القرار في الدولة والمعلومات التي تتعلق بالسياسة الداخلية والخارجية المتبعة، أو التي تنوي الدول السير عليها، وقد يكون التجسس معنوياً ونفسياً لشعوب الدول وقادتها، ومعرفة مواطن القوة والضعف في شخصية أفراد الشعب، وعوامل الوحدة والتفرقة، والقيم السائدة في المجتمع، والتيارات الحزبية والدينية، مدى تأثيرها في الأزمات، ومقدار العزيمة لدى شعب دولة ما.
2. التجسس الاقتصادي: وذلك لمعرفة موارد الدولة وحجم إنتاجها، وميزانها التجاري والاحتياطي لديها، وكذلك معرفة المرافق الاقتصادية الحيوية لديها ومواقعها، وكذلك ديونها الخارجية(37).
3. التجسس الصناعي: ينصب هذا النوع من التجسس على المعلومات الصناعية والعلمية من خلال معرفة أسرار الصناعات والأبحاث العلمية خصوصاً إذا كانت هذه الصناعات ترفد الدفاع الوطني، فهناك شركات تساهم في الإنتاج الحربي وتطوير الأسلحة، وقد يكون التجسس العلمي لمعرفة الدراسات العلمية في المجالات الزراعية أو الهندسية أو الصحية(38).

وترى الباحثة أن جميع المعلومات السرية السابقة سواء كانت عسكرية أو سياسية أو اقتصادية من الممكن أن تكون على شكل محتوى إلكتروني، وحتى لو كان هذا المحتوى محاط بوسائل الأمن المعلوماتي، فإن المخزون الإلكتروني الوجود فيه عرضة للتجسس الإلكتروني على تلك المعلومات واختراقها والحصول عليها وإفشائها. وهناك أنواع متعددة من التجسس الإلكتروني، وتتمثل أهم أنواع التجسس الإلكتروني في الأنواع التالية، وهي:

1. التجسس الإلكتروني على الأفراد: يعتبر أبسط أنواع التجسس الإلكتروني ما هو معروف ومنتشر بين الأفراد وهم مستخدمي الكمبيوتر الشخصي بشكل عام، وهذا النوع من التجسس يستخدم فيه الهكر أو من يريد التجسس برامج خارجية مبنية على أساس العميل والخادم، ويشترط في هذه العملية أن يكون برنامج الخادم يعمل في النظام الهدف ليقوم بعد ذلك الهكر بالاتصال من خلال برنامج العميل لتبدأ عملية التجسس، وهذا النوع من برامج التجسس يعمل على الكمبيوتر الشخصي، كما أنه مع انتشار الأجهزة الذكية والموبايلات في الآونة الأخيرة فقد ظهرت لهذه الأنظمة برامج تجسس مشابهة للفكرة السابقة، وهذا ما جرمه المشرع الأردني في قانون الجرائم الإلكترونية في المادة (3) الفقرة (أ)، وفي المادة (4).
2. التجسس من خلال الشبكات المحلية: بالإضافة للنوع الأول من أنواع التجسس على الأفراد فقد ظهرت أنواع أخرى للتجسس الإلكتروني في الشركات والجهات التي تستخدم الشبكات بكل أنواعها الصغيرة والكبيرة اللاسلكية والسلكية، وهناك برامج متعددة في هذا النوع التجسس تقوم على اصطيد البيانات المرسلة داخل الشبكة وتعمل على مراقبة اغلب البروتوكولات ولذلك فإن أي مستخدم بداخل شبكة محلية يستطيع الوصول والتجسس على بقية المستخدمين.

3. التجسس الإلكتروني الدولي والخارجي: ويكون ذلك عن باستخدام طرق عديدة من أبرزها التجسس من خلال النظام العالمي لاتصالات الخليوي (GSM) ونظام الثريا، أو التجسس الإلكتروني عن طريق الموجات والترددات، أو من خلال الأقمار الصناعية(39).

الخاتمة

وفي نهاية هذا البحث يمكننا القول أن ظاهرة الإرهاب أصبحت بحق اليوم أهم وأكبر تحدي يواجه كل دول العالم حاضراً ومستقبلاً، ومما لا شك فيه، أن قضية الإرهاب في عصرنا أصبحت من أهم القضايا التي تشغل بال الأوساط الدولية بأجمعها دون استثناء ولو كانت على درجات متفاوتة. والإرهاب، كلمة لها معنى ذو صور متعددة تجمعها صفات مشتركة: ترويع الأمنين، إزهاق الأنفس البريئة، إتلاف الأموال، وهتك الأعراض، وتفريق الجماعات واستغلال الشباب وتجنيدهم وزجهم في مواجهات وصراعات ترتكب فيها أفعال مخزية. وقد تعددت أساليبه ومظاهره في السنوات الأخيرة ولجأ الإرهابيون إلى استخدام وسائل العلم الحديث وتطبيقاته في سبيل الوصول إلى أغراضهم وتحقيق أهدافهم، ومما لا شك فيه، أن فساد الاعتقاد هو العامل الأول للإرهاب العالمي، وبناءً على ما تقدم توصل الباحث إلى مجموعة من النتائج والتوصيات والتي يمكن إجمال أهمها.

أولاً: النتائج:

1. أن الإرهاب لا دين له ولا وطن، ولا انتماء حقيقي للعقائد الدينية والقيم الروحية والمشاعر الإنسانية.
2. أن الدين الإسلامي والأديان والشرائع السماوية بريئة من هذه الظاهرة الإرهابية الإجرامية الشنعاء.
3. يعد الإرهاب بحق هو أخطر عدو يواجهه العالم اليوم والبشرية جمعاء.
4. أن الفهم الصحيح لآيات القرآن الكريم وأحاديث رسولنا الكريم عليه الصلاة والسلام وهو قمة الاعتدال والوسطية التي أرشدنا إليها صلى الله عليه وسلم. فما عُرض على الرسول صلى الله عليه وسلم عدة أمور إلا أختار أوسطهم.
5. أن التعاون بين جمهور المواطنين، ورجال الأمن والدولة بتفاهم وحب الوطن وإخاء، يساعد كثيراً على دحض أية ظواهر إجرامية بالمجتمع.
6. وجود إرهاب فردي من بعض الأفراد بصورة غير ممنهجة، كظاهرة إرهابية جديدة تحت مسمى الذئاب المنفردة ثم تطور المسمى إلى الخيل المسومة.

ثانياً: التوصيات:

1. يجب تحديد العناصر الإرهابية (جماعات. أفراد) ووضع قاعدة بيانات خاصة بكل فرد وكل جماعة على أن يتم تحديدها أولاً بأول. حتى يمكن عمل الترتيب اللازمة للقبض عليها أو صدها ومنعها من ارتكاب أي عمل إرهابي محتمل.
2. يجب أن تتوحد جهود علماء النفس الإرهاب مع علماء الجريمة والعقاب وعلماء الاجتماع الجنائي من أجل دراسات أعمق واشمل لتحليل تلك الظاهرة الإرهابية الإجرامية الخطيرة.
3. يجب على جميع الجهات بالدولة والمسؤولة عن الوعظ والإرشاد تعميق الوازع الديني السليم النابع من القرآن الكريم والسنة النبوية الشريفة وتعزيزها في النفس البشرية.

4. دعوة والتنسيق مع العلماء والفقهاء بإجراء الحوار البناء المستمر مع الشباب في المجتمع وتصحيح المفاهيم الخاطئة، والفهم السليم لغاية ومقاصد الإسلام، والحرص كل الحرص على توطيد مفاهيم الوسطية والاعتدال في الدين.
5. تنشئة الأجيال تنشئة سليمة. والحصول دوماً على الفتاوى من أهل الدين والتشجيع على الحوار والتواصل معهم، وعدم تركهم للأفكار الضالة المنحرفة.
6. العمل على تنمية روح الانتماء والولاء وحب الوطن والأهل والعشيرة والمجتمع الذي نعيش فيه.
7. العمل دائماً على تطوير الاجهزة الأمنية المعنية بمواجهة الإرهاب وتطوير اجهزتها وأدواتها ومعداتنا واسلحتها وفقاً لأحدث التقنيات العصرية.
8. التنسيق والتعاون الدولي والاقليمي وتبادل المعلومات والخبرات والجهود المبذولة والمشاركة بغية مكافحة الارهاب والقضاء عليه.
9. الاجتهاد في إيجاد الحلول لمجابهة ومواجهة والقضاء على اسباب تلك الظاهرة الارهابية واعمالها الخطيرة.

قائمة المراجع والمصادر:

أولاً: الكتب

- المرابي، جابر (1998) جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرائية، القاهرة: دار النهضة العربية.
- الصغير، جميل عبد الباقي (2002) الإنترنت والقانون الجنائي، القاهرة: دار النهضة العربية.
- الكردي، زين العابدين (2018) جرائم الإرهاب المعلوماتي، بيروت: منشورات الحلبي الحقوقية.
- واصل، سامي جاد عبد الرحمن (2011)، إرهاب الدولة في إطار القانون الدولي العام، الإسكندرية: منشأة المعارف.
- النوايسة، عبد الإله (2018) جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر: عمان.
- الفيل، علي عدنان (2011) الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقية: بيروت.
- بن يونس، عمر محمد أبو بكر (1995) الجرائم الناشئة عن استخدام الانترنت الأحكام الموضوعية والجوانب الإجرائية، منشورات الحلبي الحقوقية: بيروت.
- الشمري، غانم مرضي (2016) الجرائم المعلوماتية، دار الثقافة للتوزيع والنشر: عمان.
- الفاضل، محمد (1978)، الجرائم الواقعة على أمن الدولة، القاهرة: (د.ن).
- الشمالية، ماهر عودة (2015) الإعلام والإرهاب الإلكتروني، دار الإعصار العالمي للنشر والتوزيع: عمان.
- قشقوش، هاني حامد (2003) جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية: القاهرة.

ثانياً: الرسائل الإلكترونية.

- الخوالدة محمد سليمان (2012) جريمة الدخول الغير مشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني، رسالة ماجستير، الجامعة الأردنية، عمان.

ثالثاً: الدراسات والبحوث.

- سليمان، ايناس ممدوح محمد محمد (2021) دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، مصر، 64(1).

- طه، حاج طه (2003)، الإرهاب الدولي وانعكاساته الاقتصادية على الوطن العربي، مجلة جامعة تشرين والبحوث العلمية، سلسلة العلوم الاقتصادية، 25(5).
- السند، عبد الرحمن (1425هـ - 2004م). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الأول، الرياض: جامعة الإمام محمد بن سعود الإسلامية،
- العجلان، عبد الله بن عبد العزيز بن فهد (2008) الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة.
- الخليل، عماد علي (2000) التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم المؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات، جامعة الإمارات العربية المتحدة.
- العيسى، محمود (1423) الإرهاب الإلكتروني، جريدة الرياض، 13(12460).
- المزروعى، موزة (2000) الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق اقتصادية، الإمارات العربية المتحدة، 24(9).
- خليفه، محمد كاسب (2018) الإرهاب الإلكتروني وسبل مواجهته، المجلة المغربية للإدارة المحلية والتنمية، المغرب، 151(1).

رابعاً: المواقع الإلكترونية:

- المنشاوي، محمد عبد الله، مصدر سابق، بحث منشور على الموقع الإلكتروني www.minshawi.com
- ناصر، محمد، بحث بعنوان عنف المعلومات وإرهابها منشور على الموقع الإلكتروني: www.menalmuheet.com

الهوامش:

- سليمان، ايناس ممدوح محمد محمد (2021) دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، مصر، 64(1).
- الشمري، غانم مرضي (2016) الجرائم المعلوماتية، دار الثقافة للتوزيع والنشر: عمان.
- الشمري، غانم مرضي، مرجع سابق، ص 125.
- المتولي، محمد، مصدر سابق، ص 42 – 43
- المنشاوي، محمد عبد الله، مصدر سابق، بحث منشور على الموقع الإلكتروني www.minshawi.com
- المتولي، محمد، مصدر سابق، ص 44.
- ناصر، محمد، بحث بعنوان عنف المعلومات وإرهابها منشور على الموقع الإلكتروني: www.menalmuheet.com
- خليفه، محمد كاسب (2018) الإرهاب الإلكتروني وسبل مواجهته، المجلة المغربية للإدارة المحلية والتنمية، المغرب، 151(1) ص 387.
- الكردي، زين العابدين (2018)، جرائم الإرهاب المعلوماتي، منشورات الحلبي الحقوقية: بيروت، ص 88
- الصغبر، جميل عبد الباقي (2002) الإنترنت والقانون الجنائي، دار النهضة العربية: القاهرة، ص 32.
- الكردي، زين العابدين، مرجع سابق، ص 89.

- الشمالية، ماهر عودة(2015) الإعلام والإرهاب الإلكتروني، دار الإعصار العالمي للنشر والتوزيع: عمان، ص 127-128.
- الكردي، زين العابدين عواد، مرجع سابق، ص 90.
- الشمالية، ماهر عودة، مرجع سابق، ص 127-128.
- السند، عبد الرحمن(1425هـ - 2004م). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الأول، الرياض: جامعة الإمام محمد بن سعود الإسلامية، ص 7.
- العجلان، عبد الله بن عبد العزيز بن فهد(2008) الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول حماية أمن المعلومات والخصوصية في قانون الإنترنت، القاهرة، ص 15.
- الفيل، علي عدنان(2011) الإجرام الإلكتروني: دراسة مقارنة، منشورات زين الحقوقية: بيروت، ص 75.
- طه، حاج طه(2003) الإرهاب الدولي وانعكاساته الاقتصادية على الوطن العربي، مجلة جامعة تشرين والبحوث العلمية، سلسلة العلوم الاقتصادية، 25(5).
- السند، عبد الرحمن بن عبد الله، مرجع سابق، ص 114.
- الشمالية، ماهر عودة، مرجع سابق، ص 114.
- قشقوش، هاني حامد(2003) جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية: القاهرة، ص 45.
- الكردي، زين العابدين عواد، مرجع سابق، ص 92.
- العجلان، عبد الله بن عبد العزيز بن فهد، مرجع سابق، ص 17.
- زين العابدين عواد الكردي، مرجع سابق، ص 95.
- غانم مرضي الشمري، مرجع سابق، ص 152.
- سامي جاد عبد الرحمن واصل، إرهاب الدولة في إطار القانون الدولي العام، منشأة المعارف، الإسكندرية، 2011، ص 158.
- زين العابدين الكردي، مرجع سابق، ص 95.
- ماهر الشمالية، مرجع سابق، ص 85.
- موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق اقتصادية، الإمارات العربية المتحدة، العدد(9)2000م، ص 54.
- العجلان، عبد الله بن عبد العزيز بن فهد، مرجع سابق، ص 19.
- الخليل، عماد علي(2000) التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم المؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات، جامعة الإمارات العربية المتحدة، ص 4.
- العيسى، محمود(1423) الإرهاب الإلكتروني، جريدة الرياض(12460) 15، الشمالية، ماهر، مرجع سابق، ص 198.
- العجلان، عبد الله بن عبد العزيز بن فهد، مرجع سابق، ص 112.
- الفاضل، محمد (1978)، الجرائم الواقعة على أمن الدولة، القاهرة، (د.ن)، ص 264 وما بعدها.
- الخوالدة، محمد سليمان(2012) جريمة الدخول الغير مشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني، رسالة ماجستير، الجامعة الأردنية، عمان، ص 155.
- النوايسة، عبد الإله(2016) جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، دار وائل للنشر: عمان، ص 358.
- المراغي، جابر(1998) جرائم انتهاك أسرار الدفاع عن البلاد من الناحيتين الموضوعية والإجرائية، دار النهضة العربية: القاهرة، ص 117.
- النوايسة، عبد الإله، مرجع سابق، ص 365.