Arabian Gulf Journal of Humanities and Social Studies

ISSN: 3080-4086

الإصدار السابع - العدد العشرون || تاريخ الإصدار 2026-11-20

الإرهاب الإلكتروني بين التطور التقني وخطورة الجرائم الإلكترونية : دراسة قانونية في صور التجريم وآليات المواجهة

Cyberterrorism Between Technological Advancement and the Threat of Cybercrime: A Legal Study of Criminalization Forms and Countermeasures

محمد جاسر محمد الطروه

Mohammad Jaser Mohammad Altaraweh

جامعة القدس - فلسطين

DOI: https://doi.org/10.64355/agjhss7206

مجلة خليج العرب للدراسات الإنسانية والاجتماعية || هذه المقالة مفتوحة المصدر موزعة بموجب شروط وأحكام ترخيص مؤسسة المشاع الإبداعي(CC BY-NC-SA)

الملخص:
أصبح الإرهاب واحدا من أهم الظواهر التي تهدد امن واستقرار 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 الاقتصادية والسياسية والاجتماعية فأصبح إرهاب عابر للحدود .

وعلى الرغم من أنه لا يوجد اختلاف بين أسباب ودوافع الإرهاب الإلكتروني عن أسباب ودوافع الإرهاب التقليدي إلا انها تختلف في مدى تأثيرها باختلاف المجتمع المعتدى عليه حيث تنقسم الأسباب إلى نوعين وهى الأسباب العامة والأسباب الخاصة وتبرز العامة في الاسباب السياسية، الاقتصادية، الاجتماعية، الشخصية المادية، الفكرية، ومن أبرز الأسباب الخاصة ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق غياب الحدود الجغرافية وتدني مستوى المخاطرة، سهولة الاستخدام 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 الاعتماد على التكنولوجيا المتطورة.

الكلمات المفتاحية: الإرهاب الإلكتروني؛ الأمن القومي؛ الجرائم الإلكترونية؛ الحماية القانونية.

Abstract:

Terrorism has become one of the major phenomena threatening the security and stability of states. The Internet has contributed to the growing severity of this threat, as terrorism is no longer confined to its traditional concept based on violence and intimidation, but has extended to a newly emerging form known as cyberterrorism. Cyberterrorism is a complex and dangerous concept due to the technical complexities arising from the information revolution and modern technologies. The concept of terrorism is no longer restricted by geographical or temporal boundaries; rather, it has become a significant threat to countries worldwide, affecting their economic, political, and social systems, and has evolved into a transnational phenomenon.

Although the causes and motivations of cyberterrorism do not fundamentally differ from those of traditional terrorism, their impact varies depending on the society targeted. These causes can be divided into two categories: general and specific causes. General causes include political, economic, social, personal, material, and ideological factors. Specific causes include the weakness of information network infrastructure and its vulnerability to penetration, the absence of geographical boundaries, low levels of risk, ease of use and low cost, the difficulty of detecting and proving terrorist crimes, regulatory and legal gaps, and the absence of an effective authority to control and monitor information networks. Ultimately, cyberterrorism emerges within the digital environment and relies on technological knowledge and tools. Accordingly, cyberterrorism represents a threat to national security, particularly in light of the increasing dependence on advanced technologies.

Keywords: Cyberterrorism; National Security; Cybercrime; Legal Protection.

المقدمة:

إن التطور التكنولوجي المتسارع الذي يشهده العالم اليوم في ظل الثورة المعلوماتية الحديثة التي تلت الثورة الصناعية، فرض على الإنسان الاعتماد على تقنيات التكنولوجية واستعمالها في مجالات العمل والحياة، وأصبح العالم بذلك عبارة عن قرية صغيرة يمكن التواصل بين مجتمعاته بلا حدود جغرافية او زمنية او 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 الانعكاسات السلبية التي نتجت عن اساءة استخدام الأنظمة المعلوماتية، واستغلالها بطريقة غير شرعية بغرض الاضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط وصور مستحدثة من الاعمال الإرهابية تحت مسمى أعمال الإرهاب الإلكتروني.

وقد ادى التقدم التكنولوجي الهائل وخاصة في مجال الاتصالات إلى تطور الأعمال الإرهابية بوجه عام وظهور أنماط جديدة على المستوى الوطني والإقليمي والعالمي، فزادت معاناة دول العالم من النشاطات الإرهابية وفي ظل ثورة المعلومات والمعرفة الإلكترونية وتطور وسائل الاتصال 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.

ولا بد من الإشارة هنا الى التطور في القوانين الداخلية للدول بما يعكس الحماية من الارهاب الالكتروني على المستوى الداخلي فنشير الى القانون الفلسطيني بشأن الجرائم الإلكترونية، وخاصة قرار بقانون رقم 10 لسنة 2018 وتعديلاته مثل قرار بقانون رقم 28 لسنة 2020، الذي يعالج الجرائم الإلكترونية المتعلقة بالإرهاب ويتضمن مواد تجرم انشطة مثل استخدام الإنترنت في التهديد والابتزاز ونشر مواد التحريض على العنف أو الإرهاب وتمويل الإرهاب إلكترونيا كما ينص القانون على عقوبات صارمة تشمل السجن وغرامات مالية ويشمل أيضا إجراءات أمنية وقضائية خاصة بالجرائم الإلكترونية مثل تتبع الأدلة الإلكترونية والتحفظ على الأجهزة.[1]

إشكالية البحث:

أصبح الإرهاب اليوم واحدا 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 عمليا 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 الارهابية عبر الانترنت امر صعب التحقيق فبإمكانهم تبادل رسائل إلكترونية مشفرة في شكل صورة عادية أو مقطع فيديو.

وفي هذا الإطار يحاول الباحث الإجابة على التساؤل الرئيسي المتمثل في:

ما المقصود بمفهوم الإرهاب الإلكتروني؟

ويتفرع عن هذا التساؤل عدة تساؤلات فرعية من أهمها:

1- ما هي المفاهيم المرتبطة والمتداخلة مع الإرهاب الإلكتروني؟

2- ما هي أسباب ودوافع الإرهاب الإلكتروني؟

3- ما هي اساليب الارهاب الالكتروني وما هي اثاره؟

4- الحماية القانونية للحد من الارهاب الإلكتروني؟

5- الفرق بين الارهاب الالكتروني والجرائم الالكترونية وحرب المعلومات؟

منهجية البحث:

لذلك أعتمد الباحث على المنهج الوصفي التحليلي والمنهج المقارن، من خلال تفسير ظاهرة الارهاب الالكتروني وما له من تداعيات واثار على الامن القومي ومقارنة بعض قوانين الدول المجاورة بالقانون الفلسطيني.

[1] - قرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الالكترونية
ان القرار بقانون رقم (10) لسنة 2018 اعتمد سياسة تشريعية وقائية، حيث امتد نطاق التجريم ليشمل الأفعال التحضيرية والمساعدة، وليس فقط النتائج النهائية للجريمة، إدراكاً لخطورة الفضاء الإلكتروني كوسيلة سريعة الانتشار والتأثير. ويلاحظ أن هذا النهج يكمل أحكام التشريعات الخاصة بمكافحة الإرهاب إذ يشكل قانون الجرائم الإلكترونية الأداة القانونية التي تضبط الوسيلة في حين تضبط قوانين مكافحة الإرهاب الغاية الإجرامية.

أهمية البحث:

1. تزايد الاعتماد على التكنولوجيا وتوسّع استخدام الإنترنت في الحكومات والمؤسسات المالية والعسكرية والتعليمية، أصبح فهم تهديدات الإرهاب الإلكتروني ضرورياً لحماية البنية التحتية الرقمية.
2. خطورة الهجمات الإلكترونية مقارنة بالهجمات التقليدية اذ يمكن للهجوم الإلكتروني أن يسبب خسائر مالية وسياسية وأمنية هائلة دون استخدام أسلحة مادية، بل فقط عبر اختراقات تقنية.
3. الانتشار العالمي لتهديدات الإرهاب الإلكتروني لا يعترف بالحدود الجغرافية، مما يجعله خطراً عالمياً يتطلب دراسة معمقة لفهم طرق عمله وأساليبه الحديثة.

أهداف البحث:

1. تحديد مفهوم الإرهاب الإلكتروني وتعريفه العلمي وتوضيح الفرق بين الإرهاب الإلكتروني والجرائم الإلكترونية العادية.
2. التعريج على القوانين ومدى فعاليتها وشمولها للحد من الارهاب الالكتروني.
3. دراسة الأساليب والتقنيات المستخدمة في الهجمات الإرهابية الإلكترونية مثل: الاختراق، الهجمات الموزعة(DDoS) ، نشر البرمجيات الخبيثة، التجسس الرقمي.

خطة البحث:

قام الباحث بتقسيم البحث الى مطلبين:

المطلب الأول: مفهوم الإرهاب الإلكتروني

الفرع الأول: معنى الارهاب الالكتروني وتعريفاته

الفرع الثاني: الفرق بين الإرهاب الإلكتروني والجرائم الإلكترونية الاخرى

المطلب الثاني : اسباب انتشار الارهاب الالكتروني ودوافعه.

الفرع الاول : العوامل التقنية المساعدة على انتشار الارهاب الالكتروني

الفرع الثاني : مدى فعالية القوانين الداخلية للحد من الارهاب الالكتروني

المطلب الاول: مفهوم الإرهاب الإلكتروني

وجدنا في الآونة الاخيرة تطور الانترنت بصورة أصبح استخدامه متاحا في كل بيت وازداد هذا التطور بشكل مهول في السنوات الاخيرة بحيث ادا هذا التطور الى استخدام شبكة الانترنت لشن هجوما تخريبيا يثير الذعر او يعطل الانظمة وذلك لتحقيق مكاسب سياسية او مالية .

ونجد هنا انه امتداد للإرهاب التقليدي من ناحية بث الرعب والذعر لدى المواطنين ويضرب بشكل هجومي مباغت الا ان الاختلاف الحقيقي ان الارهاب الإلكتروني يكون في الفضاء ومن خلال شبكات يصعب السيطرة عليه من قبل الحكومات بشكل سريع او متوقع .

الفرع الأول: معنى الارهاب الالكتروني وتعريفاته

لا يوجد تعريف 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، وعلى الرغم من أن الخبراء لم يشكلوا تعريفاً اجتماعيا للإرهاب، فلا يوجد حتى الان تعريف موحد للإرهاب الإلكتروني، وقد وضح بارى كولن صعوبة تعريف الإرهاب الإلكتروني 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.[2]

وحيث أننا نواجه اليوم اسلحة جديدة وغير مألوفة، فإن أنظمة الاستخبارات 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 يهاجم بشحنات محملة بالمتفجرات ولا بحقائب الغاز ولا بالديناميت مربوط بأجساد المتعصبين، فهذا العدو يهاجم بأسلوب واحد صفر وفي مكان نكون فيه أكثر عرضة للخطر وهى النقطة التي يتقارب فيها العالمان المادي والافتراضي ويشكل الإرهاب الإلكتروني السلاح الجديد الذي نواجهه، بحيث يزداد الأمر حجما وأكثر تعقيدا.

كلما غامرنا أكثر في الاعتماد على التكنولوجيا ففي كل يوم نتقدم بسرعة هائلة في 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.[3]

وممكن مما سبق تعريف الارهاب الالكتروني: على أنه التقاء بين الفضاء الإلكتروني والإرهاب يكون بطريقة هجمات غير قانونية وتهديدات بالهجوم على أجهزة الحاسب الألي والشبكات والمعلومات المخزنة عليها، وذلك لتخويف أو إكراه حكومة أو شعبها من أجل تحقيق أهداف سياسة أو مالية، ولكي يصنف الهجوم على أنه إرهاب إلكتروني، يجب أن يؤدي الهجوم إلى عنف ضد الأشخاص أو الممتلكات أو على الأقل التسبب في ضرر كاف ينتج عنه توليد الخوف، ومن الأمثلة على ذلك: الهجمات التي تؤدي إلى الموت أو الإصابة الجسدية أو الانفجارات أو الخسائر الاقتصادية الفادحة، الهجمات الخطيرة ضد البنى التحتية الحيوية، الهجمات التي تعطل الخدمات الأساسية، كل ذلك يعد من أعمال الإرهاب الإلكتروني اعتمادا على تأثيرها الفادحة، الهجمات الخطيرة ضد البنى التحتية الحيوية، الهجمات التي تعطل الخدمات الأساسية، كل ذلك يعد من أعمال الإرهاب الإلكتروني اعتمادا على تأثيرها.

ومن الناحية الاصطلاحية، فيعرف الإرهاب على أنه "الاستخدام العمدي والمنظم لوسائل من طبعها إثارة الرعب والفزع بقصد تحقيق بعض الأهداف "، كما يعرف أيضا بأنه " أحد مظاهر العنف الاجتماعي وعليه فهو ظاهرة مركبة ومتعددة الأبعاد يختلط فيها العنصر النفسي بالعناصر الاجتماعية والمادية والثقافية والسياسية والتاريخية "[4]

أما الاتفاقية العربية لمكافحة الإرهاب فقد عرفته على أنه " كل فعل من أفعال العنف أو التهديد أيا كانت بواعثه أو أغراضه يقع تنفيذا لمشروع إجرامي فردي أو جماعي، ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر

---

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

تعريف فقهي موسع

يعرف بعض فقهاء القانون الإرهاب الإلكتروني بأنه:

(استخدام الوسائل الإلكترونية وتقنيات المعلومات استخداماً منظماً بقصد بث الرعب في نفوس الأفراد أو تهديد أمن المجتمع أو تقويض النظام العام، من خلال التحريض أو التخطيط أو الدعم أو التنفيذ غير المباشر للأعمال الإرهابية)

تعريف يركز على الوسيلة

ويرى اتجاه فقهي آخر أن الإرهاب الإلكتروني هو:

(كل نشاط إجرامي ذي طابع إرهابي يُرتكب عبر شبكات الإنترنت أو أنظمة المعلومات، ويستهدف الدولة أو المجتمع أو الأفراد، ويحقق ذات الأغراض التي تسعى إليها الأعمال الإرهابية التقليدية)

تعريف يربط بين الغاية والنتيجة

ويذهب بعض الفقه إلى تعريفه بأنه:

(نمط مستحدث من الإرهاب تتحقق فيه الجريمة الإرهابية باستخدام الفضاء الإلكتروني كوسيلة رئيسية، متى كان من شأن هذا الاستخدام إحداث خطر جسيم على الأمن العام أو السلم الأهلي أو المصالح الحيوية للدولة).

تعريف وقائي حديث

كما عرّفه فقه معاصر بأنه:

(مجموعة الأفعال الرقمية غير المشروعة التي تُستغل فيها التكنولوجيا الحديثة للتحريض أو الترويج أو التجنيد أو التمويل لأغراض إرهابية، ولو لم يترتب عليها عنف مادي مباشر)

[3] - 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.

[4] - عبد الصادق، عادل، الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة (القاهرة: مركز الدراسات السياسية والإستراتيجية بالأهرام، 2009، ص789.

بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر · ويتضح من التعريفات السابقة أن جوهر الإرهاب هو حالة الرعب التي يتمكن فاعلها من فرض سيطرته لتحقيق هدف ما.[5]

الفرع الثاني: الفرق بين الإرهاب الإلكتروني والجرائم الإلكترونية وحرب المعلومات

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 الاستخدام 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 الاستخدام السيئ للفضاء الإلكتروني أو الاستخدام ذو الطابع الإجرامي أو الاستخدام كأداة إرهابية، ويرجع ذلك إلى أن هناك عديد من الأنماط قد يمكن اعتبارها جميعاً إرهاباً إلكترونياً إذا ما وجهت إلى هدف معين وذا أغراض سياسية، أما إذا فقدت تلك الأنماط الصبغة السياسية فإنها يمكن تصنيفها ضمن كل نمط صفة 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 لارتكاب جريمة ما أو استخدامه بشكل غير قانوني من قبل الأفراد المرخص لهم باستخدامه.

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 في تشوية سمعة الأشخاص، والمواقع البريدية الإباحية، وغسل الأموال، وتزوير البيانات، والقمار عبر شبكة الإنترنت، وتهديدات التجارة الإلكترونية، والجرائم الاقتصادية، وانتحال شخصية الأفراد وشخصية المواقع وانتهاك الخصوصية، والإغراق بالرسائل، وفيروسات الحواسيب الآلية، والاقتحام 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 نتيجة لسهوله محو الدليل أو تدميره في زمن قياسي، كما قد يكون هناك إحجام عن الابلاغ تلك الجرائم خشية من التأثير الاقتصادي في مجتمع الأعمال، بالإضافة إلى نقص الخبرة الكافية لدى جهات القضاء والادعاء والأجهزة الأمنية في هذا النوع من الجرائم.[6]

---

[5] - الاتفاقية العربية لمكافحة الإرهاب - https://hrlibrary.umn.edu/arabic/a-terroh.html
اعتمدت الاتفاقية العربية لمكافحة الإرهاب لسنة 1998 في مرحلة كان الإرهاب فيها يتخذ في الغالب صوراً تقليدية قائمة على العنف المادي المباشر، إلا أن المشرّع العربي حرص على صياغة تعريف واسع للإرهاب لم يقيّده بوسيلة معينة، وإنما ركّز على غاية الفعل الإرهابي ونتيجته المتمثلة في بث الرعب وتهديد الأمن العام والنظام العام. وقد أتاح هذا النهج المرن إدخال الأشكال المستحدثة للإرهاب ضمن نطاق الاتفاقية، وعلى رأسها الإرهاب الإلكتروني.
ومع تطور وسائل الاتصال الحديثة واتساع استخدام الفضاء الإلكتروني في التحريض والتجنيد والتخطيط والتمويل للأعمال الإرهابية، برز الإرهاب الإلكتروني كأحد أخطر أنماط الإرهاب المعاصر، لما يتميز به من سرعة الانتشار، وصعوبة التتبع، وعابريته للحدود. وعلى الرغم من أن الاتفاقية لم تذكر الإرهاب الإلكتروني صراحة، إلا أن نصوصها تستوعبه بوصفه وسيلة حديثة لارتكاب الجريمة الإرهابية متى تحققت الأهداف التي سعت الاتفاقية إلى مكافحتها

[6] - عبد الصادق، 2009، مرجع سابق، ص 129-130.
من الممكن توضيح **الفرق بين الإرهاب الإلكتروني والجريمة الإلكترونية** على النحو الآتي:
الإرهاب الإلكتروني :هو استخدام الوسائل والتقنيات الإلكترونية لتحقيق غايات إرهابية، كبث الرعب في المجتمع، أو تهديد الأمن العام، أو تقويض النظام العام أو السلم الأهلي، وغالباً ما يكون ذا بعد سياسي أو أيديولوجي، ويستهدف الدولة أو المجتمع ككل.
أما الجريمة الإلكترونية فهي كل فعل غير مشروع يُرتكب باستخدام الحاسوب أو الإنترنت، ويهدف عادةً إلى تحقيق منفعة شخصية أو مالية، مثل الاحتيال الإلكتروني، أو سرقة البيانات، أو اختراق الحسابات، دون أن يكون الهدف منها تهديد أمن الدولة أو بث الرعب العام.
الخلاصة المبسطة:
الاختلاف الجوهري لا يكمن في الوسيلة (فكلتاهما تستخدم الإنترنت)وإنما في الغاية؛ فالإرهاب الإلكتروني يستهدف الأمن العام والنظام السياسي، بينما الجريمة الإلكترونية تستهدف الأفراد أو الأموال لتحقيق مصلحة خاصة.

يتضح لنا الفرق بين الارهاب الالكتروني والجريمة الكترونية وبشكل مبسط ان الإرهاب الإلكتروني والجرائم الإلكترونية رغم اشتراكهما في استخدام الفضاء الرقمي، الا ان الإرهاب الإلكتروني يقوم على دافع أيديولوجي أو سياسي يهدف إلى بث الرعب وزعزعة الأمن القومي أو التأثير على استقرار الدولة، بينما ترتبط الجرائم الإلكترونية غالبا بـدوافع مادية أو شخصية كسرقة البيانات أو الاحتيال أو الابتزاز.

كما أن الإرهاب الإلكتروني يستهدف عادة البنية التحتية الحيوية والمؤسسات الحكومية لتحقيق أثر واسع ومجتمعي، في حين تتجه الجرائم الإلكترونية إلى الأفراد أو الشركات لتحقيق مكاسب غير مشروعة. ويتميز الإرهاب الإلكتروني بطابعه المنظم وعلاقته بالجماعات المتطرفة، بخلاف الجرائم الإلكترونية التي قد يرتكبها أفراد أو مجموعات لأغراض ودوافع شخصية.

2- الإرهاب الإلكتروني وحرب المعلومات:

المقصود بحرب المعلومات استخدام نظم المعلومات لاستغلال 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 والاقتصادية. أما وزارة الدفاع الأمريكية تنظر إلى حرب المعلومات على أنها تلك الأعمال التي تتخذ لإحراز التفوق المعلوماتي بمساعدة الإستراتيجية القومية العسكرية للتأثير بالسلب على معلومات العدو ونظم معلوماته، وحماية ما لديها من معلومات ونظم

وتنقسم حرب المعلومات إلى ثلاثة مستويات على التوالي وهي شخصية، ومؤسسية، وعالمية:

أ- حرب المعلومات الشخصية: هي الحرب التي يتم فيها الهجوم على خصوصية الأشخاص في الفضاء المعلوماتي من خلال التصنت عليهم ومراقبة شؤونهم الإلكترونية عبر البريد الإلكتروني.

ب- حرب المعلومات المؤسسية: هي الحرب التي تدور ضمن إطار المنافسة أكثر من العداء وهى حرب يكون قوامها استباحة كل شيء لتعطيل المنافس وتهديد أسواقه، فقد تقوم شركة باختراق 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 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 يكتشف منها وهو أكثر بكثير وغير معلوم مداه.

ت- حرب المعلومات العالمية: هي الحرب التي تنشب بين الدول وبعضها البعض أو قد تشنه القوى الاقتصادية العالمية ضد دول معينة، لسرقة أسرار أعدائها وتوجيه تلك المعلومات ضدها وهي حروب قائمة وجارية بالفعل. فالنهاية يظل دور تكنولوجيا المعلومات هو جعل الأسلحة أذكى والخسائر أقل على عكس الحروب التقليدية.

تكون الأداة في حرب المعلومات هي الحاسب الالي 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[7]

وتعتبر حرب المعلومات هي ضربة استباقية 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 الارتكاب أو التعرف على مرتكبيها فهي لا تترك أثراً خلفها.

مما سبق يتضح لنا أن هناك علاقة وثيقة بين الإرهاب الإلكتروني[8] 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 إرهابي سواء كانت من خلال من يقف وراء استخدامها كالجماعات الإرهابية أو من خلال الحكم عليها وفقاً لطريقة التنفيذ التي تأخذ نفس تكتيكات العمل الإرهابي، وفي النهاية يمكن القول أن كل تلك الأشكال تعبر عن استخدام غير سلمي للفضاء الإلكتروني تعد إرهابا في طرق تنفيذها الذي يعتمد على الخوف والترويع وهجمات الكر والفر.[9]

---

[7] - **حرب المعلومات**: هي استخدام المعلومات وتقنيات جمعها ومعالجتها ونشرها للتأثير على الخصم، بهدف تعطيل قدراته أو توجيه سلوكه أو تحقيق تفوق استراتيجي دون مواجهة تقليدية.

[8] - **الإرهاب الإلكتروني**: هو استخدام الوسائل الرقمية لتنفيذ أو دعم أعمال تهدف إلى بثّ الرعب أو الإضرار بالأمن العام لتحقيق أهداف إرهابية.
الجريمة الإلكترونية: هي أي فعل غير مشروع يُرتكب باستخدام الحاسوب أو الإنترنت، مثل اختراق الأنظمة أو سرقة البيانات أو الاحتيال عبر الشبكة.

[9] - عبد الصادق، 2009، مرجع سابق، ص 135.

المطلب الثاني: أسباب الإرهاب الإلكتروني ودوافعه:

في القانون الفلسطيني، كما في أغلب التشريعات، يتم تناول الإرهاب الإلكتروني من خلال قوانين الجرائم الإلكترونية وقوانين مكافحة الإرهاب. ورغم أن النصوص قد تختلف بين تشريعات فلسطين (الضفة الغربية/غزة) تبعاً لاختلاف الحقب التشريعية، إلا أنّ أسباب الإرهاب الإلكتروني ودوافعه تُفهم من خلال تحليل نصوص قانون الجرائم الإلكترونية الفلسطيني (مثل القرار بقانون رقم 16 لسنة 2017 وتعديلاته) ومن خلال المبادئ العامة لقانون العقوبات. وبذلك تكون اسباب انتشار الارهاب الالكتروني في فلسطين يكاد يكون مبني على ركائز عامه تتغلف مع الكثير من العالم ومتشابهها لها من حيث اسباب ودوافع الارهاب الالكتروني لذا نتعرج الى الفرع الاول من هذا المطلب لبيان العوامل التي ساعدة على انتشار الارهاب الالكتروني بشكل عام

الفرع الأول: العوامل المساعدة على انتشار الارهاب الإلكتروني:

لا تختلف أسباب ودوافع الإرهاب الإلكتروني عن أسباب ودوافع الإرهاب التقليدي، إنما تختلف في مدى تأثيرها باختلاف المجتمع المعتدى عليه، وتنقسم الأسباب إلى نوعين وهي الأسباب العامة والأسباب الخاصة:

1- **الأسباب العامة:** غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروات الوطنية والخدمات والمرافق الأساسية، والاستيلاء على الأموال العامة وانعدام الأمانة، والتقصير والإهمال في أمور الرعية وعدم تسهيل أمورهم المعيشية والإنسانية.

2- **الأسباب السياسية**: إن من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب الإلكتروني ما يتعلق بسياسات الدول وخصوصا السياسات الاستبدادية غير العادلة التي تتبعها بعض الدول ضد مواطنيها، على سبيل المثال: الكبت السياسي، غياب المشاركة السياسية، التهميش السياسي لدور المواطنين، انتهاك الحقوق الإنسانية، علم تفعيل دور مؤسسات المجتمع المدني، عدم تلبية متطلبات التوازن الاجتماعي.

نجد هنا وبشكل عام ان الإحباط السياسي وانعدام حرية الرأي وغياب الديمقراطية من شأنه أن يولد ردود أفعال غاضبة لدى المواطنين وبالتالي لا تجد ما تصب فيه غضبها سوى الأعمال الإرهابية وذلك يكون بشكل خاص باستخدام الفضاء الالكتروني لرفع الاضطهاد والظلم التي تعاني منه بعض المجتمعات والشعوب الدولية، سواء كان نتيجة للسيطرة الاستعمارية أو انتهاك للحقوق والحرمات أو سلب الأموال أو خرق القوانين والمواثيق الدولية، كل ذلك دفع تلك الشعوب للتشدد والتطرف.[10]

بالنتيجة يجد الباحث ان احساس الفرد أنه مضطهد والشعور بأن حقوقه مسلوبة في المجتمع، يساعده على الانضمام لأي جهة أو جماعة لإزالة ما وقع عليه من ظلم أو قهر ومساعدته في الحصول على حقوقه، وهنا تكون الفرصة مناسبة للجماعات والتنظيمات المتطرفة لاحتواء مثل هؤلاء الأفراد، واستغلال دوافعهم والاستمرار في تضخيمها.

وفي اغلب الاحيان 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.

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 للاستحواذ عليها.

محاولة فرض مذهب سياسي أو رؤية عقائدية أو سياسية معينة أو إقامة كيان سياسي، أو إثارة النعرات الطائفية والمذهبية والتحريض على الاضطراب والفوضى التي قد تهد الوحدة الوطنية بين الشعوب وتعرضها للخطر.

3- **الأسباب الاقتصادية:** إن من أهم الأسباب الاقتصادية لظاهرة الإرهاب الإلكتروني ما يلي:

المشكلات الاقتصادية 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 واستخدام الإرهاب كنوع من التمرد على الواقع لمحاولة استرداد حقوقهم الاقتصادية المسلوبة من خلال استخدام الوسائل الإرهابية.

[10] - الداغر، مجدي محمد عبد الجواد ، دور الإعلام في تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الإنترنت : دراسة ميدانية، (الكويت: حوليات الآداب والعلوم الاجتماعية، مجلس النشر العلمي، جامعة الكويت، 2016، ص89).

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

التفاوت بين طبقات المجتمع الواحد، وتفرد جماعات أو قوى معينة بالاستحواذ على الموارد الاقتصادية، واتساع الفجوة الاقتصادية وتدني المستوى المعيشي بينهم، وزيادة الفوارق الاجتماعية بين فئات المجتمع، كل ذلك سيولد نوع من الحقد والكراهية والأنانية بلا شك، كما أن التأثيرات السلبية للأنظمة الاقتصادية من الممكن أن تنعكس بالسلب على السلوك البشري، والذي قد يدفع بعض الأفراد إلى القيام بالأعمال الإجرامية والعنف والقيام بأعمال غير قانونية من خلال استخدام وسائل الإرهاب الإلكتروني للانتقام من بعض فئات المجتمع الأخرى التي حرمتهم من أبسط حقوقهم الاقتصادية.[11]

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

4- **الأسباب الاجتماعية**: إن من أهم الأسباب الاجتماعية لظاهرة الإرهاب الإلكتروني ما يلي:

التفكك الأسري: تعد الأسرة هي الخلية الاجتماعية الأولى التي يعيش فيها الفرد وينمو، لذلك يجب أن تكون الأسرة سليمة وصالحة لتربية الأفراد تربية أخلاقية حسنة، فالإنسان منذ صغره يتأثر بالوسط الأسري الذي يعيش فيه، وتعتبر الأسرة هي المرآة التي تعكس أخلاق الفرد الذي نشأ في أحضانها.

البيئة الاجتماعية غير السليمة التي يعيش فيها الأفراد، مثل التفكك الأسري والاجتماعي، وانهيار دور الأسرة في التنشئة الاجتماعية السليمة، نقص المستوى التعليمي، وضعف دور المؤسسات التعليمية التربوية، تعد بيئة خصبة لجذب الشباب إلى الانحراف والتطرف وارتكاب الأعمال الإرهابية.

لذلك فإن المجتمع المتماسك والأسرة المترابطة تحيط الأشخاص بشعور التمامك والتعاون واحتواء من شذ عنهم ورده عن الظلم، فالمجتمعات ذات الترابط الأسري لا تظهر فيها الأعمال الإرهابية بنفس القدر الذي تظهر فيه عند المجتمعات المفككة اجتماعيا.

نقص المستوى التعليمي: غالبية المتورطين في قضايا الإرهاب قديماً كانوا من الأميين، حيث كانوا أكثر عرضة للانضمام للجماعات الإرهابية، فالجهل ونقص المستوى التعليمي من العوامل التي تساعد في سرعة الانتماء للجماعات الإرهابية، وهي نتيجة طبيعية ومتوقعة، حيث لا يتوقع من شخص متعلم ومستمر في الدراسة أن ينساق بسهولة وبسرعة للجماعات الإرهابية المتطرفة، فالإرهاب الحديث اليوم يعتمد على الفكر والثقافة ومهارات الإنترنت والتخصصات النادرة أو ما يعرف بالإرهاب الإلكتروني. [12]

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

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

عدم الشعور بالانتماء للوطن، وافتقاد الشخص لأهمية دوره في المجتمع، والفشل في الحياة الأسرية، من الأسباب التي تؤدى إلى اكتساب الشخص بعض الصفات السيئة كالتطرف والعنف، مما يؤدى الى ارتكاب الأعمال الارهابية.

---

[11] -ملالحة، عبدالرحمن عوض رجا، جريمة الإرهاب المعلوماتي أسبابه وأساليبه، مجلة جامعة الأمير عبد القادر للعلوم الإسلامية،المجلد 34، العدد1، 2020 ، ص1336.
تشهد بعض الدول الواقعة تحت **الاحتلال أو الاضطهاد** تناميًا في مظاهر الإرهاب الإلكتروني، حيث تلجأ جماعات أو أفراد إلى الفضاء الرقمي كرد فعل على الضغوط السياسية أو الأمنية، مستغلين ضعف الرقابة والاضطرابات الداخلية لنشر رسائلهم أو تنفيذ هجمات رقمية. ويعزز هذا النمط بسبب البيئة المتوترة وغياب الاستقرار، ما يجعل الفضاء الإلكتروني ساحة بديلة للتأثير والضغط بعيدًا عن المواجهة المباشرة.

[12] - عبدالله، علوية حسن، الإرهاب الإلكتروني ومخاطره على قطاع السياحة، بحث مقدم للمؤتمر العلمي الدولي العاشر تحت عنوان "التحديات الجيوفيزيائية والاجتماعية والإنسانية والطبيعية فى بيئة متغيرة"، مؤسسة البحوث الأمريكية، تركيا، 2019 ،ص211.

انخفاض كلفة التنفيذ مقارنة بالإرهاب التقليدي

لا يتطلب الإرهاب الإلكتروني موارد مالية أو بشرية كبيرة، مما يجعله خياراً عملياً للتنظيمات الإرهابية مقارنة بالأعمال المسلحة المباشرة.

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

6- 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 الانتماء للمنظمات الإرهابية التي توفر لهم الفرص المناسبة لإشباع الحاجات المثارة لديهم مقابل ممارسة بعض الأعمال الإرهابية والأنشطة الإجرامية.[13]

7- الأسباب الفكرية: إن من أهم الأسباب الفكرية لظاهرة الإرهاب الإلكتروني ما يلي:

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 والاعتقاد بصحته لوحده من أهم أسباب الإرهاب وظهور الفكر المتطرف.[14]

يجد الباحث هنا بالرغم من سرد الكثير من الاسباب التي تساعد في نشر الارهاب الالكتروني الا ان من اهم الاسباب من وجهة نظر الباحث ان الفراغ الفكري يلعب دور مباشر في انضمام الشباب للانحراف والجماعات المتطرفة، فعدم استغلال الشاب لأوقات فراغه في عمل مفيد يحقق به أهدافه ويستثمره فيما يعود عليه بالنفع لإشباع حاجاته، قد يعرضه للاكتئاب والملل والإحساس بالدونية، وبالتالي قد لا يتردد في الانضمام للجماعات الإرهابية التي تساعده على تحقيق ذاته.

وغياب المنطلقات الفكرية لدى الشباب التي تعود إلى الثورة التكنولوجية المتسارعة ومواقع التواصل الاجتماعي، حيث أصبحت مرجعيتهم الفكرية التي يستمون منها مصادر معلوماتهم دون إمكانية التحقق من صحة وسلامة تلك المعلومات، بالإضافة إلى عدم صلاحيتها للاعتماد عليها كمصادر لتشكيل هوية فكرية لحاملها، ويمثل التطور التكنولوجي 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 فكرا ضالا.

بالنتيجة هنا نجد ان الجرائم الالكترونية قد تتحد في بعض الاسباب مع الارهاب الالكتروني فنتيجة ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق بحيث اصبحت الشبكات المعلوماتية مصممة بشكل مفتوح للجميع 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 والاشخاص ايضا من استغلال هذه الثغرات في الاختراق والتسلل إلى البنى التحتية المعلوماتية للدول او التسلل الى معلومات شخصية لاي من المستخدمين وابتزازه بها بدافع المال او الهوس الفكري وممارسة الأعمال والتخريبية.

وان الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية يعد من أهم الأسباب الرئيسية في انتشار ظاهرة الإرهاب الإلكتروني والجريمة الالكترونية لدى بعض المجتمعات لسهولة القيام بالجرائم المعلوماتية ان صح التعبير، حتى لو وجدت قوانين تجريمية صارمة متكاملة، فإن الإرهابي يمكنه الانتقال 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.

وبالنتيجة أن عدم وجود جهة مركزية واحدة تتحكم فيما يعرض على الشبكات المعلوماتية وتسيطر على مدخلاتها ومخرجاتها، سبب 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.[15]

وفي ظل ما تم شرحة سابقا وبيانه بحيث تم تبيان العوامل التي ساعدة على الارهاب الالكتروني فإننا هنا نجد ان من الطبيعي ان يكون هناك قوانين وانظمة داخلية للحد من انتشاره عن طريق فرض العقوبات الصارمة او التوعية واصدار قوانين تعنى بتقليص الانتشار العشوائي للإرهاب الالكتروني وهذا ما سيتم بحثه في الفرع الثاني .

---

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

[14] - الداغر، مرجع سابق، ص89.

[15] - العجلان، عبدالله بن عبد العزيز بن فهد، الإرهاب المعلوماتي، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض، 2015. ، ص55.

الفرع الثاني: مدى فعالية القوانين الداخلية للحد من الارهاب الالكتروني

تأثرت الأنظمة القانونية العالمية بشكل كبير بالإرهاب الإلكتروني. ويشكل استغلال الإرهابيين لتكنولوجيا المعلومات والاتصالات (ICT)، وخاصة الإنترنت والتقنيات الجديدة التي تسمح بالاتصال المجهول، مصدر قلق متزايد.

ولابد من الاشارة هنا الى انه يجري حاليا تطوير استراتيجية شاملة للأمن السيبراني من قبل مكتب مكافحة الإرهاب التابع للأمم المتحدة. وفي حين أن بعض الدول قد أقرت تشريعات وطنية لمكافحة الإرهاب الإلكتروني (على سبيل المثال، المادة 33 من قانون إساءة استخدام الكمبيوتر والجرائم الإلكترونية لعام 2018 في كينيا والمادة 10 من قانون منع الجرائم الإلكترونية لعام 2016 في باكستان)، فإن الإرهاب الإلكتروني ليس محظورا صراحة بموجب القانون الدولي.

وقد تغلغل مفهوم الإرهاب الإلكتروني في أجندة الأمن القومي الصينية الموسعة، والتي تهدف إلى إدارة وتنظيم وتأمين ومراقبة سيادتها السيبرانية بشكل شامل، كما يتضح من التشريعات والسياسات والممارسات القضائية الصينية. وهذا يشير إلى أن الصين قد اعتمدت استراتيجية شاملة لإدارة وحكم فضاءها الإلكتروني لحماية مصالحها في الأمن القومي للإرهاب الإلكتروني. [16]

آثار مصطلح الارهاب الالكتروني ايضا حفيظة النظام القانوني الأمريكي، بما في ذلك من آثار على نظام العدالة الجنائية، والأمن القومي، والاقتصاد، والحريات المدنية. حيث يعد التهديد الذي يشكله الإرهاب الإلكتروني لأساليب التحقيق التقليدية أحد أهم آثاره على النظام القانوني الأمريكي. وقد يكون من الصعب تحديد هوية المسؤولين عن الهجمات الإلكترونية والقبض عليهم، نظرا لكثرة ورودها من أشخاص أو منظمات منتشرة في جميع أنحاء العالم. وتزداد عملية التحقيق والمقاضاة تعقيدا نظرا لإمكانية شن الهجمات الإلكترونية من أي مكان متصل بالإنترنت. ونتيجة لذلك، اضطر النظام القانوني إلى ابتكار أساليب جديدة للتحقيق في قضايا الإرهاب الإلكتروني ومحاكمتها. ولمنع الإرهاب الإلكتروني، طبقت الولايات المتحدة بعض التدابير والقوانين القانونية.

على سبيل المثال، يجرم قانون الاحتيال وإساءة استخدام الحاسوب (CFAA) لعام 1986 العديد من الجرائم المتعلقة بالحاسوب، مثل القرصنة والوصول غير المصرح به إلى أنظمة الحاسوب. وفي أعقاب هجمات 11 سبتمبر، أقر الكونغرس قانون باتريوت، الذي زاد من قدرات المراقبة الحكومية وسمح بجمع بيانات الاتصالات الإلكترونية. [17]

---

[1]- Escalation of Threats in the Middle East . تقرير من Peace Institute Cyber يوضح ارتفاع الهجمات السيبرانية في الأراضي الفلسطينية والصراع الإسرائيلي-الفلسطيني https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east/

ينص قانون **مكافحة الإرهاب المصري رقم 94 لسنة 2015** على مجموعة من المواد التي تجرم الأفعال الإرهابية عند ارتكابها عبر الوسائل الإلكترونية وهو ما يعرف ضمن الدراسات الحديثة بـ الإرهاب الإلكترون .فمن أبرز هذه المواد:

- المادة :(6) تنص على أنه *(يعاقب على التحريض على ارتكاب أية جريمة إرهابية، بذات العقوبة المقررة للجريمة التامة، وأياً كانت الوسيلة المستخدمة فيه، ولو لم يترتب على هذا التحريض أثر.)* ما يشمل التحريض عبر الإنترنت أو الوسائل الإلكترونية.
- المادة :(28) تنص على أنه *(يعاقب بالسجن كل من روج أو أعد للترويج، بطريق مباشر أو غير مباشر، لارتكاب أية جريمة إرهابية سواء بالقول أو الكتابة أو بأية وسيلة أخرى)* وتشمل هذه الوسائل جميع الوسائل الرقمية.
- المادة :(29) تنص على أنه *(يعاقب بالسجن المشدد كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها.)* وهذه المادة تشكّل الركيزة القانونية للإرهاب الإلكتروني، إذ تُجرّم استخدام الإنترنت كوسيلة للتخطيط أو التنسيق أو الترويج للأعمال الإرهابية.

وبذلك يظهر أن القانون المصري لم يستخدم مصطلح "الإرهاب الإلكتروني" صراحتا لكنه يجرم جميع الأفعال الإرهابية عند ارتكابها عبر الفضاء الرقمي أو الوسائل الإلكترونية بما في ذلك التحريض والترويج والتجنيد وتبادل المعلومات بين الجماعات الإرهابية.

[17] **قانون باتريوت (USA PATRIOT Act)** هو قانون أمريكي صدر عام 2001بعد أحداث 11**سبتمبر**، ويهدف إلى تعزيز قدرات الحكومة على مكافحة الإرهاب داخليا وخارجيا.

اسم القانون هو اختصار لعبارة:

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

أهم ما يتضمنه قانون باتريوت

- توسيع صلاحيات أجهزة الأمن في المراقبة الإلكترونية وجمع البيانات.

ويجب التنويه هنا الى ان الطبيعة القانونية في الضفة تختلف بين شقي الوطن في الضفة الغربية وقطاع غزة حيث يعتمد النظام القانوني للجرائم الإلكترونية (الارهاب القانوني) في فلسطين على:

• قانون العقوبات الأردني رقم 16 لعام 1960 (الساري حتى اليوم)

وهذا القانون لا يتضمن نصوصا صريحة حول "الإرهاب الإلكتروني" لأنه سابق للثورة الرقمية ولكنه يجرم

تخريب المرافق العامة، الجرائم الماسة بأمن الدولة، نشر الإشاعات بقصد الإضرار بالأمن وقد تفسر بعض هذه النصوص لتشمل الجرائم الرقمية، لكنها تظل غير كافية.

• قرار بقانون الجرائم الإلكترونية الفلسطيني رقم 10 لسنة 2018 (أصدرته السلطة الفلسطينية) :

ويعد القانون هذا الأكثر ارتباطا بالمجال السيبراني، ويجرم: الدخول غير المشروع للأنظمة، سرقة البيانات، نشر معلومات تسبب ترويع الجمهور، التهديد الإلكتروني، إنشاء مواقع دعم للإرهاب أو التحريض ويمكن التعرج هنا على موقف القانون الفلسطيني في تكييف الارهاب الالكتروني فنجد ان هذ القراربقانون هو من اهم النظم القانونية في التي تجرم ما يمكن أن يصنف ضمن الإرهاب الإلكتروني أو الجرائم الإلكترونية فنجد ان

المادة 4 منه قد جرمت الدخول غير المصرح به إلى موقع أو نظام أو شبكة إلكترونية أو تجاوز الوصول المسموح به.

والمادة 7 منه ايضا تجرم التنصت أو اعتراض أو تسجيل أو اعتراض بيانات تنقل عبر الشبكة بشكل غير قانوني وكذلك المادة 8 التي جرمت العمل على فك الشفرات أو استخدام مفاتيح أو كلمات مرور أو وسائط توقيع إلكتروني لشخص اخر بغير إذن وغيرها من المواد التي نصت وبشكل صريح على الامور التي تعتبر مجرمة في العالم الافتراضي ووضع حدود على استخدام هذا التطور المرعب في التكنولوجيا وانظمة الاتصال والانترنت .

ويرى الباحث بالرغم من ان هذا القانون يواكب جزءا من التطور الرقمي و يجرم أفعالا يمكن تصنيفها ضمن الإرهاب الإلكتروني كما ذكرنا سابقا لكنه لا يقدم تعريفا واضحا لمفهوم الإرهاب الإلكتروني ولا يعالج الهجمات الموجهة ضد البنية التحتية الحيوية ذات الطابع الأمني وكذلك يتهم بتقييد حرية التعبير في بعض مواده ما يقلل من اتساقه مع المعايير الحقوقية[18].

واخيرا ونظرا لأن الهجمات الإلكترونية تأتي في كثير من الأحيان من خارج الحدود الوطنية فإن التعاون الدولي ضروري أيضا في مكافحة الإرهاب السيبراني ولتشجيع تبادل البيانات والبحث التعاوني فقد شكلت العديد من الدول تحالفات واتفاقيات تعنى بالحد من هذا النوع من الارهاب وعلى سبيل المثال لتشجيع التعاون في قضايا الأمن السيبراني والجرائم الإلكترونية انضمت الولايات المتحدة والمملكة المتحدة إلى حوار الأمن السيبراني بين الولايات المتحدة والمملكة المتحدة في الختام اتخذت مجموعة متنوعة من التدابير القانونية الدولية لمكافحة الإرهاب السيبراني بما في ذلك إنشاء أطر قانونية دولية، وتطوير التشريعات واللوائح الوطنية، وإنشاء وحدات متخصصة لمكافحة الجرائم السيبرانية وتشجيع التعاون والشراكات العالمية ومن المتوقع أن تواصل الدول تطوير وتكييف التدابير والسياسات القانونية لمواجهة هذا التهديد المتزايد مع تطور الإرهاب السيبراني.

وذلك لما يمكن أن يحمله هذا الارهاب من اضرار وخيمة لذا من المهم اتخاذ تدابير لمكافحة الإرهاب الإلكتروني نظرا لخطورته التي قد تترتب عليه هجمات الإلكترونية مع احتمال وقوع خسائر اقتصادية خلافا عن الإضرار بسمعة الدولة واستقرارها بل قد تصل الى خسائر في الأرواح كما يمكن أن تحدث اضطرابات وفوضى واسعة النطاق عند تعطل البنية التحتية الحيوية مثل شبكات الكهرباء والمستشفيات وتقويض أمن وموثوقية التكنولوجيا مما يجعل الناس غير متأكدين من أمن وموثوقية أنظمته.

- تسهيل التنصت على الاتصالات الهاتفية والإنترنت.
- تعزيز تبادل المعلومات بين الأجهزة الأمنية.
- تمكين الحكومة من احتجاز أو ترحيل الأجانب المشتبه بصلتهم بالإرهاب.
- تشديد الرقابة على التحويلات المالية لمنع تمويل الإرهاب.

[18] - قانون الجرائم الإلكترونية الفلسطيني رقم (10) لسنة 2018 –السلطة الوطنية الفلسطينية، رام الله.

الخاتمة:

يتضح مما سبق أن الإرهاب الإلكتروني لم يعد مجرد تهديد افتراضي مرتبط بالفضاء الرقمي بل أصبح ظاهرة واقعية متجذرة تؤثر بشكل مباشر على أمن الدول واستقرار المجتمعات وحماية الأفراد فقد مكنت التكنولوجيا الحديثة الجماعات الإرهابية والمتطرفة من ابتكار أساليب هجومية متطورة وغير تقليدية تستهدف البنى التحتية الحيوية للدول مثل شبكات الكهرباء والمياه والاتصالات والأنظمة المالية بطرق قد تتجاوز في خطورتها الهجمات التقليدية كما أتاحت لها الفضاء الرقمي وسيلة لتوسيع دائرة التجنيد والتحريض ونشر الأفكار المتطرفة وجمع التمويل الإلكتروني والتنسيق بين التنظيمات الإرهابية العابرة للحدود ما جعل مواجهة الإرهاب التقليدي وحده غير كافية للحد من هذه الظاهرة الحديثة.

ولذلك أصبح من الضروري تطوير استراتيجيات متكاملة لمكافحة الإرهاب الإلكتروني، تشمل تعزيز الأطر التشريعية الوطنية والدولية لمواكبة التطور التقني المستمر، بحيث تغطي النصوص القانونية الجرائم الإلكترونية ذات الطابع الإرهابي، وتجرم التحريض الإلكتروني والترويج للأفكار المتطرفة والتخريب الرقمي، مع مراعاة الحقوق الأساسية وخصوصية الأفراد. كما يتطلب الأمر رفع مستوى الوعي لدى الأفراد والمؤسسات حول مخاطر الفضاء الرقمي وطرق استغلاله وهو ما يحد من قدرة الجماعات الإرهابية على نشر الفكر المتطرف واستقطاب عناصر جديدة. وفي الوقت نفسه، يكتسب تعزيز قدرات الأمن السيبراني لدى الجهات الرسمية والمرافق الحيوية أهمية قصوى، من خلال تبني أنظمة حماية متقدمة ومراقبة الشبكات وتطوير آليات الاستجابة السريعة للحوادث الرقمية بما يحول دون نجاح الهجمات الإلكترونية التي قد تهدد الأمن القومي.

ولا يمكن التغاضي عن أهمية التعاون الدولي والإقليمي في مواجهة الإرهاب الإلكتروني العابر للحدود، بما يشمل تبادل المعلومات الاستخبارية والتنسيق القضائي وتطوير الاتفاقيات الدولية لمكافحة الجرائم الإلكترونية والإرهابية، وهو ما يضمن تحقيق رادع فعّال للفاعلين وملاحقتهم قانونياً عبر التشريعات المختلفة كما أن مكافحة الإرهاب الإلكتروني تتطلب تكاملا بين البعد الأمني والتقني والاجتماعي والثقافي إذ يتعين غرس قيم التسامح وتعزيز الثقافة الرقمية ومكافحة الفكر المتطرف مع العمل على تمكين المجتمعات من استخدام التكنولوجيا بشكل إيجابي يخدم التنمية والابتكار دون تعريض أمنها للخطر.

في ضوء ذلك إن بناء فضاء رقمي آمن يمثل شرطاً أساسياً لتحقيق التقدم العلمي والاقتصادي والاجتماعي، وحماية الإنسان والمجتمع من تهديدات تتجاوز حدود الزمان والمكان ويؤكد على ضرورة أن يكون الأمن الإلكتروني جزءا لا يتجزأ من استراتيجيات التنمية الشاملة بما يعزز قدرة الدول والمجتمعات على مواجهة التحديات المعاصرة بفاعلية ووعي.

نتائج البحث:

1. يتضمن الإرهاب الالكتروني استغلال تقنيات الحاسوب والإنترنت لارتكاب أعمال عنف.
2. يمكن استخدام أساليب متنوعة، بما في ذلك اختراق أنظمة الحاسوب لسرقة معلومات حساسة، ونشر البرمجيات الخبيثة لتعطيل العمليات، والتحريض على العنف أو بث الفتنة على وسائل التواصل الاجتماعي.
3. يمكن أن تكون الخسائر المالية، والوفيات، والإضرار بالسمعة، وفقدان الاستقرار، جميعها نتائج للإرهاب الالكتروني.
4. التفرقة بين الارهاب الالكتروني والجرائم الالكترونية وحرب المعلومات .
5. نظرا لأن الإرهاب الإلكتروني قضية دائمة التطور، يمكن أن تركز الأبحاث المستقبلية على تحديد تأثير بعض السياسات التي وضعتها بعض الدول بشأن الإرهاب الإلكتروني.

التوصيات:

1- يعد تعزيز التعليم والتوعية بالأمن السيبراني بين الجمهور وموظفي الحكومة ومشغلي البنية التحتية الحيوية أمرا أساسيا لضمان وعي الأفراد والمؤسسات بالتهديدات المحتملة وكيفية التخفيف منها ولذلك **يوصي الباحث** تعديل المادة (3) من القانون (التي تنشئ الوحدة المتخصصة لمكافحة الجرائم الإلكترونية) لتشمل تكليف هذه الوحدة ووزارة الاتصالات بتطوير برامج تدريبية وتوعوية منتظمة حول الأمن السيبراني والجرائم الإلكترونية وذلك بهدف رفع مستوى الوعي لدى المجتمع والأجهزة الحكومية والقطاع الخاص حول طرق استغلال الفضاء الرقمي في أنشطة إرهابية .

2- يعد التعاون مع البلدان الأخرى والمنظمات الدولية أمرا ضروريا لتبادل المعلومات الاستخباراتية المتعلقة بالتهديدات والتحقيق في الحوادث الإلكترونية وتطوير استجابة عالمية منسقة للإرهاب الإلكتروني في هذا السياق لذلك **يوصي الباحث** تعديل المادة (42) من القانون (التي تنظم

التعاون مع الدول الأجنبية) لتشمل التنسيق الدولي في قضايا الجرائم الإلكترونية ذات الطابع الإرهابي، تبادل الأدلة الرقمية والمساعدة القانونية المتبادلة ما يعزز قدرة السلطة الفلسطينية على مواجهة الجرائم العابرة للحدود .

3- يعد الاستثمار في البحث والتطوير في مجال الأمن السيبراني ضروريا للبقاء في طليعة التهديدات الناشئة وتطوير تقنيات واستراتيجيات مبتكرة للحماية من الإرهاب الإلكتروني لذلك **يوصي الباحث** إضافة فقرة جديدة ضمن المادة (3) باضافة وحدة جديدة متخصصة مثل وزارة الاتصالات تكون مهمتها دعم وتمويل البحوث الأكاديمية والمشاريع التقنية في الأمن السيبراني وتعاونها مع الجامعات ومراكز البحث لتطوير حلول تقنية متقدمة لرصد ومنع الهجمات الإلكترونية.

4- إن تنفيذ وإنفاذ قوانين وأنظمة الأمن الإلكتروني يوفر أساسا قانونيا لمقاضاة مجرمي الإنترنت وردع الجهات الخبيثة لذلك **يوصي الباحث** تعديل نصوص المواد ذات الصلة بجرائم التهديد والابتزاز عبر الشبكة في المادة (15) لتوضيح شمولها للجرائم ذات الطابع الإرهابي مثل التحريض الإلكتروني والترويج للعنف وبث خطابات الكراهية المرتبطة بالأيديولوجيات المتطرفة بحيث يعامل مَن يستخدم الشبكة لتحقيق أهداف إرهابية بشكل مشدد وفقا للقانون.

5- يعد التعاون مع مؤسسات القطاع الخاص خصوصا مزودي خدمات الإنترنت وشركات الاتصالات التي تمتلك البنية التحتية الرقمية الحيوية أمرا بالغ الأهمية لضمان تبادل المعلومات وتعزيز تدابير الأمن الإلكتروني في هذا الإطار لذلك **يوصي الباحث** تعديل المادة (31) من القانون (التي تنظم التزامات مزودي الخدمة في تقديم المعلومات والبيانات) لإضافة نص صريح يلزم مزودي الخدمة بـ التعاون الفعال مع الجهات الأمنية في الإبلاغ الفوري عن التهديدات مشاركة الأدلة الرقمية وتعزيز أنظمة الحماية التقنية بما يساهم في كشف ومنع استخدام الشبكة في أنشطة إرهابية قبل وقوعها أو تفاقمها

المصادر :

أولًا :التشريعات والاتفاقيات

قرار بقانون رقم (10)لسنة 2018بشأن الجرائم الإلكترونية الفلسطيني.

قانون العقوبات الأردني رقم (16)لسنة 1960.

قانون مكافحة الإرهاب المصري رقم (94)لسنة 2015.

الاتفاقية العربية لمكافحة الإرهاب، بدأ نفاذها في 7أيار/مايو 1999، وفقًا للمادة (40).

USA PATRIOT Act. (2001). United States of America.

ثانيًا :المراجع العربية

الداغر، مجدي محمد عبد الجواد .(2016) .دور الإعلام في تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الإنترنت : دراسة ميدانية .حوليات الآداب والعلوم الاجتماعية، مجلس النشر العلمي، جامعة الكويت.

عبد الصادق، عادل .(2009) .الإرهاب الإلكتروني :القوة في العلاقات الدولية :نمط جديد وتحديات مختلفة .مركز الدراسات السياسية والاستراتيجية بالأهرام.

عبد الله، علوية حسن .(2019) .الإرهاب الإلكتروني ومخاطره على قطاع السياحة .بحث مقدم إلى المؤتمر العلمي الدولي العاشر بعنوان »التحديات الجيوفيزيائية والاجتماعية والإنسانية والطبيعية في بيئة متغيرة«، مؤسسة البحوث الأمريكية، تركيا.

العجلان، عبد الله بن عبد العزيز بن فهد .(2015) .الإرهاب المعلوماتي .المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية (ICACC)، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، الرياض.

عيسى، عقيلة هادي، وحاتم، إسراء جواد .(2010) .الإرهاب المعلوماتي)الرقمي (وطرق مكافحته .المجلة السياسية والدولية، .(16)

ثالثًا :المراجع الأجنبية

Collin, B. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. 11th Annual International Symposium on Criminal Justice Issues.

Iqbal, M. (2004). Defining cyberterrorism. Journal of Computer & Information Law, 22(2), 402.

رابعًا :المواقع الإلكترونية

CyberPeace Institute. (د.ت). Escalation of threats in the Middle East. https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east/ - العربية لمكافحة الإرهاب https://hrlibrary.umn.edu/arabic/a-terroh.html