Journal Of the Iraqia University (74-9) January (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

العوامل المؤثرة في نشوء الإرهاب الإلكتروني وتصوراته العملية

رفل صباح نوري الخيقاني
الجامعة الإسلامية قسم القانون
المشرف الأستاذ الدكتور أ.د محمد فرحات

Factors Influencing the Emergence of Cyberterrorism and Its Practical Conceptions

Supervisor: Professor Dr RAFAL SABAH NOORI
rafel.s.nouri@aliraqia.edu.iq
Prof. Dr. Mohamed Farhat
mohammad.farhat@iul.edu.lb

المستخلص

يتناول هذا البحث العوامل المؤثرة في نشوء الإرهاب الإلكتروني بوصفه أحد أخطر التحديات الأمنية والقانونية المعاصرة، لما يتميز به من طبيعة عابرة للحدود واعتماده على التقنيات الرقمية الحديثة. ويسعى البحث إلى تحليل الأسباب الفكرية والتقنية والاجتماعية والسياسية التي أسهمت في ظهور هذا النمط الإجرامي، مع بيان الكيفية التي استغلت بها الجماعات الإرهابية الفضاء الإلكتروني في نشر الفكر المتطرف، والتجنيد، والتمويل، والتخطيط للعمليات الإرهابية. كما يسلّط البحث الضوء على التصورات العملية للإرهاب الإلكتروني، ولا سيما التجسس والترويع والتهديد عبر الوسائط الرقمية، وما يترتب عليها من مخاطر تهدد أمن الدول واستقرار المجتمعات. ويخلص البحث إلى ضرورة اعتماد مقاربة شاملة تقوم على تحديث التشريعات، وتعزيز التعاون الدولي، وتطوير الآليات الوقائية والتقنية لمواجهة هذه الظاهرة المتسارعة.**الكلمات المفتاحية** :الإرهاب الإلكتروني – الجرائم الإلكترونية – الأمن الرقمي – التطرف الفكري – التجسس الإلكتروني – الترويع الرقمي

Abstract

This study examines the factors influencing the emergence of cyber terrorism as one of the most serious contemporary security and legal challenges, due to its transnational nature and its reliance on modern digital technologies. The research analyzes the intellectual, technological, social, and political factors that have contributed to the rise of this criminal phenomenon, highlighting how terrorist groups exploit cyberspace for ideological dissemination, recruitment, financing, and operational planning. The study also addresses the practical manifestations of cyber terrorism, particularly cyber espionage, intimidation, and digital threats, and their serious implications for state security and social stability. The research concludes by emphasizing the need for a comprehensive approach based on legislative modernization, enhanced international cooperation, and the development of preventive and technical mechanisms to effectively counter cyber terrorism.**Keywords:** Cyber Terrorism – Cybercrime – Digital Security – Ideological Extremism – Cyber Espionage – Digital Intimidation

المقدمة

يشكّل الإرهاب ظاهرة إجرامية بالغة الخطورة، لما ينطوي عليه من اعتداء مباشر على كيان المجتمعات الإنسانية وأمنها واستقرارها. وتتجلى هذه الخطورة في الطبيعة الفكرية المتطرفة التي يتبناها الإرهابيون، إذ يقوم تصورهم على الاعتقاد بأحقية فكرهم وسموه المطلق، مقابل إقصاء سائر الأفكار الإنسانية ووصمها بالضلال، الأمر الذي يدفعهم إلى السعي الحثيث لنشر عقيدتهم بأي وسيلة، ولو اقتضى ذلك ارتكاب أفعال إجرامية

وحشية، تحقيقًا لما يدّعونه من مشروع متكامل ذي أبعاد سياسية واقتصادية واجتماعية وثقافية.ولئن كانت الجريمة، في جوهرها، ظاهرة ملازمة للمجتمعات الإنسانية منذ أقدم العصور، فإن وسائل ارتكابها وأساليب تنفيذها لم تكن ثابتة، بل تطورت بتطور المجتمعات وأدواتها. ومع بروز تقنيات المعلومات والاتصال الحديثة، وما وفرته من إمكانات هائلة في سرعة التواصل وانتشار المعلومات، سعت الجماعات الإرهابية إلى توظيف هذه الوسائل، لا لخدمة المجتمع، بل للإضرار به. فأضحت شبكة الإنترنت أداة رئيسة لنشر الفكر المتطرف، والدعاية للتنظيمات الإرهابية، واستقطاب وتجنيد العناصر الجديدة، فضلًا عن جمع التمويل والتخطيط والتنفيذ للعمليات الإرهابية. وفي هذا السياق، برز مصطلح الإرهاب الإلكتروني أو الإرهاب المعلوماتي، بوصفه نمطًا إجراميًا مستحدثًا يشكّل تهديدًا حقيقيًا للدول والأفراد على حد سواء، الأمر الذي يفرض، في ضوء إدراك الفقه القانوني والباحثين لخطورة هذه الظاهرة، ضرورة دراستها وتحليلها وبيان سبل مواجهتها.

أولاً: أهمية البحث:

تنبع أهمية هذا البحث من كونه يتناول ظاهرة حديثة ومتطورة تتجاوز الحدود الجغرافية وتفرض تحديات قانونية وأمنية غير تقليدية. كما تكمن أهميته في تحليل العوامل المؤثرة في نشوء الإرهاب الإلكتروني، بما يساعد على فهم أسبابه الحقيقية والحد من انتشاره. ويسهم البحث في سد النقص التشريعي والفكري المتعلق بتنظيم هذا النوع من الجرائم. إضافةً إلى ذلك، يوفر إطارًا علميًا يمكن أن يُستفاد منه في صياغة سياسات وقائية واستراتيجيات وطنية فعّالة. وتبرز أهمية البحث أيضًا في كونه مرجعًا أكاديميًا يخدم الباحثين والمشرّعين والجهات المختصة.

ثانياً: إشكالية البحث:

يثير الإرهاب الإلكتروني إشكالية قانونية وأمنية معقدة تتمثل في صعوبة تحديد مفهومه الدقيق وتمييزه عن غيره من صور الجرائم الإلكترونية. كما تتجسد الإشكالية في تعدد العوامل المؤثرة في نشأته، سواء كانت تقنية أو اجتماعية أو فكرية أو سياسية، وتداخلها بشكل يصعّب معالجتها بشكل منفرد. ويضاف إلى ذلك قصور بعض التشريعات الوطنية عن مواكبة التطور السريع في أساليب الإرهاب الإلكتروني. ومن هنا يبرز التساؤل الرئيسي للبحث :ما هي العوامل المؤثرة في نشوء الإرهاب الإلكتروني، وكيف تنعكس هذه العوامل على تصوراته العملية وسبل مواجهته قانونيًا وأمنيًا؟

ثالثاً: منهجية البحث:

يعتمد هذا البحث على المنهج التحليلي الوصفي من خلال تحليل مفهوم الإرهاب الإلكتروني وبيان العوامل المؤثرة في نشأته وتطوره. كما يستند إلى المنهج الاستقرائي في تتبع النصوص القانونية والاتفاقيات الدولية ذات الصلة بالجرائم الإلكترونية والإرهاب. ويُستكمل ذلك بالمنهج المقارن عند الاقتضاء، من خلال مقارنة بعض التشريعات الوطنية في معالجتها للإرهاب الإلكتروني.

رابعاً: هيكلية البحث:

سوف نقوم بتقسيم هذا البحث الى مطلبين وكل مطلب الى فرعيين وذلك على الشكل الاتي:**المطلب الأول: الأسباب العامة والخاصة للإرهاب الإلكتروني الفرع الأول: الدوافع العامة للإرهاب الإلكتروني.الفرع الثاني: الدوافع الخاصة للإرهاب الإلكتروني.المطلب الثاني التصورات المحتملة للإرهاب الالكتروني.الفرع الأول: التجسس واحتمالات الإرهاب الإلكتروني.الفرع الثاني: الترويع والتهديد الإلكتروني.**

المطلب الأول الأسباب العامة والخاصة للإرهاب الإلكتروني

إن العوامل المؤدية إلى نشوء الإرهاب الإلكتروني ودوافعه تتسم بالتعدد والتنوع، ويعود جانب منها إلى ذات الأسباب التي تقف وراء ظاهرة الإرهاب التقليدي عمومًا، ذلك أن الإرهاب الإلكتروني يُعد أحد صور الإرهاب وأشكاله المعاصرة. وإلى جانب هذه الأسباب، تبرز عوامل خاصة أسهمت في جعل الإرهاب الإلكتروني وسيلة مناسبة وسلاحًا سهل الاستخدام من قبل التنظيمات الإرهابية، ولا سيما في ظل التطور التكنولوجي واتساع نطاق الفضاء الرقمي. ومن خلال نظرة شاملة ومتوازنة، يمكن القول إن هذه العوامل تتسم بالتشابك والتداخل، حيث تتقاطع الدوافع الشخصية مع الدوافع الفكرية والسياسية والاقتصادية والاجتماعية [١] **.وبناءً على ما سبق نقسم هذا المطلب إلى فرعين، حيث نتناول في الفرع الأول الدوافع العامة للإرهاب الإلكتروني أما الفرع الثاني نتناول الدوافع الخاصة للإرهاب الإلكتروني.**

الفرع الأول الدوافع العامة للإرهاب الإلكتروني

مما لا خلاف فيه أن أسباب الإرهاب ودوافعه تتباين من حيث درجة أهميتها ومدى تأثيرها تبعًا لاختلاف البيئات الدولية، وذلك لاختلاف التوجهات السياسية، والظروف الاقتصادية، والأوضاع الاجتماعية، فضلًا عن التباين الديني والعقائدي بين المجتمعات. وبناءً على ذلك، فإن العوامل التي تسهم في نشوء الإرهاب داخل مجتمع معيّن قد تجد ما يماثلها أو يقاربها في مجتمعات أخرى، وإن اختلفت في حدّتها أو صور تجلّيها، الأمر الذي

يؤكد نسبية هذه الأسباب وعدم انحصارها في إطار مجتمعي واحد، وتعد العوامل التالية من أهم العوامل العامة المساعدة على تكوين الإرهاب الإلكتروني ويمكن أجمالها وعلى النحو الآتي[٢]:

أولاً: الدوافع السياسية: إن من أبرز الدافع السياسية لظاهرة الإرهاب ما يأتي[٣]:

١- وصول السلطة السياسية في الدولة إلى الحكم بطريقة غير ديمقراطية وتماديها في الغي والاستهتار في سرقة أموال الشعب وتدمير البلاد ومصادرة الحقوق والحريات، فإن ذلك سيؤدي من دون شك إلى ردة فعل لدى الشعب الأمر الذي يدفع أبناءه إلى ممارسة أنواع العنف للتخلص من هؤلاء الحكام والذي يقترن مع أسباب أخرى دينية أو عنصرية.

٢- الإحباط السياسي: يُعدّ الإحباط السياسي من أبرز الدوافع المؤدية إلى تنامي ظاهرة الإرهاب، ولا سيما في عدد من الدول العربية والإسلامية، حيث واجهت بعض الحركات والتنظيمات قيودًا صارمة أدت إلى تضييق نشاطها السياسي وحصره أو تجميده.

٣- قصور النظام الدولي: يتمثل أحد العوامل المؤثرة كذلك في افتقار النظام الدولي إلى آليات فعّالة وإجراءات حازمة للرد على المخالفات والانتهاكات التي تتعرض لها المواثيق الدولية، فضلًا عن غياب عقوبات دولية شاملة ورادعة في بعض الحالات.

٤- وجود بعض الممارسات التعسفية من قبل العاملين في أجهزة الدولة عند تطبيقهم للقوانين واللوائح التي تجعل المواطنين في حالة استفزازية في بعض الأحيان.

٥- ضعف الأحزاب السياسية والتنظيمات الثقافية والمهنية وعدم تمكنها من استيعاب الشباب والمواطنين وتلبية مطالبهم واحتياجاتهم، وقد أسهم ذلك في أن ينخرط بعض الشباب في صفوف التنظيمات الإرهابية.

ثانياً: الدوافع الاقتصادية: إن من أهم الدوافع الاقتصادية المؤدية إلى تفشي ظاهرة الإرهاب هي[٤]:

١- تفاقم المشكلات والأزمات الاقتصادية في المجتمعات الدولية بالإضافة إلى المتغيرات الاقتصادية العالمية والاستغلال غير المشروع للموارد الاقتصادية لبلد معين. إذ إن للعوامل الاقتصادية تأثيراً مهم وكبير في حياة الإنسان وسلوكه أكان هذا التأثير إيجابياً أم سلبياً، فإن تدهور الأوضاع الاقتصادية وتردي الحالة المعيشية وما ينتج عنهما من ظواهر سيئة كاختلال التوازن في توزيع الثروات والتفاوت الكبير بين طبقات المجتمع والفقر والبطالة والعوامل الأخرى تؤدي إلى حالة الكراهية والحقد عند الأفراد الذين يعيشون في ظل تلك الظواهر، إذ تؤدي هذه الظواهر إلى خلق حالة عقلية ونفسية لدى الأفراد تدفعهم إلى ارتكاب السلوك الإجرامي، لذلك فإن اللجوء إلى ارتكاب الإرهاب عبر الإنترنت ما هو إلا نتيجة يقررها سوء النظام الاقتصادي، إذ إنّ الظاهرة الإجرامية ترتبط ارتباطاً وثيقاً بالنظام الاقتصادي.

٢-يتمثل أحد العوامل المؤثرة في تنامي ظاهرة الإرهاب في عدم قدرة المجتمع الدولي، ولا سيما منظمة الأمم المتحدة، على إرساء تعاون دولي جاد وفعّال لمعالجة المشكلات الاقتصادية والسياسية العالمية. كما يبرز عجز المنظمة في إيجاد حلول عادلة ودائمة لعدد من القضايا الدولية الجوهرية، مثل اغتصاب الأراضي، والنهب، والاختطاف، وهي أوضاع تعاني منها شعوب عديدة، الأمر الذي يسهم في تغذية مشاعر الظلم وتهيئة بيئة خصبة لانتشار التطرف والإرهاب.

٣-تُعدّ المعاناة الاقتصادية التي يواجهها الأفراد، والمتمثلة في مشكلات الإسكان، وتراكم الديون، وانتشار الفقر، وارتفاع تكاليف المعيشة، والتضخم في أسعار المواد الغذائية والخدمات الأساسية، إلى جانب تدني مستوى دخل الفرد.

٤-يُشكّل انتشار البطالة وازدياد أعداد العاطلين عن العمل، مع محدودية فرص التشغيل، أحد أقوى العوامل المساهمة في تفشي الجريمة والانحراف والسلوك العنيف، بما في ذلك الإرهاب.

٥-أسهم التقدم العلمي والتقني في الأنظمة المصرفية العالمية في تسهيل حركة الأموال وانتقالها وتحويلها عبر مختلف أنحاء العالم، ولا سيما من خلال شبكة المعلومات الدولية (الإنترنت)[٥].

نخلص أن الأسباب الاقتصادية تعدّ عاملاً أساسياً في محور الإرهاب الإلكتروني وزيادة في انتشاره، فضلاً عن أنها تودي إلى استمراره من عدمه كونها تمثل التربة الخصبة لانتشاره والتي تؤثر فيه. إذ تنوعت الأساليب والطرائق المتبعة في عمليات الإرهاب الإلكتروني، ومن تلك الأساليب تقديم الوصفات الجاهزة وبث الأفكار المنحرفة ومهاجمة نظم التحكم الوطني سواء في مجال الطيران أم السكك الحديدية وتعطيل البنوك وعمليات التمويل المالي الأمر الذي يلحق الأذى المالي وثم الحاق الضرر بالاقتصاد الوطني[٦].

ثالثاً: الدوافع الاجتماعية: تعددت الأسباب الاجتماعية الداعية إلى ظهور الإرهاب ويمكن تصنيف أهمها فيما يأتي[٧]:

1- التفكك الأسري والاجتماعي: يؤدي التفكك الأسري والاجتماعي إلى انتشار الاضطرابات النفسية والانحراف والإجرام والإرهاب، في حين يسهم تماسك الأسرة وترابط المجتمع في إشاعة روح التعاون والانتماء واحتواء السلوك المنحرف. ولذلك تقلّ الأعمال الإرهابية في المجتمعات المتماسكة مقارنة بالمجتمعات المفككة اجتماعيًا.

2- ضعف التربية والتوجيه القيمي: يتمثل هذا العامل في غياب التربية السليمة التي توجه الأفراد نحو مكارم الأخلاق، وانعدام التربية الإيمانية القائمة على أسس راسخة تستحضر المصلحة العامة وتسعى إلى درء المفاسد.

3- اختلال الهوية والعدالة الاجتماعية: ينشأ الإرهاب نتيجة فقدان الهوية المجتمعية والعقيدة الصحيحة، وغياب العدل وانتشار الظلم، واختلال العلاقة بين الحاكم والمحكوم، فضلًا عن غياب لغة الحوار بين فئات المجتمع المختلفة.

4- تراجع الدور التوعوي للعلماء: يسهم غياب دور العلماء أو انشغالهم، إلى جانب تقصير بعض أهل العلم والفقه والمعرفة، في ضعف التوجيه والإرشاد المجتمعي، بما يفسح المجال لانتشار الأفكار المتطرفة.

5- الفراغ الفكري والروحي: يُعدّ الفراغ النفسي والروحي والعقلي والزمني بيئة خصبة لتغلغل الأفكار الهدامة والتطرف، إذ إن النفس إن لم تُشغل بما ينفع شُغلت بما يضر، وتترسخ تلك الأفكار على نحو يصعب اقتلاعها إلا بالعمل الصالح والعلم النافع.

٦- للصداقة أو لبيئة الصداقة دور لا يستهان به في توجيه الفرد نحو الخير أو الشر، فكما هو معروف أن الإنسان بطبعه كائن قابل للتأثير والتأثر والتغيير والتغير، فإذا ما صادفته بيئة غير صالحة وأصدقاء سوء فإن مرافقتهم بلا شك ستؤدي به إلى الانحراف والشذوذ عن الطريق السليم، ومن ثم قد تكون بيئة الصداقة عاملاً أساسيا يدفع الإنسان إلى ارتكاب الجرائم على اختلاف أنواعها وبضمنها الإرهاب الإلكتروني، كما أن لبيئة العمل والمهن ذات التأثير في الإنسان في نية الصداقة[٨].

رابعاً: الدوافع الفكرية:

تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب، تبعاً لظروف البلاد التي ينطلق فيها الإرهاب وكما يلي[٩]:

- الجهل بمقاصد الشريعة الإسلامية، والتلاعب بمعانيها بالظن من غير يقين وثبات.
- التطرف، وهو أمر بالغ الخطورة في أي مجال من المجالات ولاسيما في الأمور الفكرية.
- الانقسامات الإيديولوجية الفكرية المتباينة بين التيارات المتنوعة والأحزاب المختلفة.

وتأسيسا لما تقدم إن للكيانات السياسية أثراً بارزا وكبيرا في حل الأزمات والمشكلات السياسية، فإذا كانت الكيانات السياسية متخلفة وغير واعية وليست نزيهة وإن همها هو الاستيلاء على السلطة من دون وضع الحلول الواقعية والملموسة لمشكلات الدولة، فإن ذلك سيؤدي إلى استخدام الشبكة الدولية للمعلومات للقيام بالأعمال الإرهابية[١٠].

خامساً: الدوافع الشخصية:

تتعدد الدوافع الشخصية المؤدية للإرهاب ويمكن إيجازها وعلى النحو الآتي: [١١]

- الرغبة في الظهور وحب الشهرة.
- الإحباط في تحقيق بعض الأهداف أو الرغبات أو الوصول إلى المكانة المنشودة وإحساس الشخص بأنَّه أقل من غيره.
- افتقاد الشخص لأهمية دوره في الأسرة والمجتمع وفشله في الحياة الأسرية.
- الإخفاق الحياتي والفشل.
- نقمة الشخص على المجتمع الذي يعيش فيه نتيجة ما يراه من ظلم وإهدار لحقوق المجتمع فيتولد لديه الحقد والاستعداد للقيام بأي عمل يضر المجتمع.

الفرع الثاني الدوافع الخاصة للإرهاب الإلكتروني

ذكرنا آنفًا أن أسباب الإرهاب الإلكتروني ودوافعه متعددة ومتنوعة، وهي في جوهرها ذات الأسباب التي تقوم عليها ظاهرة الإرهاب بوجه عام، غير أنه يجدر التنبيه إلى وجود عوامل وبواعث خاصة أسهمت في جعل الإرهاب الإلكتروني مجالًا ملائمًا ووسيلة سهلة تعتمدها الجماعات والتنظيمات الإرهابية لتحقيق أهدافها، وعليه يمكننا بيان أبرز دوافع انتشار الإرهاب الإلكتروني بوجه خاص وعلى النحو الآتي[١٢] :

أولاً: تمويل الإرهاب الإلكتروني: إن من أهم أسباب قيام الدول في العادة هو المال والرجال والقوة، ولان الإرهاب قد واجه الدول، بل أعجز الكثير منها في إيقافه أو الرد عليه، لذا فإن أمر التمويل جاء سبباً أساساً ورئيساً في قيامه، ومن ثم ديمومته واستمرار وجوده وتأكيد نشاطاته الموجعة في

آثارها على الفرد والمجتمع والدول جميعها بشكل عام.لا شك أن جريمة تمويل الإرهاب قد حظيت في السنوات القليلة الماضية باهتمام كبير من قبل معظم الدول والمنظمات الدولية، وذلك من خلال اتخاذ آلية معينة لمحاربة تلك الجريمة، سواء كان ذلك بتشريع القوانين التي تمنع هذه الجريمة أو التي تعاقب مرتكبيها أم بالتدابير الأمنية أو الرقابية، وذلك نظراً لخطورتها المتزايدة، ولاسيما الأمنية منها على المستويين الوطني والدولي، لذا بدأ الاهتمام الدولي يبرز في موضوع تمويل الإرهاب، وذلك لما تسببه جريمة الإرهاب الإلكتروني من أثر على المجتمع نتيجة العنف وإحداث الخسائر في الأرواح أو الضحايا البريئة، فضلاً عن التأثير السلبي في الاقتصاد الوطني والنظام العالمي بشكل عام[١٣]تجدر الإشارة إلى أن الدافع المالي يُعد من أبرز البواعث على ارتكاب معظم الجرائم، ولا سيما الجرائم الإرهابية، الأمر الذي يقتضي أن تنصرف جهود مكافحة الإرهاب بوجه عام، والإرهاب الإلكتروني بوجه خاص، إلى حرمان التنظيمات الإرهابية من الوسائل المادية اللازمة لتنفيذ أنشطتها. ويشمل ذلك منعها من إيجاد بيئات آمنة لتنظيم عناصرها والتخطيط لعملياتها، فضلًا عن اتخاذ التدابير القانونية والإدارية الكفيلة بمنعها من الحصول على مصادر التمويل. كما يتعين الحيلولة دون امتلاكها للأدوات والوسائل والأسلحة التي تُستخدم في الاعتداء على المدنيين والمنشآت الوطنية. ويحصل الإرهابيون على الدعم المالي بوسائل متعددة، مباشرة أو غير مباشرة، من خلال منظمات تدّعي العمل الخيري أو الاجتماعي أو الثقافي، أو عبر ممارسة أنشطة غير مشروعة كالاتجار بالمخدرات والأسلحة وابتزاز الأموال[١٤]في الحقيقة أن أسباب انتشار الجرائم الإرهابية في العالم كثيرة ومتعددة، إلا أن العامل الرئيس الذي يقف وراء ارتكاب هذه الجرائم ويسهم في تجنيد الإرهابين، وكذلك في عمليات شراء وتوزيع الأسلحة التي تستعمل في الجرائم الإرهابية وإيواء الإرهابين، فإن كل ذلك يستند إلى عملية التمويل الذي تحصل عليه الجماعات الإرهابية ولا سيما وإن المنظمات الإرهابية أصبحت تدرك أن تكنولوجيا المعلومات والاتصالات تستطيع أن تؤدي دوراً في التمويل والتجنيد، وتعكف الكثير من هذه المنظمات على توسيع نطاق الاستفادة القصوى من هذه التكنولوجيا، الأمر الذي يؤكد أن القضاء على التمويل وحرمان الجماعات الإرهابية من الحصول عليه يؤدي في نهاية المطاف إلى القضاء على الجرائم الإرهابية أو في أقل تقدير الحد منها بشكل كبير جداً، إذ إنَّ ذلك قد دفع الكثير من الدول التي تحارب الإرهاب باتخاذ قرارات بشأن تجفيف منابع تمويله، وإذا كان هذا الأمر سهلاً لتجفيف منابع الإرهاب الظاهرة، إلا أن الأمر يبدو صعباً بالنسبة لتمويل الجريمة الإرهابية عن طريق مصادر التمويل غير الظاهرة، إذ إنَّ تمويل الإرهاب بواسطة غسيل الأموال القذرة يشكل مصدراً خفياً للتمويل لتلك الجرائم الإرهابية.

ثانياً: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق:إن شبكة المعلومات صُمِّمت في الأصل على نحوٍ مفتوح، مع تقليل القيود والحواجز الأمنية، بهدف التوسع وتيسير وصول المستخدمين، الأمر الذي أفرز بيئة رقمية تحتوي على أنظمة وشبكات معلوماتية تضم شفرات وبرمجيات قابلة للاختراق. وقد أتاح ذلك للمنظمات الإرهابية استغلال الثغرات التقنية للتسلل إلى البنى التحتية المعلوماتية وممارسة أنشطة تخريبية وإرهابية تهدد أمن الدول والمؤسسات.ويُعرَّف الاختراق بوجه عام بأنه القدرة على الوصول إلى هدف معيّن بطريقة غير مشروعة، من خلال استغلال ثغرات في أنظمة الحماية الخاصة به. ويُعدّ هذا السلوك من أخطر الممارسات الإجرامية، لما ينطوي عليه من انتهاك لخصوصية الأفراد وتمكين المخترق من النفاذ إلى أجهزتهم دون علمهم أو رضاهم، وما قد يترتب على ذلك من أضرار جسيمة تمس بياناتهم الشخصية أو تُحدث آثارًا نفسية ومعنوية خطيرة نتيجة الاستيلاء على ملفاتهم ومعلوماتهم الخاصة[١٥].

ثالثاً: غياب الحدود الجغرافية وتدني مستوى المخاطرة:إن السمة العالمية لشبكات المعلوماتية فضلاً عن عدم وضوح الهوية الرقمية للمستخدم وانها مفتوحة وتعد فرصة مناسبة للإرهابيين، حيث يستطيع محترف الحاسوب أن يقدم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ويطلق على نفسه ألقاباً أو أسماء مستعارة ويؤيدها بأدلة ملموسة كالصور، أو بعض المعلومات الصحيحة ليثبت جديته ومن ثم يشن هجومه الإلكتروني وهو في منزله من دون مخاطرة مباشرة بعيداً عن أعين الناظرين[١٦]تأسيساً على ما تقدم نستطيع القول إن غياب الحدود المكانية في الشبكة المعلوماتية وعدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته غير المقفلة والمفتوحة، كل هذا يشكل فرصة كبيرة ومناسبة للإرهابين لتحقيق مآربهم.

رابعاً: الفراغ التنظيمي والقانوني وغياب جهة السيطرة والمراقبة على الشبكات المعلوماتية:إن الفراغ التشريعي والتنظيمي القائم في بعض المجتمعات فيما يتعلق بالجرائم المعلوماتية والإرهاب الإلكتروني يُعد سببًا رئيسًا في انتشار هذه الظاهرة، إذ إن غياب قوانين تجريمية متكاملة يتيح للمجرمين التحرك عبر الحدود واستغلال تفاوت النظم القانونية. وعلى العكس من ذلك، فإن سن تشريعات صارمة وشاملة من شأنه تقييد نشاط الجناة والحد من قدرتهم على الانتقال من دولة إلى أخرى لممارسة أنشطتهم غير المشروعة.كما أن عدم وجود جهة مركزية موحدة تشرف على ما يُعرض عبر شبكة المعلومات وتتحكم في مدخلاتها ومخرجاتها يُعد عاملًا مهمًا في تفشي الإرهاب الإلكتروني، حيث يتيح الطابع المفتوح للشبكة لأي شخص

نشر ما يشاء من محتوى. ولا يتجاوز دور الجهات الرقابية في الغالب حجب بعض المواقع أو إغلاقها بعد وقوع الفعل ونشر المحتوى الإجرامي، وهو ما يقلل من فاعلية المواجهة الوقائية لهذه الظاهرة(١٧).

خامساً: سهولة الاستخدام وقلة التكاليف:إن الفراغ التنظيمي والتشريعي القائم في بعض المجتمعات الدولية في مجال الجرائم المعلوماتية والإرهاب الإلكتروني يُعد سببًا رئيسيًا في انتشار هذا النوع من الإرهاب، إذ إن غياب منظومة قانونية متكاملة يتيح للمجرمين التحرك عبر الحدود دون عوائق فعّالة. ومن شأن سنّ تشريعات جزائية صارمة ومتكاملة أن يحدّ من هذه الظاهرة، عبر منع الجناة من الانتقال من دولة إلى أخرى هربًا من المساءلة. كما أن عدم وجود جهة مركزية موحدة تُشرف على ما يُنشر عبر الشبكة وتتحكم بمدخلاتها ومخرجاتها يسهم في تفشي الإرهاب الإلكتروني، حيث تقتصر وسائل الرقابة غالبًا على حجب بعض المواقع أو إغلاقها بعد استغلالها ونشر المحتوى الإجرامي من خلالها (١٨).

سادساً: أسباب أخرى تمثلت بالآتي- : غياب دور البيت والمدرسة في الرقابة على عموم أفراد العائلة ما يفسح المجال أمامهم في استعمال هذه التكنولوجيا استعمالاً خاطئاً، أو تمادي الطالب في استعمال التقنية استخداماً سيئاً -. الغلو والتشدد في بعض أمور الدين، فالبعض ومن الشباب الذين يستعملون الشبكة العالمية للمعلومات من الشباب يرون أنهم أعلم من غيرهم وإن بعض العلماء على ضلالة، ما يتطلب محاربة آرائهم تقنياً.

– الفراغ الذي يشكل سبباً رئيساً يدفع الشباب للجوء إلى استعمال هذه التكنولوجيا، ما يجعله عرضة للوقوع في مصائد الجماعات الإرهابية بسبب مواقع التواصل الاجتماعي فضلاً عن أن التطور الكبير والمتنامي في مجال الإنترنت وتكنولوجيا المعلومات، يجعل الإرهابيين أكثر اعتماداً على تكنولوجيا الاتصالات الإلكترونية وخاصة الإنترنت مستقبلاً، الأمر الذي سيجعل الإرهاب أكثر تعقيداً وخطورة لذلك لا بد من التريث في تقدير الأخطار الحالية للتمكن من مواجهة تلك التحديات بشيء من الدراية والعلم.[19]وفي الحقيقة أن الإرهابيين لديهم القدرة على استعمال الشبكة الدولية للمعلومات لتنفيذ مأربهم وتحقيق أهدافهم، وبالمقابل فإن بإمكان صانعي السلام استعمال الشبكة أيضاً ومحاربتهم، وذلك من خلال تعميم كلما يمكن أتباعه من فكر يهدف تحقيق المحبة والتعايش السلمي بين المجتمعات المختلفة لنشر المواقع الصالحة التي تدعو إلى الخير وتحد من دور نشر الأفكار المنحرفة عبر المواقع الإلكترونية، الأمر الذي يتوجب الدول والحكومات للسعي إلى فرض الرقابة الصارمة على كل ما ينشر على شبكة المعلومات الدولية للحد من دخول مواقع المتطرفين التي تشجع على الإرهاب.وفي الواقع فإن العالم وبمختلف مستوياته ذهب إلى مواجهة الإرهاب الإلكتروني، وخاصة بعد التطور الكبير في تكنولوجيا المعلومات، حيث وضعت تشريعات خاصة لضبط هذه التقنيات لوقف إمكانية ارتكاب هذا النوع من الجرائم[20].وأخيراً فإن العاملين على إدخال البرامج الخاصة بمواجهة الإرهاب الإلكتروني قبل البدء به يعد إنذاراً، ذلك أن الجهود المبذولة في تطوير تكنولوجيا المعلومات وخبراء الإنترنت يجب أن يستمروا في ملاحقة الأنشطة الإرهابية التوسعية بإعداد أنشطة حماية لسد الثغرات تاميناً لهذا الفضاء الحيوي ومنع الآثار الإرهابية المدمرة. لكل ما أوردناه من أسباب ودوافع فإن الإرهاب الإلكتروني بات هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية ومن ثم لا يمكن لأية دولة أن تعيش بمعزل عن التكنولوجيا والتي أصبحت من أهم وسائل التواصل العالمي، وأداة تربط بين دول العالم، عن طريق تقنيات المعلومات والاتصالات والتطبيقات التي كانت وما تزال وسطاً لانتشار الأفكار الإرهابية بين مستخدمي هذه التقنيات الحديثة ما أوجب قيام الدول بحماية أفرادها ومؤسساتها وحضاراتها من آثار هذا الانفتاح، رغم الفوائد الكثيرة لتكنولوجيا المعلومات الحديثة وما يجب إدراكه من مخاطر قد تسبب بها هذه التقنيات، الأمر الذي يحتم على كل دولة ضع الضوابط لمواجهة هذه المخاطر، وأولها العمل على منع وحجب المواقع الضارة والمنحرفة، التي تشجع على العمل الإرهابي والإيمان بطريقة أسلوباً لتحقيق أغراض الإرهابيين، وتصوير كون أهدافهم إنسانية ودينية تحقق رضا الله خلافاً للحقيقة، باستغلالهم شبكات المعلوماتية وسيلة لتحقيق مآربهم الخبيثة والدنيئة[٢١].وتجدر الملاحظة إلى الجهود الدولية والإقليمية التي بذلت من أجل القضاء أو الحد من عمليات تمويل الجرائم الإرهابية، وقد سعى المجتمع الدولي إلى ذلك من خلال وضع آليات معينة تتمثل بالآتي:

- الاتفاقية الدولية لقمع تمويل الإرهاب.
- قرار مجلس الأمن رقم ١٣٧٣[٢٢].

الجهود الإقليمية لمكافحة تمويل الإرهاب.

وخلاصة ما سبق أن تعد الدوافع السياسية والدوافع الاقتصادية والدوافع الاجتماعية والدوافع الشخصية والدوافع الفكرية والدوافع النفسية من الدوافع العامة للإرهاب الإلكتروني.أبرز دوافع الخاصة لانتشار الإرهاب الإلكتروني: تمويل الإرهاب الإلكتروني وضعف بنية الشبكات المعلوماتية وقابليتها للاختراق وغياب الحدود الجغرافية وتدني مستوى المخاطرة والفراغ التنظيمي والقانوني وغياب جهة السيطرة والمراقبة على الشبكات المعلوماتية وسهولة الاستخدام وقلة التكاليف وصعوبة اكتشاف وإثبات الجريمة الإرهابية.

المطلب الثاني التصورات المحتملة للإرهاب الإلكتروني

إن الفراغ التشريعي والتنظيمي في بعض المجتمعات فيما يتعلق بالجرائم المعلوماتية والإرهاب الإلكتروني يُعد من الأسباب الرئيسة لانتشار هذه الظاهرة، إذ إن غياب القوانين الجزائية المتكاملة يتيح للجناة حرية التنقل والانطلاق من دولة إلى أخرى. وعلى العكس من ذلك، فإن سنّ تشريعات صارمة ومتكاملة من شأنه الحد من هذه الجرائم من خلال تضييق نطاق الإفلات من العقاب. كما أن غياب جهة مركزية موحدة تتولى الرقابة على ما يُنشر عبر الشبكة، وتتحكم بمدخلاتها ومخرجاتها، يسهم في تفشي الإرهاب الإلكتروني، حيث يتيح لأي شخص نشر المحتوى الذي يريده، ولا تقتصر وسائل المواجهة المتاحة غالبًا إلا على حجب بعض المواقع أو إغلاقها بعد أن يكون المحتوى الإجرامي قد أُتيح وانتشر[٢٣].تتسم شبكات المعلومات بطابعها العالمي، وبكونها سهلة الاستخدام، قليلة الكلفة، وسريعة التنفيذ، ولا تتطلب جهدًا أو وقتًا كبيرًا، الأمر الذي وفر للتنظيمات الإرهابية وسيلة فعّالة لتحقيق أهدافها غير المشروعة دون الحاجة إلى تمويل ضخم. فتنفيذ هجوم إرهابي إلكتروني لا يتطلب في الغالب أكثر من جهاز حاسوب متصل بالشبكة المعلوماتية ومزوّد بالبرمجيات اللازمة، وهو ما يزيد من خطورة هذا النمط الإجرامي وسهولة انتشاره[٢٤].**وبناء على ما سبق سنقوم بتقسيم هذا المطلب إلى فرعين، سنتناول في الفرع الأول التجسس واحتمالات الإرهاب الإلكتروني، بينما سنتناول في الفرع الثاني الترويع والتهديد الإلكتروني.**

الفرع الأول التجسس واحتمالات الإرهاب الإلكتروني

أفضى التطور المتسارع في تقنيات المعلومات والاتصالات، وما نتج عنه من اندماج وثيق بين هذين المجالين، إلى إحداث نقلة نوعية شكّلت الأساس لما يُعرف بثورة المعلومات. وقد انعكس هذا التحول على مختلف القطاعات، التي أصبحت تعتمد اعتمادًا جوهريًا على الأنظمة المعلوماتية في إنجاز أعمالها، لما توفره من سرعة ودقة في جمع البيانات ومعالجتها وتخزينها، فضلًا عن سهولة نقلها وتداولها بين الأفراد والمؤسسات داخل الدولة الواحدة أو عبر الحدود الدولية. وبذلك، بات هذا العصر يُوصَف بعصر المعلومات.ومع اتساع نطاق المعرفة الإنسانية وتزايد حجم البيانات الناتجة عن الأنشطة البشرية، لم يعد الكم المتاح من المعلومات أمرًا يسير التعامل معه كما كان في السابق، إذ أصبحت الأساليب التقليدية في جمع المعلومات وتنظيمها عاجزة عن مواكبة هذا التنامي المتسارع. وقد فرض ذلك الحاجة إلى وسائل تقنية حديثة قادرة على إدارة هذا التدفق المعرفي بكفاءة وفعالية، بما يلبّي متطلبات المستخدمين ويواكب التطور العلمي والتقني المتواصل[٢٥].

أولاً: ماهية وأساليب التجسس الإلكتروني: إن من الضروري اللجوء إلى استخدام أساليب علمية وتقنية متطورة لمواجهة هذه ثورة المعلومات والاتصالات، ووسائل الاتصال؛ لذا فقد أدى هذا إلى شيوع جريمة التهديد عبر هذه الوسائل الإلكترونية، وسنتناول ماهية وأساليب التجسس الإلكتروني على النحو الآتي:

١- **ماهية التجسس الإلكتروني:**شهد مجالا تقنية المعلومات والاتصالات تطورًا متسارعًا وغير مسبوق، أعقبه اندماج وثيق بينهما شكّل الأساس الذي قامت عليه ثورة المعلومات المعاصرة. وقد أدى ذلك إلى اعتماد مختلف القطاعات الحيوية، بصورة متزايدة، على الأنظمة المعلوماتية في أداء أعمالها، لما توفره من سرعة ودقة في جمع البيانات، وتخزينها، ومعالجتها، ثم تداولها وتبادلها بين الأفراد والمؤسسات داخل الدولة الواحدة أو عبر الحدود الدولية. ونتيجة لذلك، أُطلق على المرحلة الراهنة وصف "عصر المعلومات". وبعد أن كان حجم البيانات المتداولة في فترات سابقة محدودًا ولا يشكّل عبئًا على عمليات التنظيم والاسترجاع، أدى التقدم العلمي وتراكم المعارف الإنسانية إلى تضخم كمّ المعلومات بشكل كبير، الأمر الذي كشف عن قصور الأساليب التقليدية في إدارتها وعدم قدرتها على تلبية حاجات المستفيدين بالكفاءة المطلوبة[٢٦].ولا تُعد محاولات اختراق الشبكات والمواقع الإلكترونية من قبل بعض العابثين من مخترقي الأنظمة المعلوماتية (Hackers) أعمالًا إرهابية، ذلك أن مخاطرهم غالبًا ما تكون محدودة، وتقتصر على العبث بالمحتويات أو إتلافها، وهي أضرار يمكن تجاوزها باستعادة نسخ احتياطية محفوظة في مواقع آمنة[٢٧].

٢- **أساليب التجسس:** تتم عملية إرسال نظم التجسس الإلكتروني بوسائل متعددة، ويُعدّ البريد الإلكتروني من أكثرها شيوعًا، إذ يقوم الضحية بفتح المرفقات الواردة ضمن رسائل مجهولة المصدر. كما قد تُزرع أدوات التجسس من خلال استخدام أحصنة طروادة، أو عبر تنزيل بعض البرامج من مواقع غير موثوق بها. كذلك يمكن إعادة تكوين أحصنة طروادة بواسطة وحدات الماكرو الموجودة في برامج معالجة النصوص، فضلًا عن إمكانية لجوء الإرهابيين إلى استخدام الفيروسات كوسيلة للاختراق والتجسس المعلوماتي[٢٨].تُعدّ أساليب التجسس الإلكتروني من أخطر الأدوات التي تعتمدها التنظيمات الإرهابية في عصر المعلومات، ومن أبرزها أسلوب إخفاء المعلومات داخل معلومات أخرى، حيث يلجأ الجاني إلى تضمين البيانات أو المعلومات الحساسة المستهدفة ضمن محتوى عادي مخزّن على الحاسب الآلي، ثم يعمل على تهريب هذا المحتوى في مظهره الطبيعي، بما لا يثير الشكوك حتى في حال ضبط الشخص متلبسًا. وقد يلجأ كذلك إلى استخدام وسائل غير تقليدية للحصول على المعلومات السرية.

ومن بين الممارسات الشائعة في هذا الإطار، قيام الإرهابيين باختراق حسابات البريد الإلكتروني للأفراد، وانتهاك خصوصيتهم من خلال الاطلاع على مراسلاتهم وبياناتهم الشخصية، والتجسس عليها، بقصد الاستفادة منها في تنفيذ عملياتهم الإرهابية أو استخدامها كوسيلة للضغط والتهديد لحمل الضحايا على القيام بأفعال معينة تخدم أهدافهم الإجرامية.وتتجلى خطورة هذه الأفعال في ضعف الوسائل الأمنية المعتمدة لحماية شبكات المؤسسات والهيئات الحكومية، إذ لا يمكن الاعتماد بصورة مطلقة على أنظمة الحماية المنتَجة من قبل الشركات الأجنبية، لعدم توفر الضمان الكافي لأمنها وسلامتها بشكل كامل.كما يجدر التنبيه إلى أن الأساليب الفنية للتجسس المعلوماتي مرشحة لأن تكون الأكثر استخدامًا في المستقبل من قبل التنظيمات الإرهابية، نظرًا للأهمية البالغة للمعلومات التي تمتلكها المؤسسات والقطاعات الحكومية، ولا سيما في المجالات العسكرية والسياسية والاقتصادية، إذ إن الحصول على هذه المعلومات واستغلالها من شأنه الإضرار بالمصلحة العامة والأمن الوطني[٢٩].

ثانياً: التصورات المحتملة للإرهاب الإلكتروني:هنالك الكثير من التصورات المحتملة للإرهاب الإلكتروني، وسنقوم بتقسيم هذه الاحتمالات على النحو الآتي:

١- **استهداف النظم العسكرية:** تستهدف هذه الفئة من الهجمات، في الغالب، الأهداف العسكرية غير المدنية المرتبطة بشبكات المعلومات، ويُعد هذا التصور من أخطر الاحتمالات التي قد تهدد المجتمعات المعاصرة. إذ تبدأ مرحلته الأولى باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، وأنظمة الدفاع الجوي، والصواريخ النووية. وقد تتهيأ لإرهابي المعلومات، في هذه الحالة، فرصة فك الشفرات السرية الخاصة بأنظمة التحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية والأسلحة المدمرة، بما قد يفضي إلى عواقب جسيمة وغير محمودة على الصعيد العالمي[٣٠].

٢- **استهداف البنية التحتية الاقتصادية:**أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال، الأمر الذي يجعل هذه الشبكات، بحكم طبيعتها المترابطة وانفتاحها على المحيط العالمي، هدفًا مغريًا للمجرمين والتنظيمات الإرهابية. وتزداد جاذبية الأهداف الاقتصادية والمالية نظرًا لتأثرها الكبير بالانطباعات السائدة والتوقعات العامة، إذ إن مجرد التشكيك في صحة المعلومات أو العبث بها بصورة محدودة قد يفضي إلى نتائج خطيرة، من شأنها زعزعة الثقة بالنظام الاقتصادي وإضعاف استقراره.ويشمل هذا التصور إحداث اضطراب واسع في نظم الشبكات التي تتحكم بسير عمل المصارف وأسواق المال العالمية، ونشر حالة من الفوضى في المعاملات والصفقات التجارية الدولية. كما يمكن أن يؤدي ذلك إلى تعطيل جزئي أو كلي لمنظومات التجارة والأعمال، بما ينعكس سلبًا على الحركة الاقتصادية العامة والاستقرار المالي.

٣- **استهداف نظم الاتصالات:**يشمل هذا التصور اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وتعطيل محطات توزيع خدمات الاتصالات، فضلًا عن تنفيذ هجمات متتابعة على شبكات الهواتف المحمولة، بما يؤدي إلى عرقلة الاتصال بين أفراد المجتمع ومؤسساته الحيوية، الأمر الذي يفضي إلى إشاعة حالة من الرعب والفوضى، ويحول دون القدرة على متابعة آثار الهجمات الإرهابية المعلوماتية[٣١].ولا يقتصر نطاق هذه الهجمات على ما تقدم فحسب، إذ تتعدد الأهداف الأخرى التي يمكن للمجرمين والإرهابيين استغلالها لإشاعة الفساد ونشر الفوضى. ومن بين هذه الأهداف شبكات المعلومات الطبية، حيث قد يؤدي اختراقها والتلاعب ببياناتها إلى خسائر بشرية جسيمة، كما حدث في بعض الدول الغربية عندما تم التلاعب بسجلات المستشفيات وملفات المرضى، الأمر الذي أسفر عن إعطاء أدوية وعلاجات كانت قاتلة لهم. وحتى مع افتراض متانة الأنظمة المعلوماتية للمؤسسات الطبية، فإن مجرد نشر رسالة إلكترونية تفيد بوجود دماء ملوثة في المستشفيات أو ما شابه ذلك، قد تكون كفيلة بإحداث آثار اجتماعية خطيرة ومدمرة.

الفرع الثاني التهديد والترويع الإلكتروني لقد عرف بعض الفقهاء التهديد بأنه فعل الشخص الذي ينذر آخر بخطر يريد إيقاعه بشخصه أو ماله، أو توجيه عبارة أو ما في حكمها إلى المجني عليه عمداً يكون من شأنها إحداث الخوف عنده من ارتكاب جريمة أو إفشاء سر أو نسبة أمور مخدشه بالشرف إذا وجهت بالطريقة التي يعاقب عليها القانون[٣٢]ومن خلال الشبكة العالمية للمعلومات (الإنترنت)، تتعدد أساليب التهديد وتتنوع وسائله، بما يهدف إلى نشر الخوف والرعب بين الأفراد والدول والشعوب، سعيًا للضغط عليهم وإجبارهم على الرضوخ لمطالب التنظيمات الإرهابية من جهة، ولتحقيق مكاسب مالية وإبراز قوة هذه التنظيمات من جهة أخرى. وتجدر الإشارة إلى أن المقصود بالتهديد يتمثل في الوعيد بإلحاق الضرر وبثّ الخوف في النفوس، عبر التأثير على إرادة الإنسان وتخويفه من احتمال وقوع أذى يلحق به أو بأشخاص أو أشياء تربطه بها صلة. وقد يلجأ إرهابيو الإرهاب الإلكتروني إلى استخدام أساليب التهديد وترويع الآخرين عبر وسائل الاتصال والشبكات المعلوماتية، بهدف تحقيق الغاية الإجرامية المنشودة. ومن أبرز الوسائل التي تعتمدها الجماعات الإرهابية في هذا الإطار إرسال الرسائل الإلكترونية المتضمنة عبارات التهديد، فضلًا عن التهديد عبر المواقع الإلكترونية، والمنتديات، وغرف الدردشة.وفي الواقع، تتعدد صور وأساليب التهديد الإرهابي؛ فقد يكون التهديد بالقتل موجّهًا إلى شخصيات سياسية أو عامة بارزة، وقد يتمثل في التهديد بتفجير المنشآت الوطنية، أو بنشر الفيروسات بقصد إلحاق الضرر بالشبكات

المعلوماتية والأنظمة الإلكترونية. كما قد يمتد التهديد ليشمل تدمير البنية التحتية المعلوماتية، وغير ذلك من الأساليب التي تلجأ إليها الجماعات الإرهابية لتحقيق أهدافها. ويستخدم الإرهابيون مختلف الوسائل لتحقيق غاياتهم، ومن بينها أساليب التهديد والترويع بمختلف صورها، عبر شبكات الاتصال والمعلومات، بما يعرّض حياة الأفراد للخطر، ويؤدي إلى إلحاق أضرار جسيمة بالبنى التحتية والشبكات المعلوماتية، الأمر الذي يفرض ضرورة تكثيف الجهود الدولية وتعزيز التنسيق والتعاون لمواجهة ظاهرة الإرهاب الإلكتروني.كان لانتشار استخدام شبكة الإنترنت على نطاق عالمي آثار عميقة في مختلف مجالات الحياة، ومن بينها اتساع نطاق الجريمة، ولا سيما جريمة التهديد. وتكمن خطورة هذه الجرائم المستحدثة في سهولة ارتكابها نتيجة سوء استخدام التقنيات المعلوماتية وما توفره من تسهيلات تقنية، فضلًا عن أن آثارها لا تقتصر على الإطار الإقليمي لدولة معينة، بل تمتد عبر الحدود، إضافة إلى ما يتمتع به مرتكبوها من مهارة ودراية في التعامل مع أنظمة المعالجة الآلية. وتلجأ الجماعات والتنظيمات الإرهابية إلى ممارسة التهديد عبر وسائل الاتصالات المختلفة، ولا سيما من خلال الشبكة العالمية للمعلومات(Internet) ، حيث تتعدد أساليب التهديد وتتنوع وسائله بهدف نشر الخوف والرعب بين الأفراد والدول والشعوب، والضغط عليهم للرضوخ لأهداف تلك التنظيمات من جهة، والحصول على التمويل المالي وإظهار قوة التنظيم الإرهابي من جهة أخرى.ويُقصد بالتهديد الوعيد بالشر وزرع الخوف في نفس الإنسان من خلال التأثير على إرادته وتخويفه من وقوع ضرر يلحق به أو بأشخاص أو أشياء تربطه بها صلة. وقد يلجأ مرتكبو الإرهاب الإلكتروني إلى استخدام أساليب التهديد والترويع عبر الاتصالات والشبكات المعلوماتية لتحقيق الغاية الإجرامية المرجوة، ومن أبرز هذه الأساليب إرسال الرسائل الإلكترونية المتضمنة للتهديد، فضلًا عن التهديد عبر المواقع الإلكترونية والمنتديات وغرف الحوار والدردشة الإلكترونية[٣٣].تنوّعت الأساليب التي تعتمدها الجماعات الإرهابية في مجال التهديد، إذ قد يكون التهديد موجّهًا بالقتل إلى شخصيات سياسية بارزة في المجتمع، وقد يتمثل أحيانًا في التهديد بتفجير منشآت وطنية، أو بنشر فيروسات إلكترونية بقصد إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، كما قد يتخذ التهديد صورة السعي إلى تدمير البنية التحتية المعلوماتية للدولة[٣٤].

الخاتمة

في ضوء ما تقدّم، يتبيّن أن الإرهاب الإلكتروني يُعد امتدادًا معاصرًا لظاهرة الإرهاب التقليدي، إلا أنه يتميز بوسائل أكثر تعقيدًا وخطورة، مستفيدًا من التطور التكنولوجي والفضاء الرقمي المفتوح لتحقيق أهدافه الفكرية والتنظيمية والعملية. وقد أظهر البحث أن نشوء الإرهاب الإلكتروني لا يرتبط بعامل واحد، بل هو نتاج تفاعل معقّد بين عوامل فكرية وعقائدية، وتقنية، واجتماعية، واقتصادية، فضلًا عن أوجه القصور التشريعي وضعف التعاون الدولي. كما أوضح البحث أن التصورات العملية للإرهاب الإلكتروني، كالتجسس والترويع والتهديد عبر الوسائط الرقمية، تشكّل تهديدًا مباشرًا لأمن الدول واستقرار المجتمعات، الأمر الذي يستوجب مقاربة قانونية وأمنية شاملة تقوم على الوقاية إلى جانب الردع.

وفي الختام توصلنا إلى جملة من الاستنتاجات والمقترحات وذلك على النحو الآتي:

أولاً: الاستنتاجات:

١. إن العوامل المؤثرة في نشوء الإرهاب الإلكتروني متعددة ومتشابكة، ويُعد التطور التكنولوجي غير المصحوب بضوابط قانونية وفكرية من أبرز المحركات التي أسهمت في توسّع هذه الظاهرة وانتشارها عابرًا للحدود.

٢. تُظهر التصورات العملية للإرهاب الإلكتروني أن هذا النمط الإجرامي لم يعد يقتصر على الدعاية أو التحريض، بل تطوّر ليشمل التجسس، والتهديد، والترويع، والتخطيط والتنفيذ غير المباشر للعمليات الإرهابية، بما يحدّ من فعالية الأدوات التقليدية لمكافحته.

ثانياً: المقترحات:

١. يوصي البحث بضرورة تطوير التشريعات الوطنية وتحديثها بما يواكب الأساليب المستحدثة للإرهاب الإلكتروني، مع وضع تعريف قانوني دقيق له، وتجريم أفعاله وصوره بصورة واضحة تضمن فعالية الردع دون المساس بالحقوق والحريات الأساسية.

٢. يقترح البحث تعزيز التعاون الدولي والإقليمي في مجال مكافحة الإرهاب الإلكتروني، ولا سيما في مجالات تبادل المعلومات، وبناء القدرات التقنية، ووضع استراتيجيات وقائية مشتركة تجمع بين المعالجة الأمنية والفكرية والتقنية.

قائمة المراجع

أولاً: الكتب القانونية

١. أحمد حسين سويدان، الإرهاب الدولي في ظل المتغيرات الدولية، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٩.

٢. أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، دار الجامعة الجديدة، مصر، ٢٠١٩.

٣. أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمّان، ٢٠١٠.
٤. أمير فرج يوسف، جريمة مكافحة الإرهاب الإلكتروني، دار الكتب والدراسات العربية، القاهرة، ٢٠١٦.
٥. حسنين المحمدي بوادي، تجربة مواجهة الإرهاب، دار الفكر الجامعي، مصر، ٢٠٠٥.
٦. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١٤.
٧. خالد سالم عبد المجيد فلاح، السياسة الجنائية الموضوعية في مواجهة الجريمة الإرهابية، الطبعة الأولى، دار النهضة العربية، مصر، ٢٠١٤.
٨. راستي الحاج، الإرهاب في وجه المساءلة الجزائية محليًا ودوليًا (دراسة مقارنة)، الطبعة الأولى، منشورات زين الحقوقية، بيروت، ٢٠١٢.
٩. زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي، منشورات الحلبي الحقوقية، بيروت، ٢٠١٨.
١٠. سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٠.
١١. سلمان عبد المنعم، علم الإجرام والجزاء، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، ٢٠٠٥.
١٢. عبد الجبار رشيد الجميلي، جرائم الإرهاب الدولي في ضوء اختصاص المحكمة الجنائية الدولية، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥.
١٣. عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، ٢٠٢٠.
١٤. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ٢٠١٣.
١٥. محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٤.
١٦. محمد حماد مرهج، التكنولوجيا الحديثة والقانون الجزائي، دار الثقافة للنشر والتوزيع، عمّان، ٢٠٠٤.
١٧. محمد علي سويلم، جرائم الإرهاب والإرهاب الإلكتروني، المكتبة المصرية، مصر، ٢٠١٩.
١٨. مصطفى محمد موسى، الإرهاب الإلكتروني، دار الكتب والوثائق المصرية، مصر، ٢٠٠٩.
١٩. منير الجنبيهي، ممدوح الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، القاهرة، ٢٠٠٦.
٢٠. نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١١.
٢١. هبة الله أحمد خميس، الإرهاب الدولي، الطبعة الأولى، منشورات جادة الإسكندرية، بيروت، ٢٠١٠.
٢٢. هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية، لبنان، ٢٠٠٥.
٢٣. يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١.

ثانياً: الاطاريح الجامعية:

١. تركي بن عبد الرحمن المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراه مقدمة إلى كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، ٢٠٠٩.

ثالثاً: المجلات والدوريات:

١. اسراء جواد كاظم، الإرهاب الرقمي المعلوماتي وطرق مكافحته، بحث منشور في مجلة العلوم القانونية والسياسية، العدد ٣٢٨، العراق، ٢٠١٠.
٢. جبار علي صالح، الجهود العربية لمكافحة الإرهاب، بحث منشور في مجلة دراسات دولية، العدد ٤٦، العراق، ٢٠١٠.
٣. جميل عبد الباقي الصغير، الإنترنت والإرهاب، بحث منشور في مجلة العلوم القانونية والسياسية، عدد خاص، جامعة ديالى، العراق، ٢٠١٢.
٤. عادل عبد الصادق، هل يمثل الإرهاب شكلًا جديدًا من أشكال الصراع الدولي، مقال منشور في جريدة الأهرام، العدد ١٥٦، مركز الأهرام للدراسات السياسية والاستراتيجية، مصر، ٢٠٠٧.
٥. عواطف محمد عثمان عبد الحليم، الجرائم المعلوماتية: تعريفها وصورها، بحث منشور في مجلة العدل، العدد الرابع والعشرون، العراق، ٢٠١١.

هوامش البحث

[1] عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، ٢٠٢٠، ص ٨٠.

[٢] حسنين المحمدي بوادي، تجربة مواجهة الإرهاب، دار الفكر الجامعي، مصر، ٢٠٠٥، ص ٢٨٨.

[٣] أحمد حسين سويدان، الإرهاب الدولي في ظل المتغيرات الدولية، منشورات الحلبي الحقوقية، لبنان ٢٠٠٩، ص١٦١ – ١٦٢.

[٤] سلمان عبد المنعم، علم الإجرام والجزاء، الطبعة الأولى، منشورات الحلبي للحقوقية، لبنان، ٢٠٠٥، ص ٢٧٤.

[٥] محمد حماد مرهج، التكنولوجيا الحديثة والقانون الجزائي، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٤، ص ٤٤.

[٦] راستي الحاج، الإرهاب في وجه مساءلة الجزائية محلياً ودولياً "دراسة مقارنة"، الطبعة الأولى، منشورات زين الحقوقية، بيروت، ٢٠١٢، ص١١٩.

[٧] أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٠، ص٢٣١.

[٨] هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، دار الكتب العلمية، لبنان، ٢٠٠٥، ص ١٣٨.

[٩] جبار علي صالح، الجهود العربية لمكافحة الإرهاب، بحث منشور في مجلة دراسات دولية، العدد ٤٦، العراق، ٢٠١٠، ص١٣٢.

[١٠] نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١١، ص١٤٠.

[١١] احمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، دار الجامعة الجديدة، مصر، ٢٠١٩، ص٧٢.

[١٢] هبة الله أحمد خميس، الإرهاب الدولي، الطبعة الأولى، منشورات جاده الإسكندرية، بيروت – لبنان، ٢٠١٠، ص ٧١.

[١٣] أحمد حسين سويدان، الإرهاب الدولي في ظل المتغيرات الدولية، مرجع سابق، ص٢٠٠.

[١٤] أمير فرج يوسف، جريمة مكافحة الإرهاب الإلكتروني، دار الكتب والدراسات العربية، القاهرة، ٢٠١٦، ص١٠١.

[١٥] زين العابدين عواد كاظم الكردي، جرائم الإرهاب المعلوماتي، منشورات الحلبي الحقوقية، بيروت، ٢٠١٨، ص٥٦.

[١٦] هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، مرجع سابق، ص ١٤٠.

[١٧] محمد السعيد رشدي، الإنترنت والجوانب القانونية لنظم المعلومات، دار النهضة العربية، القاهرة، ٢٠٠٤، ص٢٤.

[١٨] سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، ٢٠١٠، ص١٠٦.

[19] عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي، مرجع سابق، ص١٣٤.

[20] سعد صالح الجبوري، الجرائم الإرهابية في القانون الجنائي، مرجع سابق، ص١١١.

[٢١] عبد الجبار رشيد الجميلي، جرائم الإرهاب الدولي في ضوء اختصاص المحكمة الجنائية الدولية، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥، ص١٢٦.

[٢٢] اتخذ مجلس الأمن القرار ١٣٧٣ في ٢٨ سبتمبر ٢٠٠١، وألزم جميع الدول بمكافحة تمويل الإرهاب وتجميد الاعتمادات المالية والأصول الأخرى والموارد الاقتصادية للدول التي تصنع الإرهاب أو تشجع الإرهاب أو تسهل ذلك بصورة مباشرة أو غير مباشرة، وكذلك الأشخاص الذين يتصرفون باسمها، أو بناء على تعليمات من هذه الدول أو هيئاتها.

[٢٣] محمد علي سويلم، جرائم الإرهاب والإرهاب الإلكتروني، المكتبة المصرية، مصر، ٢٠١٩، ص٤٥.

[٢٤] عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الالكتروني في القانون الدولي، مرجع سابق، ص٤٥.

[٢٥] مصطفى محمد موسى، الارهاب الإلكتروني، دار الكتب والوثائق المصرية، مصر، ٢٠٠٩، ص٧٨.

[٢٦] جميل عبد الباقي الصغير، الإنترنت والإرهاب، بحث منشور في مجلة العلوم القانونية والسياسية عدد خاص، جامعة ديالي، العراق، ٢٠١٢، ص٦.

[٢٧] عادل عبد الصادق، هل يمثل الإرهاب شكل جديداً من أشكال الصراع الدولي، مقال منشور في جريدة الأهرام، العدد ١٥٦، مركز تصدر عن الأهرام للدراسات السياسية والاستراتيجية، مصر، ٢٠٠٧، ص٣٤.

[٢٨] مصطفى محمد موسى، الارهاب الإلكتروني، مرجع سابق، ص٩٠.

[٢٩] منير الجنبيهي وممدوح الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، القاهرة، ٢٠٠٦، ص١٠١.

(٣٠) يوسف حسن يوسف، الجرائم الدولية للأنترنت، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١١، ص١٢

(٣١) تركي بن عبد الرحمن المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة أعدت لنيل درجة دكتوراه، مقدمة إلى كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية، ٢٠٠٩، ص١٧٥.

(٣٢) عواطف محمد عثمان عبد الحليم، جرائم المعلوماتية– تعريفها– صورها، بحث منشور في مجلة العدل، العدد الرابع والعشرون، العراق، ٢٠١١، ص٦٩.

(٣٣) نايف بن محمد المرواني، تمويل الإرهاب إلكترونياً التحديات وطرق المواجهة، بحث منشور في المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٩، العدد٥٨، السعودية، ٢٠١٣، ص١٨.

(٣٤) علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، بيروت، ٢٠١٣، ص٢٣١.