مفهوم الإرهاب الإلكتروني وأسبابه ودوافعه

حسن عادل يسري *

ملخص

أصبح الإرهاب واحداً من أهم الظواهر التي تهدد أمن وإستقرار الدول، وقد ساعدت شبكة الإنترنت في تنامي خطورته، فهو لم يعد ينحصر في المفهوم التقليدي الذي يعتمد على العنف والترويع، بل تجاوزه إلى نوع مستحدث من الإرهاب ألا وهو الإرهاب الإلكتروني، ويعد مفهوم الإلكتروني من المفاهيم المعقدة والخطيرة، نتيجة للتعقيدات الفنية الناجمة عن ثورة المعلومات والتقنيات الحديثة، ولم يعد مفهوم الإرهاب هو ذلك المفهوم الضيق الذي يحدده المكان والزمان، بل أصبح يشكل تهديداً كبيراً لدول العالم على مستوى أنظمتها الإقتصادية والسياسية والإجتماعية فأصبح إرهاب عابر للحدود.

الكلمات المفتاحية: الإرهاب الإلكتروني، الأسباب، الدوافع.

* طالب بحث لإستكمال درجة الماجستير في العلاقات الدولية بكلية التجارة وإدارة الأعمال جامعة حلوان.

The Concept of Cyberterrorism, Its Causes and Motives

Abstract

Terrorism has become one of the most important phenomena threatening the security and stability of States. The Internet has helped to increase its seriousness. It is no longer confined to the traditional concept of violence and intimidation. and even beyond it into an evolving type of terrorism, namely cyberterrorism, the electronic concept is a complex and dangerous concept, as a result of the technical complexities of the information revolution and modern techniques, The concept of terrorism is no longer the narrow concept defined by place and time. s economic, political and social systems have become transnational terrorism.

Keywords: Cyberterrorism, Causes, Motives.

أولاً: مقدمة

إن التطور التكنولوجي المتسارع الذي يشهده العالم اليوم في ظل الثورة المعلوماتية الحديثة التي تلت الثورة الصناعية، فرض على الإنسان الإعتماد على التقنيات التكنولوجية وإستعمالها في مجالات العمل والحياة، وأصبح العالم بذلك عبارة عن قرية صغيرة يمكن التواصل بين مجتمعاته بلا حدود جغرافية او زمنية مما ترك آثاراً إيجابية ونقلة حضارية نوعية مست قطاعات الحياة المختلفة، واستطاعت أن تقدم خدمات عظيمة للأمم والشعوب، إلا أن هذا الجانب الإيجابي للتطور التكنولوجي المعلوماتي أفرز معه بعض الإنعكاسات السلبية التي نتجت عن إساءة استخدام الأنظمة المعلوماتية، وإستغلالها بطريقة غير شرعية بغرض الإضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط وصور مستحدثة من الأعمال الإرهابية تحت مسمى أعمال الإرهاب الإلكتروني.

وقد أدى التقدم التكنولوجي الهائل وخاصة في مجال الإتصالات إلى تطور الأعمال الإرهابية بوجه عام وظهور أنماط جديدة على المتسوى الوطني والإقليمي والعالمي، فزادت معاناة دول العالم من النشاطات الإرهابية وفي ظل ثورة المعلومات والمعرفة الإلكترونية وتطور وسائل الإتصال التقني والرقمي الحديث، استفادت الجماعات الإرهابية من مكاسب هذه الثورة والمعرفة التقنية لتحسين أهدافها ووظائفها، حيث استغلت هذه الجماعات شبكة الإنترنت في تمويل نشاطها والسرقة الرقمية وغسل الأموال والمتاجرة بالمخدرات وغيرها وتمارس كل هذه النشاطات تحت غطاء ما يعرف بالإرهاب الإلكتروني.

ثانياً: إشكالية الدراسة

أصبح الإرهاب اليوم واحداً من أخطر الظواهر التي تهدد أمن الدول واستقرارها، وقد ساهمت شبكة الإنترنت في تنامي خطورته، إذ لم يعد ينحصر في المفهوم التقليدي الذي يقوم على العنف والترويع، بل تجاوزه إلى صورة مستحدثة من الإرهاب، وهو الإرهاب الإلكتروني.

تدور الإشكالية الرئيسية حول توضيح مفهوم ظاهرة الإرهاب الإلكتروني وأسبابه ودوافعه، ومدى تأثير الإرهاب الإلكتروني على الأمن القومي وهل هو يمثل أداه من أدوات القوة التي تمتلكها الدول للتأثير على سلوك الدول الأخرى لتحقيق أهداف معينة. ويكمن الإشكال فيما يتعلق بالإرهاب الإلكتروني، في صعوبة التنبؤ بما يستجد من صوره ومساراته، ومن ثم صعوبة مكافحته، إذ يصعب عملياً مراقبة كل المواقع الإلكترونية عبر العالم وحجب المواقع ذات النزعة الإرهابية. ولا شيء يمنع الإرهابيين من إعادة إنشاء المواقع الإلكترونية المحجوبة، كما أن تعقب كل اتصالات القائمين بالأعمال الإرهابية عبر الإنترنت أمر صعب التحقيق، فبإمكانهم تبادل رسائل إلكترونية مشفّرة في شكل صورة عادية أو مقطع فيديو. وفي هذا الإطار تحاول الدراسة الإجابة على التساؤل الرئيسي المتمثل في:

ما مدى تأثير ظاهرة الإرهاب الالكتروني على الأمن القومي للدولة؟

ويتفرع عن هذا التساؤل عدة تساؤلات فرعية من أهمها:

1- ما المقصود بمفهوم الإرهاب الإلكتروني؟

2- ما هى المفاهيم المرتبطة والمتداخلة مع الإرهاب الإلكتروني؟

3- ما هى أسباب ودوافع الإرهاب الإلكتروني؟

ثالثاً: منهجية الدراسة

إن ظاهرة الإرهاب الالكتروني هى ظاهرة مركبة ومن الصعب الإعتماد على منهج علمي بذاته لتفسيرها، نظراً لما تنطوي عليه من أبعاد وجملة من المتغيرات.

لذلك أعتمد الباحث على أكثر من منهج لتفسير ظاهرة الإرهاب الالكتروني وتأثيرها على الأمن القومي. فيما يلى بيان لهذه المناهج:

1- منهج المصلحة القومية:

يعتبر هذا المنهج أن السعى نحو تحقيق المصلحة القومية للدولة هو الهدف النهائي والمستمر في السياسة الخارجية بمعنى أن المصلحة القومية هى محور الإرتكاز أو القوة الرئيسية المحركة للسياسة الخارجية لأي دولة.

2- المنهج الوصفي التحليلي:

يقوم المنهج على تفسير ظاهرة الإرهاب الإلكتروني، بالإضافة وصف وتحليل تأثير ظاهرة الإرهاب الالكتروني على الأمن القومي وهو ما يجيب على الإشكالية بشكل مباشر.

مفهوم الإرهاب الإلكتروني

لا يوجد تعريف جامع مانع لمفهوم ظاهرة الإرهاب الإلكتروني وذلك نتيجة لحداثة المفهوم وغياب وجود تعريف دقيق لمفهوم الإرهاب في حد ذاته، ففي هذا الإطار نحاول التطرق لبعض التعريفات الخاصة بالإرهاب الإلكتروني.

قدم بارى كولن (Barry Collin) مصطلح الإرهاب الإلكتروني لأول مرة في فترة الثمانينيات وهو زميل أبحاث فى معهد الأمن والإستخبارات في كاليفورنيا، على الرغم من أن الخبراء لم يشكلوا تعريفاً إجتماعياً للإرهاب، فلا يوجد حتى الأن

تعريف موحد للإرهاب الإلكتروني، وقد وضح بارى كولن صعوبة تعريف الإرهاب الإكترونى بدقة وتحديد دور الكمبيوتر والإنترنت في العمل الإرهابي يرجع إلى أن استخدام الإرهاب الإلكتروني يتم على نطاق واسع، حيث يجمع المصطلح بين اثنين من أكبر مخاوف هذا القرن وهما الفضاء الإلكتروني والإرهاب[1].

وقد وضح بارى كولن في دراسته إن وجه الإرهاب آخذ في التغير بينما تظل الدوافع كما هى، حيث أننا نواجه اليوم أسحلة جديدة وغير مألوفة، فإن أنظمة الإستخبارات والتكتيكات والإجراءات الأمنية والمعدات التي كان من المتوقع أن تحمي الناس والأنظمة والدول، أصبحت عاجزة أمام هذا السلاح الجديد المدمر للغاية، علاوة على ذلك فإن أساليب مكافحة الإرهاب التي وضحها المتخصصون في عالمنا على مر السنين غير فعالة ضد هذا العدو، لأن هذا العدو لا يهاجمنا بشحنات محملة بالمتفجرات ولا بحقائب غاز السارين ولا بالديناميت مربوط بأجساد المتعصبين، فهذا العدو يهاجمنا بأسلوب واحد صفر وفي مكان نكون فيه أكثر عرضة للخطر، وهى النقطة التي يتقارب فيها العالمان المادي والإفتراضي.

ويقصد بالعالم المادي (المادة والطاقة – الضوء والظلام – الساخن والبارد) وكلها مادة فيزيائية تعني ذلك المكان الذي نعيش فيه، ويقصد بالعالم الإفتراضي هو تمثيل رمزي – صحيح – مجازي للمعلومات ويعني ذلك المكان الذي تعمل فيه برامج الكمبيوتر وتتحرك البيانات، فالعالمان المادي والإفتراضي عالمان متباينان بطبيعتهما إلا أن التقاطع والتقارب بين هذين العالمين يشكل مركبة الإرهاب الإلكتروني وهو ذلك السلاح الجديد الذي نواجهه، ويزداد الأمر حجماً وأكثر تعقيداً كلما غامرنا أكثر في الإعتماد على التكنولوجيا، ففي كل يوم نتقدم بسرعة هائلة في

[1] Iqbal, Mohammad, Defining Cyberterrorism, **Journal of Computer & Information Law**, Volume 22, Issue 2, P 402, Winter 2004.

مجال التكنولوجيا والحوسبة في كل مهمة وعملية نواجهها، ولقد أصبحنا معتمدين عليها بشكل لا ينفصم أكثر من أي وقت مضى ومعتمدين على تقارب هذين العالمين[2].

تُعرفه دينيج دروثي (Dorothy E. Denning) وهى باحثه أمن معلومات أمريكية، على أنه إلتقاء بين الفضاء الإلكتروني والإرهاب يشير إلى الهجمات غير القانونية والتهديدات بالهجوم على أجهزة الحاسب الألي والشبكات والمعلومات المخزنة عليها، وذلك لتخويف أو إكراه حكومة أو شعبها من أجل تحقيق أهداف سياسة أو إجتماعية، ولكي يصنف الهجوم على أنه إرهاب إلكتروني، يجب أن يؤدي الهجوم إلى عنف ضد الأشخاص أو الممتلكات أو على الأقل التسبب فى ضرر كافٍ ينتج عنه توليد الخوف، ومن الأمثلة على ذلك: الهجمات التي تؤدي إلى الموت أو الإصابة الجسدية أو الإنفجارات أو الخسائر الإقتصادية الفادحة، الهجمات الخطيرة ضد البنى التحتية الحيوية، الهجمات التي تعطل الخدمات الأساسية، كل ذلك يعد من أعمال الإرهاب الإلكتروني إعتماداً على تاثيرها[3].

---

(2) Collin, Barry, **The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge**, 11th Annual International Symposium on Criminal Justice Issues, March, 1997, pp.15-18.

Available at: https://www.crime-research.org/library/Cyberter.htm, last accessed (Feb 22, 2023).

(3) Denning, Dorothy, **Cyberterrorism**, p 1, August 24, 2000.
Available at: Cyberterror-Denning.pdf - Cyberterrorism DOROTHY E DENNING This is a prepublication version of a paper that appeared in Global Dialogue Autumn 2000 In | Course Hero, last accessed (Feb 28, 2023).

يُعرفه جيمس لويس (James A. Lewis) وهو مدير برنامج التكنولوجيا والسياسة العامة في مركز الدراسات الاستراتيجية والدولية (CSIS) في واشنطن، الإرهاب الإلكتروني هو استخدام أدوات شبكة الكمبيوتر لإغلاق البنى التحتية الوطنية الحيوية (مثل: الطاقة والنقل والعمليات الحكومية) أو لإكراه أو تخويف حكومة أو سكان مدنيين [4].

تعريف مكتب التحقيقات الفيدرالي FBI: (The U.S. Federal Bureau of Investigation)

يرى الإرهاب الإلكتروني هو أي هجوم متعمد ذو دوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلي عنف ضد أهداف غير مقاتلة من قبل مجموعات فرعية أو عملاء سريين[5].

تعريف مركز حماية البنية التحتية الوطنية الأمريكية NIPC: (The U.S. National Infrastructure Protection Center)

يرى الإرهاب الإلكتروني فعل إجرامي يُرتكب عن طريق استخدام أجهزة الكمبيوتر وقدرات الإتصالات السلكية واللاسلكية، مما يؤدي إلى العنف أو التدمير أو تعطيل الخدمات لإثارة الخوف من خلال التسبب فى الإرتباك وعدم اليقين داخل

(4) Lewis, James, **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats**, Center for Strategic and International Studies, p 2, December 2002.

(5) Elmusharaf, Mudawi Mukhtar, **Cyber Terrorism: The new kind of Terrorism**, Computer Crime Research Center, April 8, 2004.
Available at: Cyber Terrorism: The new kind of Terrorism (crime-research.org), last accessed (Mar 1, 2023).

مجموعة سكانية معينة، بهدف التأثير على الحكومة أو السكان للتوافق لأجندة سياسية أو إجتماعية أو أيديولوجية معينة[6].

يُعرفه عادل عبدالصادق وهو خبير بوحدة الإعلام ودراسات الرأي العام بمركز الأهرام للدراسات السياسية، الإرهاب الإلكتروني هو العدوان أو التخويف أو التهديد مادياً أو معنوياً بإستخدام الوسائل الإلكترونية الصادرة من الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني أو أن يكون هدفاً لذلك العدوان بما يؤثر على الإستخدام السلمى له[7].

المفاهيم المرتبطة والمتداخلة مع الإرهاب الإلكتروني:

هناك كثير من التباين والجدل قد ظهرا حول طبيعة المفاهيم المرتبطة والمتداخلة مع الإرهاب الإلكتروني، حيث أن وصف تلك المفاهيم بالإرهاب الإلكتروني ينطوي على الإستخدام السيئ للتكنولوجيا ومن أبرز تلك المفاهيم ما يلي:

1- الإرهاب الإلكتروني والجريمة الإلكترونية:

هناك تداخل واضح بين بعض الأفراد في عدم القدرة على التمييز بين الإستخدام السيئ للفضاء الإلكتروني أو الإستخدام ذو الطابع الإجرامي أو الإستخدام كأداة إرهابية، ويرجع ذلك إلى أن هناك عديد من الأنماط قد يمكن اعتبارها جميعاً إرهاباً إلكترونياً إذا ما وُجهت إلى هدف معين وذا أغراض سياسية،

---

(6) Garrison, Linda and Grand, Martin, Cyberterrorism: An Evolving Concept, **The U.S. National Infrastructure Protection Center**, Issue 6, p 2, June 15, 2001.

(7) عبدالصادق، عادل، **الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة** (القاهرة: مركز الدراسات السياسية والإستراتيجية بالأهرام، 2009).

أما إذا فقدت تلك الأنماط الصبغة السياسية فإنها يمكن تصنيفها ضمن كل نمط بصفة منفردة، حيث يوجد مجالات لسوء استخدام الحاسب الآلي والإنترنت تتمثل في استهداف مراكز معالجة البيانات المخزنة في الكمبيوتر واستغلالها بطريقة غير مشروعة أو استهدافها بقصد التلاعب بها أو تدميرها جزئياً أو كلياً، أو استخدام الحاسوب لإرتكاب جريمة ما أو استخدامه بشكل غير قانوني من قبل الأفراد المرخص لهم بإستخدامه.

الترابط بين الأعمال الإرهابية والإجرامية وشبكة الإنترنت من المتوقع أن يزدهر في المستقبل حيث يتم دمج الجريمة في الإرهاب لتظهر في مؤشرات الأمن بصفة عامة، فإذا كان كلاً من الجريمة والإرهاب يتفقا في الوسيلة إلا أنهما يختلفا في الغاية التي تحرك كل منهما، حيث تتعدد الجرائم التي تكون مصحوبة وظيفياً بالإرهاب مثل: التجسس الإلكتروني، والقرصنة الإلكترونية، والجرائم المنظمة، والمواقع المتخصصة في التحريض ضد المعتقدات الدينية، والمواقع المتخصصة في تشوية سمعة الأشخاص، والمواقع البريدية الإباحية، وغسل الأموال، وتزوير البيانات، والقمار عبر شبكة الإنترنت، وتهديدات التجارة الإلكترونية، والجرائم الإقتصادية، وانتحال شخصية الأفراد وشخصية المواقع وانتهاك الخصوصية، والإغراق بالرسائل، وفيروسات الحواسيب الآلية، والإقتحام أو التسلل وغيرها.

تتميز الجريمة الإلكترونية بقدرة مرتكبيها الهائلة على إلحاق خسائر كبيرة، حيث تواجه جهات التحقيق صعوبات كثيرة في ضبط الجرائم الإلكترونية، ويرجع ذلك إلى أن الجريمة الإلكترونية تتم بصورة مستترة وخفية لا يلاحظها المجني عليه، بالإضافة إلى غياب الدليل المادي أو المرئي وإعاقة الوصول إليه بوسائل الحماية الفنية، وافتقاد آثار الجريمة التقليدية نتيجه لسهوله محو الدليل أو تدميره في زمن قياسي، كما قد يكون هناك إحجام عن الإبلاغ تلك الجرائم خشية من التأثير

الإقتصادى في مجتمع الأعمال، بالإضافة إلى نقص الخبرة الكافية لدى جهات القضاء والإدعاء والأجهزة الأمنية في هذا النوع من الجرائم[8].

2- الإرهاب الإلكتروني وحرب المعلومات:

المقصود بحرب المعلومات استخدام نظم المعلومات لإستغلال وتخريب وتدمير وتعطيل معلومات الخصم وعملياته المبنية على المعلومات ونظم معلوماته وشبكات الحاسب الآلي الخاصة بها، وكذلك الحماية من خطر الهجوم من قبل الخصم، لإحراز السبق، والتقدم على نظمه العسكرية والإقتصادية. أما وزارة الدفاع الأمريكية تنظر إلى حرب المعلومات على أنها تلك الأعمال التي تُتخد لإحراز التفوق المعلوماتي بمساعدة الإستراتيجية القومية العسكرية للتأثير بالسلب على معلومات العدو ونظم معلوماته، وحماية ما لديها من معلومات ونظم.

تنقسم حرب المعلومات إلى ثلاثة مستويات على التوالي وهى شخصية، ومؤسسية، وعالمية: حرب المعلومات الشخصية: هى الحرب التى يتم فيها الهجوم على خصوصية الأشخاص في الفضاء المعلوماتي من خلال التصنت عليهم ومراقبة شؤونهم الإلكترونية عبر البريد الإلكترونى. حرب المعلومات المؤسسية: هى الحرب التي تدور ضمن إطار المنافسة أكثر من العداء وهى حرب يكون قوامها استباحة كل شيء لتعطيل المنافس وتهديد أسواقه، فقد تقوم شركة بإختراق النظام المعلوماتي لمنافسها وسرقة نتائج وتفاصيل أبحاثه، وليس هذا فقط بل قد يصل الأمر إلى تدمير البيانات الخاصة بالمنافس أو استبدالها ببيانات زائفة في لمح البصر، وتستطيع الشركة بعد هذه الجولة من الحرب المعلوماتية أن تجعل الأمر

[8] المرجع السابق، ص ص 129، 130.

يبدو وكأنه حادثاً أحدثه فيروس حاسوب آلي، والكشف عن القائم بهذا الأمر يكون احتمال ضعيف، بالإضافة إلى أن المؤسسات والشركات غالباً ما تخشى الإعلان عن ما وقع عليها من ضرر خوفاً من التأثير السلبي للإعلام عنها إلى جانب ما لم يُكتشف منها وهو أكثر بكثير وغير معلوم مداه. حرب المعلومات العالمية: هى الحرب التي تنشب بين الدول وبعضها البعض، أو قد تشنه القوى الإقتصادية العالمية ضد دول معينة، لسرقة أسرار أعدائها وتوجيه تلك المعلومات ضدها وهى حروب قائمة وجارية بالفعل. فالنهاية يظل دور تكنولوجيا المعلومات هو جعل الأسلحة أذكى والخسائر أقل على عكس الحروب التقليدية.

تكون الأداة في حرب المعلومات هى الحاسب الآلى وكذلك الوسيلة وقد يكون الهدف في ذات الوقت، وتقل المخاطر التي يمكن أن يتعرض لها من يقوم بهذا العمل، بالإضافة إلى أن العمليات تتم من خلال شبكة الإنترنت لما تتميز به من رخص التكلفة مقارنة بتكاليف العمليات العسكرية التي تتم في الحروب التقليدية، والقائم بتلك العمليات هو شخص ذو كفاءة وخبرة فنية عالية، وتعتبر حرب المعلومات هى ضربة إستباقية ليكون المستهدف في موقف رد الفعل، بالإضافة إلى أن نشاطها عابر للحدود متجاوز الزمان والمكان مما يضفي عليها إطار العالمية، تعتمد على الخداع والتضليل سواء في الإرتكاب أو التعرف على مرتكبيها فهى لا تترك أثراً خلفها. وهناك خمس خصائص لحرب المعلومات تشير إلى إمكانية تأجيج النزاع وإندلاع الحرب، وهى: إمكانية توسيع دائرة المشاركين بالعمل الهجومي. وإمكانية الوصول إلى أماكن بعيدة الوصول. والإنكار. وسهولة الإنتشار. والتاثير على الأهداف الجاهزة إلكترونياً.

تشكل تلك المميزات إغراءات لعديد من الدول التي يغلب عليها الطابع الإستخباراتي، حيث تمتلك هذه الدول الإمكانيات والقدرات التي تؤهلها للدخول لهذا

النوع من الحروب المعلوماتية وشن هجمات بين بعضها البعض والمقصود هنا هي الدول المتقدمة، ويمكن القول أن الدول النامية تتأثر بشدة من تلك الحروب وذلك لضعف البنية المعلوماتية لديها، وتتميز الحرب المعلوماتية التي تعتمد على الحاسب الآلي بأن مجالها ليس له حدود بالإضافة إلى أن مداها لا يمكن التحكم فيه والهدف غير مأمون العواقب، كما تتميز بقدرتها العالية على الإنتشار عبر الحدود لإصابة دول عديدة، كما أن تلك العملية تستغرق دقائق معدودة، وقد يقوم بها دولة معادية أو دولة صديقة أو جماعات إرهابية أو أفراد.

تتميز الحرب المعلوماتية بتعدد الفاعلين سواء من الدول أو الجماعات الإرهابية أو أفراد، كما تتعدد الوسائل والغايات وهذا ما يسبب وجود تداخل بين الحرب المعلوماتية وغيرها من الأشكال، وفى الواقع هناك تداخل واضح بين بعض الأفراد في عدم القدرة على التمييز بين الإستخدام السيئ للحاسب الألي أو كأداة إرهابية واستخدامه كأداة في النزاع المسلح، فهناك عدد من الأنماط والأشكال يمكن اعتبارها جميعاً إذا ما وجهت إلى هدف معين وذا أغراض سياسية بأنها حرباً معلوماتية.

من العرض السابق يتضح أن هناك علاقة وثيقة بين الإرهاب الإلكترونى وحرب المعلومات، حيث أن الفاعلون في الإرهاب الإلكتروني يمكنهم استخدام حرب المعلومات كأداة لتنفيذ أهدافهم وغاياتهم، كما أن حرب المعلومات قد تتحول في حد ذاتها إلى فعل إرهابى سواء كانت من خلال من يقف وراء استخدامها كالجماعات الإرهابية أو من خلال الحكم عليها وفقاً لطريقة التنفيذ التي تأخذ نفس تيكتيكات العمل الإرهابي، وفي النهاية يمكن القول أن كل تلك الأشكال تعبر عن استخدام

غير سلمي للفضاء الإلكتروني تُعد إرهاباً في طرق تنفيذها الذي يعتمد على الخوف والترويع وهجمات الكر والفر[9].

أسباب الإرهاب الإلكتروني ودوافعه

لا تختلف أسباب ودوافع الإرهاب الإلكتروني عن أسباب ودوافع الإرهاب التقليدي، إنما تختلف فى مدى تأثيرها بإختلاف المجتمع المعتدى عليه، وتنقسم الأسباب إلى نوعين وهى الأسباب العامة والأسباب الخاصة:

1- الأسباب العامة: تتعدد الأسباب العامة للإرهاب الإلكتروني ومن أبرزها ما يلي:

أ- الأسباب السياسية:

إن من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب الإلكتروني ما يلي:

غياب العدالة الإجتماعية وعدم المساواة في توزيع الثروات الوطنية والخدمات والمرافق الأساسية، والإستيلاء على الأموال العامة وإنعدام الأمانة، والتقصير والإهمال في أمور الرعية وعدم تسهيل أمورهم المعيشية والإنسانية[10].

السياسات الإستبدادية غير العادلة التي تتبعها بعض الدول ضد مواطنيها، على سبيل المثال: الكبت السياسي، غياب المشاركة السياسية، التهميش السياسي لدور

[9] المرجع السابق، ص ص 131: 135.

[10] جواد، إسراء طارق، **جريمة الإرهاب الإلكتروني دراسة مقارنة**، رسالة ماجستير، (العراق: كلية الحقوق، جامعة النهرين ، 2012، ص32).

المواطنين، انتهاك الحقوق الإنسانية، عدم تفعيل دور مؤسسات المجتمع المدني، عدم تلبية متطلبات التوازن الإجتماعي[11].

الإحباط السياسي وإنعدام حرية الرأي وغياب الديمقراطية من شأنه أن يولد ردود أفعال غاضبة لدى المواطنين وبالتالى لا تجد ما تصب فيه غضبها سوى الأعمال الإرهابية[12].

الإضطهاد والظلم التي تعاني منه بعض المجتمعات والشعوب الدولية، سواء كان نتيجة للسيطرة الإستعمارية أو انتهاك للحقوق والحرمات أو سلب الأموال أو خرق القوانين والمواثيق الدولية، كل ذلك دفع تلك الشعوب للتشدد والتطرف[13]. احساس الفرد أنه مضطهد والشعور بأن حقوقه مسلوبة في المجتمع، يساعده على الإنضمام لأي جهة أو جماعة لإزالة ما وقع عليه من ظلم أو قهر ومساعدته في الحصول على حقوقه، وهنا تكون الفرصة مناسبة للجماعات والتنظيمات المتطرفة لإحتواء مثل هؤلاء الأفراد، واستغلال دوافعهم والإستمرار في تضخيمها[14].

---

[11] قادة، محمودي، مخاطر ومظاهر الإرهاب الإلكتروني، **مجلة الحقوق القانونية**، العدد 9، ص171، 2018.

[12] جواد، إسراء طارق، مرجع سبق ذكره، ص32.

[13] قادة، محمودي، مرجع سبق ذكره، ص171.

[14] الداغر، مجدي محمد عبد الجواد ، **دور الإعلام فى تشكيل معارف واتجاهات الشباب الجامعى نحو ظاهرة الإرهاب على شبكة الإنترنت : دراسة ميدانية**، (الكويت: حوليات الآداب والعلوم الاجتماعية، مجلس النشر العلمى، جامعة الكويت، 2016، ص89).

إفتقار النظام الدولي إلى الحزم في الرد على المخالفات والإنتهاكات التي تتعرض لها مواثيقه بعقوبات دولية رادعة وشاملة[15].

يعتبر الدافع السياسي من أهم الدوافع المؤدية إلى الإرهاب، حيث تلجأ الجماعات والأفراد إلى استخدام العنف لتحقيق أهداف سياسية معينة، على سبيل المثال ما يلي:

تهديد الأمن القومي، واستهداف النظم العسكرية والمصالح الإستراتيجية للدولة، من خلال التجسس السياسي والعسكري، مما أدى إلى ظهور ما يسمى بحرب المعلومات، والإرهاب المعلوماتي، والتجسس الإلكتروني[16].

زعزعة أمن واستقرار الدولة، وتفتيت الأساس الشرعي لبقاء النظام الحاكم، والإخلال بالنظام العام ومحاولة تغيير نظام الحكم في الدولة، من أجل التطلع إلى السلطة والتنافس للإستحواذ عليها[17].

محاولة فرض مذهب سياسي أو رؤية عقائدية أو سياسية معينة أو إقامة كيان سياسي[18]، أو إثارة النعرات الطائفية والمذهبية والتحريض على الإضطراب والفوضى التي قد تهدد الوحدة الوطنية بين الشعوب وتعرضها للخطر[19].

---

[15] العجلان، عبدالله بن عبد العزيز بن فهد، **الإرهاب المعلوماتى**، المؤتمر الدولى الأول لمكافحة الجرائم المعلوماتية– ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015، ص54.

[16] المرجع السابق، ص54.

[17] عبد اللطيف، سامر مؤيد، الإرهاب الإلكتروني وسبل مواجهته، **مجلة جامعة كربلاء العلمية**، المجلد 14، العدد 3، ص61، 2016.

[18] المرجع السابق، ص61.

[19] العجلان، عبدالله بن عبد العزيز بن فهد، مرجع سبق ذكره، ص54.

ب- الأسباب الإقتصادية:

إن من أهم الأسباب الإقتصادية لظاهرة الإرهاب الإلكتروني ما يلي:

المشكلات الإقتصادية التي يعاني منها الأفراد المتعلقة بالفقر وغلاء المعيشة والتضخم في أسعار المنتجات الغذائية والخدمات الأساسية، أنشأت روح التذمر في صفوف الأمة، مما دفع بعض الشباب إلى التطرف وإستخدام الإرهاب كنوع من التمرد على الواقع لمحاولة إسترداد حقوقهم الإقتصادية المسلوبة من خلال إستخدام الوسائل الإرهابية[20].

انتشار البطالة والفقر وزيادة عدد العاطلين عن العمل في المجتمع وعدم توافر فرص العمل، قد يدفع الشباب إلى التطرف والإنحراف من أجل الحاجة إلى المال لإشباع إحتياجاته الضرورية، كل تلك العوامل قد تدفع الفرد إلى الإنتماء للتنظيمات الإرهابية المتطرفة التي تساهم في إشباع احتياجاته المادية مقابل القيام بتنفيذ بعض العمليات الإرهابية[21]، فالأفراد يحركهم الفقر والجوع وعدم العمل، ويسكتهم المال والعمل[22].

التفاوت بين طبقات المجتمع الواحد، وتفرد جماعات أو قوى معينة بالإستحواذ على الموارد الإقتصادية، وإتساع الفجوة الإقتصادية وتدني المستوى المعيشي بينهم، وزيادة الفوارق الإجتماعية بين فئات المجتمع، كل ذلك سيولد نوع من الحقد والكراهية والأنانية بلا شك، كما أن التأثيرات السلبية للأنظمة الإقتصادية من الممكن أن تنعكس بالسلب على السلوك البشري، والذي قد يدفع بعض الأفراد

---

[20] عبد اللطيف، سامر مؤيد، مرجع سبق ذكره، ص62.

[21] الداغر، مجدي محمد عبد الجواد، مرجع سبق ذكره، ص88.

[22] العجلان، عبدالله بن عبد العزيز بن فهد، مرجع سبق ذكره، ص54.

إلى القيام بالأعمال الإجرامية والعنف والقيام بأعمال غير قانونية من خلال إستخدام وسائل الإرهاب الإلكتروني للإنتقام من بعض فئات المجتمع الأخرى التي حرمتهم من أبسط حقوقهم الإقتصادية[23].

ساهمت التطورات المعلوماتية والتقدم التقني والعلمي في توظيف كل هذه الدوافع المتنوعة بسلوكياتها واتجاهاتها المختلفة وتوفير أجواء العمل الإرهابي[24]، نظراً لما تتيحه التكنولوجيا من سهولة إنتقال الأموال وتبادلها في جميع أنحاء العالم، والتي تعد من أهم الأسباب التي قد تدفع الأفراد إلى التطرف والعنف وإرتكاب جرائم الإرهاب المعلوماتي نظراً لسهولة إرتكابها مقارنة بالإرهاب التقليدي، الأمر الذي ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أهدافهم غير المشروعة[25].

ت- الأسباب الإجتماعية:

إن من أهم الأسباب الإجتماعية لظاهرة الإرهاب الإلكتروني ما يلي:

التفكك الأسري: تعد الأسرة هى الخلية الإجتماعية الأولى التي يعيش فيها الفرد وينمو، لذلك يجب أن تكون الأسرة سليمة وصالحة لتربية الأفراد تربية أخلاقية

---

[23] ملالحة، عبدالرحمن عوض رجا ، جريمة الإرهاب المعلوماتي أسبابه وأساليبه، **مجلة جامعة الأمير عبد القادر للعلوم الإسلامية**، المجلد 34، العدد 1، ص1336، 2020.

[24] الشمري، عبدالصمد سعدون عبدالله، الخزرجي، ليلى عاشور حاجم ، ظاهرة الإرهاب في عصر المعلوماتية الرقمية مبررات الحدث وسبل المواجهة، **مجلة قضايا سياسية**، المجلد 4، العدد 26، ص173، 2012.

[25] جواد، إسراء طارق، مرجع سبق ذكره، ص34.

حسنة، فالإنسان منذ صغره يتأثر بالوسط الأسري الذي يعيش فيه، وتعتبر الأسرة هى المراَة التي تعكس أخلاق الفرد الذي نشأ في أحضانها[26].

البيئة الإجتماعية غير السليمة التي يعيش فيها الأفراد، مثل التفكك الأسري والإجتماعي، وانهيار دور الأسرة في التنشئة الإجتماعية السليمة، نقص المستوى التعليمي، وضعف دور المؤسسات التعليمية التربوية، تعد بيئة خصبة لجذب الشباب إلى الإنحراف والتطرف وارتكاب الأعمال الإرهابية[27].

لذلك فإن المجتمع المتماسك والأسرة المترابطة تحيط الأشخاص بشعور التماسك والتعاون وإحتواء من شذ عنهم ورده عن الظلم، فالمجتمعات ذات الترابط الأسري لا تظهر فيها الأعمال الإرهابية بنفس القدر الذي تظهر فيه عند المجتمعات المفككة إجتماعياً[28].

نقص المستوى التعليمي: غالبية المتورطين في قضايا الإرهاب قديماً كانوا من الأميين، حيث كانوا أكثر عرضة للإنضمام للجماعات الإرهابية، فالجهل ونقص المستوى التعليمي من العوامل التي تساعد في سرعة الإنتماء للجماعات الإرهابية، وهى نتيجة طبيعية ومتوقعة، حيث لا يتوقع من شخص متعلم ومستمر في الدراسة أن ينساق بسهولة وبسرعة للجماعات الإرهابية المتطرفة، فالإرهاب الحديث اليوم

---

[26] ملالحة، عبدالرحمان عوض رجا، مرجع سبق ذكره، ص1337.

[27] عبدالله، علوية حسن، **الإرهاب الإلكتروني ومخاطره على قطاع السياحة**، بحث مقدم للمؤتمر العلمى الدولى العاشر تحت عنوان "التحديات الجيوفيزيائية والإجتماعية والإنسانية والطبيعية فى بيئة متغيرة"، مؤسسة البحوث الأمريكية، تركيا، ص2211، 2019.

[28] جواد، إسراء طارق، مرجع سبق ذكره، ص34.

يعتمد على الفكر والثقافة ومهارات الإنترنت والتخصصات النادرة أو ما يعرف بالإرهاب الإلكتروني[29].

ث-الأسباب الشخصية:

هى أسباب تتعلق بالهدف الذاتي لمرتكب الأعمال الإرهابية الإلكترونية، وتتعدد الدوافع الشخصية المؤدية للإرهاب الإلكتروني ومن أهمها ما يلي:

الرغبة في الظهور ولفت الإنتباه وحب الشهرة، فعندما يكون الشخص غير مؤهلاً يبحث عما يؤهله ليصبح بطلاً، فيلجأ إلى العدوان والتخريب والتدمير[30].

الإحباط والفشل في تحقيق بعض الأهداف والرغبات أو الوصول للمكانة المنشودة، والشعور بالنقص وإحساس الفرد بأنه ينظر إليه نظرة متدنية وأنه أقل من غيره، يدفعه إلى الإرهاب والتطرف والخروج عن النظام[31].

عدم الشعور بالإنتماء للوطن، وافتقاد الشخص لأهمية دوره في المجتمع، والفشل في الحياة الأسرية، من الأسباب التي تؤدى إلى اكتساب الشخص بعض الصفات السيئة كالتطرف والعنف، مما يؤدي إلى ارتكاب الأعمال الإرهابية[32].

الفشل المعيشي والإخفاق الحياتي، والإخفاق قد يكون في الحياة العملية أو العلمية، أو النواحي الوظيفية، أو المسيرة الإجتماعية، أو التجارب العاطفية، مما يجعل الشخص يشعر بالفشل في الحياة[33].

---

[29] الداغر، مجدي محمد عبد الجواد، مرجع سبق ذكره، ص ص 89، 90.

[30] جواد، إسراء طارق، مرجع سبق ذكره، ص30.

[31] المرجع السابق، ص30.

[32] قادة محمودي، مرجع سبق ذكره، ص168.

[33] المرجع السابق، ص169.

شعور الشخص بالنقمة على المجتمع الذي يعيش فيه، نتيجة لما يراه من ظلم وإهدار لحقوقه في المجتمع، فيتولد لديه الحقد والكراهية والإستعداد للقيام بأي عمل يضر بالمجتمع، فيلجأ للإنضمام للمنظمات الإرهابية[34].

الأمراض النفسية مثل الشعور باليأس والإحباط وعقدة الشعور بالنقص الجسماني (كالشخص المصاب بعاهة دائمة تمنعه من القيام بأعماله وتؤدى للإستهانه به من قبل أفراد المجتمع)، مما يدفع الشخص إلى الإنتقام وإحداث تغيرات جذرية قد تصل إلى التضحية بأرواح الأخرين في المجتمع سواء أفراد السلطة أو الأفراد العاديين[35].

ج- الأسباب المادية:

تمثل الدوافع المادية نسبة لا بأس بها الدوافع المؤدية للإرهاب، فالإمكانيات المادية المتاحة حين تُقصر في تلبية احتياجات الأفراد يثور التعارض بين الحاجة وإشباعها، مما يدفع بعض الأشخاص إلى الإنتماء للمنظمات الإرهابية التي توفر لهم الفرص المناسبة لإشباع الحاجات المثارة لديهم مقابل ممارسة بعض الأعمال الإرهابية والأنشطة الإجرامية[36].

ح- الأسباب الفكرية:

إن من أهم الأسباب الفكرية لظاهرة الإرهاب الإلكتروني ما يلي:

---

[34] العجلان، عبدالله بن عبد العزيز بن فهد، مرجع سبق ذكره، ص54.

[35] عيسى، عقيلة هادي، حاتم، اسراء جواد، الإرهاب المعلوماتي(الرقمي) وطرق مكافحته، **المجلة السياسية والدولية**، العدد 16، ص183، 2010.

[36] المرجع السابق، ص184.

الفهم الخاطئ للأديان: حيث يعد الفهم الخاطئ بأصول وقواعد العقيدة والجهل بمقاصد الشريعة من العوامل المساعدة على تطرف الشباب، فالجهل بأصول الدين الصحيحة وحفظ النصوص دون فقه وتفسيرها على غير حقيقتها والغلو في الدين والتعصب لدين معين والإعتقاد بصحته لوحده من أهم أسباب الإرهاب وظهور الفكر المتطرف[37].

الفراغ الفكري: يلعب الفراغ الفكري دور مباشر في انضمام الشباب للإنحراف والجماعات المتطرفة، فعدم إستغلال الشاب لأوقات فراغه في عمل مفيد يحقق به أهدافه ويستثمره فيما يعود عليه بالنفع لإشباع حاجاته، قد يعرضه للإكتئاب والملل والإحساس بالدونية، وبالتالى قد لا يتردد في الإنضمام للجماعات الإرهابية التي تساعده على تحقيق ذاته[38].

وضعف المنطلقات الفكرية لدى الشباب تعود إلى الثورة التكنولوجية المتسارعة ومواقع التواصل الإجتماعي، حيث أصبحت مرجعيتهم الفكرية التي يستمدون منها مصادر معلوماتهم دون إمكانية التحقق من صحة وسلامة تلك المعلومات، بالإضافة إلى عدم صلاحيتها للإعتماد عليها كمصادر لتشكيل هوية فكرية لحاملها، ويمثل التطور التكنولوجى خطورة على الفراغ الفكري لدى الشباب، لأن العقل الفارغ أسرع في التأثر من العقل الممتلئ بالعلم والحكمة، فالفارغ فكرياً سريع التأثر بأي فكر يكون قوياً في عرضه وجذاباً في مظهره حتى ولو كان فكراً ضالاً[39].

---

[37] الداغر، مجدي محمد عبد الجواد، مرجع سبق ذكره، ص89.

[38] المرجع السابق، ص88.

[39] النيل، حسن عبدالله حمد، الفراغ الفكري وخطورته على الشباب في ظل ثورة الإتصالات الحديثة، **مجلة العلوم والبحوث الإسلامية**، العدد 3، ص60، 2011.

2- الأسباب الخاصة: تتعدد الأسباب الخاصة للإرهاب الإلكتروني ومن أبرزها ما يلي:

أ- ضعف بنية الشبكات المعلوماتية وقابليتها للإختراق:

الشبكات المعلوماتية في الأصل مصممة بشكل مفتوح دون قيود عليها أو حواجز أمنية، وذلك رغبة في التوسع وتسهيل دخول مستخدمين جدد، وتحتوي الشبكات المعلوماتية والأنظمة الإلكترونية على ثغرات معلوماتية تمكن المنظمات الإرهابية من استغلال هذه الثغرات في الإختراق والتسلل إلى البنى التحتية المعلوماتية للدول، وممارسة الأعمال الإرهابية والتخريبية[40].

ب- غياب الحدود الجغرافية وتدني مستوى المخاطرة:

تتميز الشبكات المعلوماتية بغياب الحدود المكانية بالإضافة إلي عدم وضوح بيئة المستخدم المستوطن بها لعدم وضوح هويته الرقمية، مما يعد فرصة مناسبة للإرهابيين لممارسة أعمالهم التخريبية، حيث يستطيع الإرهابي أن يقدم نفسه بالهوية أو الصفة التي يرغب بها أو التخفي تحت شخصية وهمية، وبالتالي يقوم بشن هجومه الإلكتروني وهو مسترح في منزله بعيداً عن أعين الناظرين بدون أي جهد أو مخاطرة مباشرة[41].

ت- سهولة الإستخدام وقلة التكلفة:

تتمثل السمة العولمية للشبكات المعلوماتية في كونها وسيلة سهلة الإستخدام، قليلة التكلفة، طيعة الإنقياد، لا تستغرق جهداً ولا وقتاً كبيراً، مما هيأ فرصة ثمينة

---

[40] جواد، إسراء طارق، مرجع سبق ذكره، ص36.

[41] المرجع السابق، ص36.

للإرهابيين للقيام بأعمالهم غير المشروعة، والوصول إلى أهدافهم بأقصى سرعة وأعمق أثراً، دون الحاجة لمصادر تمويل ضخمة، فالقيام بعمل هجوم إرهابي إلكتروني لا يحتاج أكثر من جهاز كمبيوتر متصل بشبكة الانترنت ومزود ببعض البرامج اللازمة[42].

ث- صعوبة اكتشاف وإثبات الجريمة الإرهابية:

في كثير من أعمال الجرائم الإرهابية المعلوماتية لا يُعلم بوقوع الجريمة وخاصة في مجال جرائم الإختراق الإلكتروني، مما يساعد الإرهابي في التحرك بحرية تامة داخل المواقع التي يستهدفها قبل تنفيذ جريمته، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على القيام بالأعمال الإرهابية الإلكترونية، لإنها تعطي للمجرم أملاً في الإفلات من العقوبة[43].

ج- الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية:

يعد الفراغ التنظيمي والقانوني من أهم الأسباب الرئيسية في انتشار ظاهرة الإرهاب الإلكتروني لدى بعض المجتمعات الدولية حول الجرائم المعلوماتية، حتى لو وجدت قوانين تجريمية صارمة متكاملة، فإن الإرهابي يمكنه الإنتقال من دولة إلى أخرى فيستطيع شن هجومه الإلكتروني من دولة لا توجد فيها قوانين صارمة على دولة أخرى يوجد بها قوانين صارمة، ومن هنا تثار مشكلة تنازع القوانين والقانون الواجب تطبيقه.

---

[42] العجلان، عبدالله بن عبد العزيز بن فهد، مرجع سبق ذكره، ص55.

[43] المرجع السابق، ص55.

كما أن عدم وجود جهة مركزية واحدة تتحكم فيما يُعرض على الشبكات المعلوماتية وتسيطر على مدخلاتها ومخرجاتها، يُعد من الأسباب المهمة في تفشى ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي فرد الدخول على تلك الشبكات ووضع ما يريد، وكل ما تملكه جهات السيطرة والرقابة هو منع الوصول إلى بعض المواقع المحجوبة، أو تدميرها وإغلاقها بعد ما قام الإرهابي بنشر ما يريده فيها[44].

[44] الفتلاوي، صلاح هادي، جريمة الإرهاب الإلكتروني، **مجلة القانون للبحوث القانونية**، المجلد 2016، العدد 13، ص597، 2016.

الخاتمة

في ختام هذا البحث، نخلص إلى أن مفهوم الإرهاب الإلكتروني قد طرأ عليه الكثير من التعديل والتغيير، فهو لم يعد ينحصر في المفهوم التقليدي الذي يعتمد على القوة العسكرية، فقد توسع مفهومه ليشمل جميع مجالات الحياة، ويرجع ذلك إلى العصر الرقمي وبفضل ثورة المعلومات والإتصالات، حيث انتشرت القوة وتوزعت بين الفاعلين الدوليين، وتحول الصراع من العالم المادي إلى العالم الإفتراضي، وأصبحت الحروب تقاس بأسلوب واحد صفر، وعلى الرغم من أنه لا يوجد اختلاف بين أسباب ودوافع الإرهاب الإلكتروني عن أسباب ودوافع الإرهاب التقليدي، إلا انها تختلف في مدى تأثيرها بإختلاف المجتمع المعتدى عليه، حيث تنقسم الأسباب إلى نوعين وهى الأسباب العامة والأسباب الخاصة، ومن أبرز الأسباب العامة، الأسباب السياسية، الإقتصادية، الإجتماعية، الشخصية، المادية، الفكرية، ومن أبرز الأسباب الخاصة، ضعف بنية الشبكات المعلوماتية وقابليتها للإختراق، غياب الحدود الجغرافية وتدني مستوى المخاطرة، سهولة الإستخدام وقلة التكلفة، صعوبة اكتشاف وإثبات الجريمة الإرهابية، الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية، في النهاية الإرهاب الإلكتروني ينشأ في بيئة إلكترونية ويقوم على أساس أدوات المعرفة التقنية ونستنتج من ذلك أن الإرهاب الإلكتروني يمثل تهديد للأمن القومي، خاصة بزيادة الإعتماد على التكنولوجيا المتطورة.

المراجع:

أولاً: المراجع العربية:

1- الداغر، مجدي محمد عبد الجواد ، **دور الإعلام فى تشكيل معارف واتجاهات الشباب الجامعى نحو ظاهرة الإرهاب على شبكة الإنترنت : دراسة ميدانية**، (الكويت: حوليات الآداب والعلوم الاجتماعية، مجلس النشر العلمى، جامعة الكويت، 2016، ص89).

2- الشمري، عبدالصمد سعدون عبدالله، الخزرجي، ليلى عاشور حاجم ، ظاهرة الإرهاب في عصر المعلوماتية الرقمية مبررات الحدث وسبل المواجهة، **مجلة قضايا سياسية**، المجلد 4، العدد 26، ص173، 2012.

3- العجلان، عبدالله بن عبد العزيز بن فهد، **الإرهاب المعلوماتى**، المؤتمر الدولى الأول لمكافحة الجرائم المعلوماتية- ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015، ص54.

4- الفتلاوي، صلاح هادي، جريمة الإرهاب الإلكتروني، **مجلة القانون للبحوث القانونية**، المجلد 2016، العدد 13، ص597، 2016.

5- النيل، حسن عبدالله حمد، الفراغ الفكري وخطورته على الشباب في ظل ثورة الإتصالات الحديثة، **مجلة العلوم والبحوث الإسلامية**، العدد 3، ص60، 2011.

6- جواد، إسراء طارق، **جريمة الإرهاب الإلكتروني دراسة مقارنة**، رسالة ماجستير، (العراق: كلية الحقوق، جامعة النهرين ، 2012، ص32).

7- عبد اللطيف، سامر مؤيد، الإرهاب الإلكتروني وسبل مواجهته، **مجلة جامعة كربلاء العلمية**، المجلد 14، العدد 3، ص61، 2016م.

8- عبدالصادق، عادل، **الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة** (القاهرة: مركز الدراسات السياسية والإستراتيجية بالأهرام، 2009).

9- عبدالله، علوية حسن، **الإرهاب الإلكتروني ومخاطره على قطاع السياحة**، بحث مقدم للمؤتمر العلمى الدولى العاشر تحت عنوان "التحديات الجيوفيزيائية والإجتماعية والإنسانية والطبيعية فى بيئة متغيرة"، مؤسسة البحوث الأمريكية، تركيا، ص2211، 2019.

10- عيسى، عقيلة هادي، حاتم، اسراء جواد، الإرهاب المعلوماتي(الرقمي) وطرق مكافحته، **المجلة السياسية والدولية**، العدد 16، ص183، 2010.

11- قادة، محمودي، مخاطر ومظاهر الإرهاب الإلكتروني، **مجلة الحقوق القانونية**، العدد 9، ص171، 2018.

12- ملالحة، عبدالرحمن عوض رجا ، جريمة الإرهاب المعلوماتي أسبابه وأساليبه، **مجلة جامعة الأمير عبد القادر للعلوم الإسلامية**، المجلد 34، العدد 1، ص 1336، 2020.

ثانياً: المراجع الأجنبية:

1- Collin, Barry, **The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge**, 11th Annual International Symposium on Criminal Justice Issues, March, 1997, pp.15-18.
Available at: https://www.crime-research.org/library/Cyberter.htm, last accessed (Feb 22, 2023).

2- Denning, Dorothy, **Cyberterrorism**, p 1, August 24, 2000.
Available at: Cyberterror-Denning.pdf - Cyberterrorism DOROTHY E DENNING This is a prepublication version of a paper that appeared in Global Dialogue Autumn 2000 In | Course Hero, last accessed (Feb 28, 2023).

3- Elmusharaf, Mudawi Mukhtar, **Cyber Terrorism: The new kind of Terrorism**, Computer Crime Research Center, April 8, 2004. Available at: Cyber Terrorism: The new kind of Terrorism (crime-research.org), last accessed (Mar 1, 2023).

4- Garrison, Linda and Grand, Martin, Cyberterrorism: An Evolving Concept, **The U.S. National Infrastructure Protection Center**, Issue 6, p 2, June 15, 2001.

5- Iqbal, Mohammad, Defining Cyberterrorism, **Journal of Computer & Information Law**, Volume 22, Issue 2, P 402, Winter 2004.

6- Lewis, James, **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats**, Center for Strategic and International Studies, p 2, December 2002.