j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study)

Samar Adel Shehata

College of Law, Tanta University, Egypt.

samaradel943@gmail.com

Abstract In light of the global technological boom, cyberterrorism has emerged as one of the most serious threats to national security and societal stability. Terrorist groups increasingly exploit modern digital tools to execute their plans, taking advantage of the accessibility of the dark web, social media platforms, and electronic payment applications. In response to this reality, artificial intelligence (AI) stands out as a promising tool capable of supporting national efforts to counter this complex phenomenon. This study aims to provide a comparative analytical perspective on the role of AI in combating cyberterrorism by reviewing the technological applications used in threat detection and prediction, analyzing the digital behavior of terrorist groups, and evaluating the effectiveness of the legal and regulatory frameworks that govern this use.

10.36371/port.2025.3.8

Keywords: *Artificial Intelligence – Cyberterrorism – Cybersecurity – Terrorism Financing – Dark Web – Cryptocurrencies*

المواجهة الجنائية للإرهاب الإلكتروني : (دراسة تحليلة مقارنة)

سمر عادل شحاته

كلية الحقوق / جامعة طنطا ، مصر

الخلاصة : في ظل الطفرة التكنولوجية العالمية، أصبح الإرهاب الإلكتروني من أخطر التحديات التي تهدد أمن الدول واستقرار المجتمعات، إذ توظف الجماعات الإرهابية الوسائل الرقمية الحديثة لتنفيذ مخططاتها، مستفيدة من سهولة الوصول إلى الشبكات المظلمة، والمنصات الاجتماعية، وتطبيقات الدفع الإلكتروني. أمام هذا الواقع، يبرز الذكاء الاصطناعي كأداة واعدة قادرة على دعم جهود الدول في التصدي لتلك الظاهرة المعقدة. تهدف هذه الدراسة إلى تقديم رؤية تحليلية مقارنة لدور الذكاء الاصطناعي في مواجهة الإرهاب الإلكتروني، من خلال استعراض التطبيقات التقنية المستخدمة في كشف التهديدات والتنبؤ بها، وتحليل السلوك الرقمي للجماعات الإرهابية، مع تقييم فعالية الأطر القانونية والتنظيمية التي تحكم هذا الاستخدام.

الكلمات الدالة: *: الذكاء الاصطناعي- الإرهاب الإلكتروني- الأمن السيبراني- تمويل الإرهاب- الشبكة المظلمة (Dark Web)- العملات المشفّرة*

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

المقدمة

أضحى الإرهاب الإلكتروني في العقود الأخيرة أحد أخطر التحديات الأمنية التي تواجهها الدول والمجتمعات، بفعل التقدم التكنولوجي الهائل الذي مكّن التنظيمات الإرهابية والأفراد المتطرفين من استغلال الفضاء الرقمي لتنفيذ مخططاتهم الإجرامية دون الحاجة إلى استخدام القوة المادية أو التواجد الفعلي في مسرح الجريمة. فقد انتقلت ساحات المعارك من الميدان التقليدي إلى العالم الافتراضي، حيث يُمكن بلمسة زر تعطيل شبكات حيوية، واختراق بيانات سيادية، وبث رسائل تخويف وتحريض تهدد أمن الدولة واستقرارها.

ويُعد الإرهاب الإلكتروني من الجرائم المستحدثة التي لم تكن معروفة بالصورة الحالية في التشريعات التقليدية، مما أوجد فجوة قانونية في منظومة المواجهة الجنائية، خاصة في ظل الطبيعة غير النمطية لهذا النوع من الجرائم، الذي يتميز بكونه عابراً للحدود، سريع الانتشار، ومبنياً على تقنيات معقدة تُصعّب من تعقبه والكشف عن مرتكبيه. ومن هنا، أصبحت الحاجة مُلحّة لإعادة النظر في مفاهيم القانون الجنائي، وتطوير أدوات التجريم والعقاب بما يتناسب مع خصوصية الجرائم السيبرانية ذات الطابع الإرهابي.

إن المواجهة الجنائية للإرهاب الإلكتروني لا تقتصر على الجانب العقابي وحده، بل تشمل كذلك الجوانب الوقائية والتقنية، بما فيها التعاون القضائي الدولي، وتبادل المعلومات الاستخباراتية، وتوفير بيئة تشريعية مرنة وقادرة على التنبؤ بالخطر قبل وقوعه. كما يُشكّل التوازن بين الحريات العامة وضرورات الأمن العام محوراً رئيسياً في معادلة المواجهة، إذ إن الاستخدام المفرط للأدوات الجنائية قد يُفضي إلى المساس بحقوق الإنسان وحرية التعبير، في حين أن التساهل مع هذه الجرائم يُهدد كيان الدولة وسيادتها.

وقد دفعت هذه الإشكاليات العديد من التشريعات الوطنية، مثل التشريع الفرنسي والإماراتي والمصري، إلى تعديل قوانينها أو إصدار قوانين خاصة بمكافحة الجرائم الإرهابية الإلكترونية، سواء من خلال توسيع نطاق الركن المادي ليشمل الوسائل الرقمية، أو من خلال الاعتراف بالأدلة الرقمية، أو عبر النص على التعاون الدولي في مكافحة هذا الخطر المتنامي. وفي هذا الإطار، تسعى المواجهة الجنائية للإرهاب الإلكتروني إلى تحقيق عدة أهداف، من بينها الردع العام والخاص، حماية البنية التحتية المعلوماتية، صيانة الأمن القومي، وتجفيف منابع التمويل والدعاية الإلكترونية للتنظيمات الإرهابية.

وهكذا، تفرض جريمة الإرهاب الإلكتروني تحديات غير مسبوقة على القانون الجنائي بمفاهيمه الكلاسيكية، وهو ما يستدعي ضرورة التحرك نحو تطوير نظرية قانونية متكاملة تُراعي خصوصية الجريمة الرقمية، وتضمن في الوقت ذاته الفعالية والعدالة الجنائية في مواجهة هذا النمط المعولم والمتجدد من الجرائم.

أهمية البحث :

تنبع أهمية هذا البحث من خطورة التهديدات التي يطرحها الإرهاب الإلكتروني على أمن الدول واستقرارها السياسي والاقتصادي والمجتمعي، حيث أصبح الفضاء الرقمي مجالًا واسعًا تنشط فيه الجماعات الإرهابية عبر وسائل جديدة مثل التحريض، والتجنيد، والتخطيط، والتمويل، وتنفيذ هجمات إلكترونية قد تُشلّ من خلالها البنى التحتية الحيوية للدول.

أهداف البحث :

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، أبرزها:

- تحديد الإطار المفاهيمي والقانوني للإرهاب الإلكتروني، وبيان خصائصه التي تميّزه عن صور الإرهاب التقليدي.
- تحليل الركائز القانونية للمواجهة الجنائية للإرهاب الإلكتروني، من حيث صور التجريم، والأركان القانونية، والعقوبات المقررة في التشريعات المختلفة.

إشكالية البحث :

تتمثل إشكالية هذا البحث في كيفية تحديد إطار قانوني فعّال لمكافحة الإرهاب الإلكتروني في ظل التحديات التقنية والاقتصادية التي تفرزها الجريمة السيبرانية.

تساؤلات البحث :

ما هي الطبيعة القانونية للإرهاب الإلكتروني؟ وكيف يختلف عن الإرهاب التقليدي في إطار الجرائم الإلكترونية والتقنيات المستحدثة؟

هل تمتلك التشريعات الوطنية (العربية والغربية) فعالية كافية في التصدي للجرائم الإرهابية الإلكترونية، وخاصة في ظل التطور المستمر في تقنيات الهجوم والاختراق؟

ما هي العقبات التي تواجه المؤسسات القضائية والأمنية في مواجهة الإرهاب الإلكتروني، خاصةً فيما يتعلق بتحديد المسؤولية الجنائية للأفراد والكيانات عبر الشبكات الإلكترونية الدولية؟

منهجية البحث :

اتبعت تطبيق المنهج المقارن للمقارنة بين التشريعات الوطنية المختلفة المتعلقة بالإرهاب الإلكتروني، مثل القوانين في الدول

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

العربية (مصر، الإمارات) مقارنة بالقوانين الغربية (الولايات المتحدة، المملكة المتحدة).

خطة البحث :

المبحث الأول : ماهية الإرهاب الالكتروني

المبحث الثاني : الأحكام العامة في جريمة الإرهاب الالكتروني

المبحث الثالث : المواجهة الجنائية للإرهاب الالكتروني

المبحث الأول

ماهية الإرهاب الالكتروني

تمهيد وتقسيم :

الإرهاب الإلكتروني هو شكل من أشكال الإرهاب الذي يستخدم تكنولوجيا المعلومات والإنترنت لتنفيذ أعمال تهدف إلى ترويع الأفراد أو المجتمعات أو الدول. يعد هذا النوع من الإرهاب حديثًا نسبيًا مقارنة بالأشكال التقليدية الأخرى للإرهاب، لكنه أصبح يشكل تهديدًا متزايدًا في العصر الرقمي الحالي، حيث تعتمد العديد من الدول والمؤسسات على الأنظمة الإلكترونية في جميع المجالات الحيوية، مثل الاقتصاد، والصحة، والتعليم، والأمن القومي.

يشمل الإرهاب الإلكتروني مجموعة واسعة من الأنشطة المدمرة، مثل الهجمات على الشبكات الحاسوبية، نشر الفيروسات والبرمجيات الخبيثة، اختراق البيانات الحساسة، وترويج التطرف من خلال منصات الإنترنت. وقد يُستخدم أيضًا لأغراض تخريبية، مثل تعطيل البنية التحتية الحيوية أو نشر الأخبار المزيفة التي تؤدي إلى زعزعة الاستقرار الاجتماعي.

المطلب الأول : مفهوم الإرهاب الإلكتروني

المطلب الثاني : وسائل وخصائص الإرهاب الإلكتروني

المطلب الثالث : أسباب الإرهاب الإلكتروني

المطلب الأول

مفهوم الإرهاب الالكتروني

أدى التقدم التكنولوجي المتسارع إلى نشوء نمط جديد من التهديدات الأمنية غير التقليدية، من بينها ما يُعرف بـ"الإرهاب الإلكتروني"، الذي بات يشكّل تحديًا حقيقيًا للأمن القومي والسيادة الوطنية للدول، بل ويمثل أحد أخطر صور الجرائم المستحدثة في العصر الرقمي. فالإرهاب الإلكتروني لا يعتمد على القوة المادية أو العنف المسلح كما هو الحال في الإرهاب التقليدي، بل يستند إلى أدوات التكنولوجيا ووسائل الاتصال الحديثة في تنفيذ جرائمه، من خلال استهداف الأنظمة الإلكترونية، وتعطيل البنية التحتية الحيوية، وبث الرعب في نفوس المواطنين، والتحريض على العنف والكراهية عبر الوسائط الرقمية.

ويختلف الإرهاب الإلكتروني عن غيره من الجرائم الإلكترونية في كونه ذو طابع خاص يتصل بأهدافه ودوافعه، حيث يتخذ غالبًا أبعادًا سياسية أو أيديولوجية أو دينية، ويهدف إلى التأثير في السلطات العامة، أو تهديد استقرار المجتمع، أو الإضرار بمصالح الدولة الحيوية. ويتميّز هذا النوع من الجرائم بطابعه الخفي والعابر للحدود، مما يصعّب من اكتشاف مرتكبيه أو ملاحقتهم جنائيًا وفقًا للحدود الإقليمية التقليدية.

الفرع الأول : تعريف الإرهاب الالكتروني

الفرع الثاني : الإرهاب الالكتروني في الإتفاقيات العربية والعالمية

الفرع الأول

تعريف الإرهاب الالكتروني

قد يرتبط مفهوم الإرهاب في نظر البعض بالعنف المادي واستخدام الأسلحة والذخائر ضمن وسائل هذا العنف ، ألا انه مع التقدم التكنولوجي وانتشار تقنيات الذكاء الاصطناعي والذي كان له بعض من الآثار السلبية يعتبر الإرهاب الإلكتروني من أهم نتائج ثورة الذكاء الاصطناعي وعلي ذلك تعددت مفاهيم الإرهاب الألكتروني نوردها فيما يلي :

عرف بعض الفقهاء الإرهاب الإلكتروني بأنه : خرق للقانون يقدم عليه فرد من الأفراد ، أو تنظيم جماعي بهدف إثارة اضطراب غاية في الخطوره في النظام العام ، عن طريق شبكة المعلومات العالمية " الإنترنت " .[1]

وعرفه آخر بأنه : الإستخدام العدائي والعدواني غير المشروع للإنترنت ، بهدف ترويع الحكومة والمدنيين ، أو قسم منهم في إطار السعي إلي تحقيق أهداف سياسية أو إجتماعية .[2]

كما عرف بأنه : هجمات غير مشروعة ، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنه الكترونياً ، توجه من أجل الإنتقام أو ابتزاز أو إجبار أو تأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة .[3]

وهو : نوع حديث عن الإرهاب بمفهومه العادي يقوم على استخدام شبكة الإنترنت وشبكات المعلومات وأجهزة الكمبيوتر وما يرتبط بها من تطورات تكنولوجية متسارعة من أجل التخويف والإرغام والتخريب لتحقيق أهداف سياسية ويمثل الإرهاب الإلكترونى أحد مظاهر الدمج والربط بين استخدام كل من العنف لتحقيق أهداف سياسية، وتوظيف

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

التكنولوجيا الحديثة فى مجالات الاتصال والمعلوماتية، والتى تعد من أبرز آليات العولمة.[٤]

كما تعرفه دينيج دروثي " عل انه إلتقاء بين الفضاء الإلكتروني والإرهاب يشير إلي الهجمات غير القانونية والتهديدات بالهجوم علي أجهزة الحاسب الآلي والشبكات والمعلومات المخزنة عليها ، وذلك لتخويف أو إكراه حكومة أو شعبها من أجل تحقيق أهداف سياسية أو إجتماعية ، ولكي يصنف الهجوم علي انه إرهاب إلكتروني يجب أن يؤدي الهجوم إلي عنف ضد الأشخاص أو الممتلكات أو علي الأقل التسبب في ضرر كاف ينتج عنه توليد الخوف ومن الأمثلة علي ذلك : الهجمات التي تؤدي إلي الإصابات الجسدية أو الإنفجارات أو الخسائر الإقتصادية الفادحة ، الهجمات الخطيرة ضد البني التحتية الحيوية ، الهجمات التي تعطل الخدمات الأساسية ، ويعد كل ذلك من أعمال الإرهاب الإلكتروني إعتماداً علي تأثيرها .[5]

وعرفه بعض الفقه بأنه : هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وتنتج عنها آثار تخريبية مدمرة مكافئة لآثار الأفعال المادية للإرهاب"، وذلك وفقا لبا رى كولين الذى ناقش ديناميكية الإرهاب هذه باعتبارها تجاوز للواقع المادى إلى العالم الإفتراضي و"تقاطع والتقاء العالمين". وكولين هو أول من استخدم هذا المفهوم خلال عقد الثمانينيات من القرن العشرين .[٦] كما عرفه جيمس لويس لاحقا، بأنه: "استخدام أدوات شبكات الحاسوب فى تدمير أو تعطيل البنى التحتية الوطنية المهمة ، مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين ".[٧]

ويمكن القول أن الإرهاب الألكتروني يرتبط بإستخدام أساليب الخوف والرعب ، من قبل فرد أو جماعة أو دولة ما بالإستناد إلي دوافع ذات طبيعة سياسية ، بقصد الإخلال بالنظام العام وزعزعة الأمن والطمأنينة وتعطيل نظم السيطرة والرقابة الإلكترونية وهو ما يعرض سلامة المجتمع وأمنه للخطر ويؤدى إلي تعطيل عمل الأجهزة والمرافق الحكومية والمؤسسات الخاصة ، إضافة إلي إلحاق الضرر بالحريات الأساسية وانتهاكه لكرامة الإنسان .[٨]

مما سبق : يمكن تعريف الإرهاب الإلكتروني بأنه إستخدام التقنيات الحديثة والوسائل التكنولوجية مثل تقنيات الذكاء الإصطناعي ضد أحد الأشخاص أو المؤسسات أو الدول بدوافع سياسية وبهدف بث الخوف والفزع بين المواطنين وإشعارهم بوجود خطر قد يداهمهم . وهو الهجمات غير القانونية والتهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها و يتم ذلك لترهيب أو إكراه حكومة أو شعبها من أجل تحقيق أهداف سياسية أو اجتماعية.

كما يعني : الإستخدام المتعمد للأنشطة التخريبية، أو التهديد بها، ضد الشبكات والمعلومات المخزنة عليها، بقصد التسبب في ضرر أو تعزيز الأهداف الاجتماعية أو الإيديولوجية أو الدينية أو السياسية أو الأهداف المماثلة، أو ترهيب أي شخص لتعزيز هذه الأهداف .

الفرع الثاني

الإرهاب الالكتروني في الإتفاقيات العربية والعالمية

أولاً : تعريف الإتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010 للإرهاب الإلكتروني :

لم تضع الإتفاقية مفهوماً بعينه لجريمة الإرهاب الإلكتروني وإنما رصدت الأفعال المكونه لهذه الجريمة علي النحو التالي :[٩]

1- نشر أفكار ومبادئ جماعة إرهابية والدعوة لها

2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الإتصال بين التنظيمات الإرهابية

3- نشر طرق صناعة المتفجرات والتي تستخدم بشكل خاص في العمليات الإرهابية

4- نشر النعرات والفتن والإعتداء علي المقدسات والأديان

ثانياً : تعريف الإرهاب الإلكتروني في الاتفاقيات الدولية والإقليمية

رغم تصاعد المخاوف من التهديدات الرقمية ذات الطابع الإرهابي، لم تُفرز الاتفاقيات الدولية تعريفًا دقيقًا لمصطلح "الإرهاب الإلكتروني"، بل عالجت السلوكيات المرتبطة به ضمن مفاهيم أوسع مثل "الإرهاب" أو "الجريمة المعلوماتية". ومع ذلك، يمكن استخلاص اتجاهات بعض الاتفاقيات كما يلي:

1- اتفاقية الأمم المتحدة لقمع تمويل الإرهاب (1999)

لا تُشير هذه الاتفاقية بشكل مباشر إلى الإرهاب الإلكتروني، لكنها تضع إطارًا عامًا يمكن أن يشمل تمويل الجرائم الإرهابية عبر الوسائل الرقمية، بما في ذلك التحويلات المشفّرة أو جمع التبرعات عبر الإنترنت لصالح تنظيمات إرهابية.

2- اتفاقية بودابست لمكافحة الجرائم السيبرانية (2001)

تُعد هذه الاتفاقية أول صك دولي يُعالج الجرائم المرتكبة عبر الإنترنت، لكنها لم تتناول الإرهاب الإلكتروني كجريمة ذات طابع خاص. ورغم ذلك، تُشكّل أساسًا قانونيًا يمكن للدول الاعتماد عليه في تجريم الأفعال الإلكترونية ذات الطابع الإرهابي، لا سيما في ما يتعلق بالوصول غير المشروع إلى النظم، أو نشر برامج خبيثة.

3- الاستراتيجية الدولية للأمم المتحدة لمكافحة الإرهاب (2006)

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

تُشير إلى ضرورة منع استخدام الإنترنت لأغراض الإرهاب، وتدعو الدول إلى تعزيز الأمن الإلكتروني، لكنها تترك تحديد المفاهيم والتعريفات للتشريعات الوطنية.

4- الاتحاد الأوروبي (توجيه 541/2017)

يتناول هذا التوجيه "الجرائم الإرهابية المرتكبة من خلال تكنولوجيا المعلومات"، ويشمل في طياته أفعال مثل التحريض على الإرهاب، أو التلقين، أو التخطيط له من خلال الوسائل الإلكترونية، وهو بذلك يُقارب مفهوم الإرهاب الإلكتروني دون أن يفرده بتعريف مستقل.

5- البيان العربي حول استخدام الإنترنت في الإرهاب (مجلس وزراء الداخلية العرب)

أصدر المجلس عدة بيانات وتصريحات منذ مطلع الألفية الثالثة تؤكد خطورة استخدام الإنترنت في الدعاية والتحريض والتمويل لصالح جماعات إرهابية، دون أن يصوغ تعريفًا دقيقًا للإرهاب الإلكتروني، لكنه يعترف به كجريمة عابرة للحدود تتطلب تعاونًا إقليميًا فعالًا.

المطلب الثاني

وسائل وخصائص الإرهاب الإلكتروني

تمهيد وتقسيم :

يُعد الإرهاب الإلكتروني من أبرز الظواهر الجديدة التي تهدد الأمن السيبراني العالمي في العصر الحديث، حيث يجسد تطورًا خطيرًا في أساليب تنفيذ الجرائم الإرهابية باستخدام الفضاء الرقمي. يختلف الإرهاب الإلكتروني عن الإرهاب التقليدي في أنه يستغل الفضاء الإلكتروني الذي لا يعترف بالحدود الجغرافية، مما يجعله أكثر تعقيداً وأقل قابلية للرقابة والملاحقة.

تتمثل وسائل الإرهاب الإلكتروني في استخدام الإنترنت، الشبكات الاجتماعية، والأنظمة الرقمية في نشر الفكر المتطرف، تنظيم الهجمات السيبرانية، وتعطيل الأنظمة الحيوية في الدول، بالإضافة إلى التهديدات المباشرة عبر التقنيات الحديثة مثل البرمجيات الخبيثة (Malware) والهجمات الموزعة (DDoS).

الفرع الأول : وسائل الإرهاب الإلكتروني

الفرع الثاني : خصائص الإرهاب الإلكتروني

الفرع الأول

وسائل الإرهاب الإلكتروني

1- التنسيق والإتصال

تستخدم الجماعات الإرهابية البريد الإلكتروني وشبكات التواصل الاجتماعي والمنتديات وغيرها من وسائل الاتصال الحديثة وتقنيات الذكاء الاصطناعي، بوصفها وسيلة للتواصل وتبادل المعلومات والمقترحات فيما بين أعضائها، وللتخطيط لعملياتها، وذلك بهدف تقليل المخاطر الأمنية التي قد تلحقهم و التي تنتج عن القيام باللقاءات المباشرة بين أعضاء الجماعات الإرهابية على أرض الواقع، أو للتخفيف من استخدام وسائل الاتصال التقليدية التي يسهل من خلالها تتبع الإرهابيين وإلقاء القبض عليهم .[١٠]

فعبر وسائل التواصل الاجتماعي تقوم الجماعات المتطرفة بحملات اتصال مستمرة، تستهدف الضعفاء والمتعاطفين معهم، لحثهم ودفعهم على التطرف وممارسة العنف باسم الأيديولوجيات المتطرفة، ومع هذا التواصل الغير محدود ، أصبحت هذه الوسائل طرفاً أساسياً في نشر الإرهاب بسهوله .

2- التجسس علي المواقع وتدميرها

يقوم الإرهابيون المبرمجون الذين يسمون ب(الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية، ومع تطور تقنيات الذكاء الاصطناعي أصبح هذا الأمر سهلاً وحدث للعديد من الدول في مواقعها الإلكترونية الهامة .

وفي الثالث من يوليو 2021 تعرضت نحو 200 شركة أمريكية لهجوم إلكتروني "موسع" ببرمجيات الفدية الخبيثة، وفقا لإحدى مؤسسات الأمن الإلكتروني في الولايات المتحدة.

ومن الأمثلة الواقعية أيضاً عندما تمكن احد القراصنة من السيطرة على نظام الكومبيوتر في مطار أمريكي، وإطفاء مصابيح إضاءة ممرات الهبوط ،مما هدد بحصول كارثة، ومثله ما حدث في ايطاليا حينما تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها وما حدث في عام 2001 حينما اخترق متسللون حاسبات شبكة كهرباء كاليفورنيا[١١]

وبالتالي فإن ارتكاب جرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب الآلي، في إطار جرائم الإرهاب الإلكتروني، يتم باستخدام الفيروسات الإلكترونية ، بقصد الحصول على معلومات متعلقة بالأماكن والمنشآت الحيوية لاستهدافها بالعمليات الإرهابية، أو من أجل تدمير أو تعطيل في برامج الحواسيب . [١٢]

3- الترويج الإعلامي

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

لعل من أهم الأهداف التي يسعي إليها الإرهابيين هو بث المعلومات المضللة ضد أي مؤسسة أو دولة هو بث الأفكار المتطرفة التي تتبناها الجماعة الإرهابية التي قامت بالإنشاء. كما أنها تقوم على نشر الأخبار الكاذبة والمضللة لأجهزة الأمن والرأي العام، أو الآراء التي تسبب التفرقة، أو الإساءة إلى الأديان أو الأعراق أو الأصول.

إضافة لما سبق يمكن أن يكون الهدف من استخدام الإرهابيين للتكنولوجيا نشر ثقافة العنف، والتشجيع على الاستخدام المفرط له، والإنسياق في أعمال الإرهاب، من خلال نشر الجهات الإرهابية لنصوص وصور وتسجيلات ومقاطع فيديو تظهر الإرهابي بمظهر البطل الشجاع مما يغرس في عقيدة الأطفال والشباب الصغار علي ان مثل هذه التصرفات هي معني الشجاعه والبطولة وإبعادهم عن ساحة الحرب لصالح بلادهم.

الفرع الثاني

خصائص الإرهاب الإلكتروني

يتميز الإرهاب الإلكتروني بعدد من الخصائص والسمات التي يختلف فيها عن الإرهاب العادي ولعل أهم ما يختلف فيه هو أن الإرهاب الإلكتروني يعتمد علي الوسائل التقنية الحديثة في تنفيذه وفيما يلي بيان خصائص الإرهاب الإلكتروني .

1- الإرهاب الالكتروني لا يحتاج في ارتكابه إلى العنف والقوة

الإرهاب الالكتروني لا يحتاج في ارتكابه إلى العنف والقوة بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة لعملية نشر المعلومات .

يتميّز الإرهاب الإلكتروني عن صور الإرهاب التقليدي في كونه لا يشترط استخدام العنف المادي أو القوة المسلحة لتحقيق أهدافه، بل يعتمد بشكل أساسي على التقنيات الرقمية وأدوات التكنولوجيا الحديثة.

2- الإرهاب الإلكتروني جريمة عابره للحدود

يتسم الإرهاب الالكتروني بكونه جريمة إرهابية متعدية الحدود وعابره للدول والقارات وغير خاضعة لنطاق إقليمي محدود ، ليس فقط من حيث آثارهَا وأضرارها، بل أيضا، من حيث مراحل إعداده وتنفيذه، فقد يتم التخطيط للجريمة الإرهابية بدولة، ويتم جمع التمويل اللازم لتنفيذها ورصده بدولة أخرى، ويتم التنفيذ بدولة ثالثة. ويختلف الإرهاب الإلكترونى بهذه السمة، عن الجرائم الإلكترونية الأخرى والتى عادة ما تحدث فى نطاق محلى، كما ينتمى الإرهاب الإلكترونى، فى المقابل، على أثر هذه الخاصية إلى طائفة الجرائم المنظمة . [١٣] وذلك يرجع إلي تطور التكنولوجيا وتقنيات الذكاء الاصطناعي والإتصالات وجدت التنظيمات الإرهابية المجال الخصب لإرتكاب أنشطتها الإرهابية علي الصعيد الرقمي ، فأصبح الإرهاب الإلكتروني بلا حدود ، حيث يمكن أن يكون المجرم في مكان ما ويقوم بجريمته في مكان آخر مما أسبغ علي هذه الجرائم صفة العالمية .

4- مهارة في التقنيات التكنولوجية

توافر قدر من المهارة والخبرة بتكنولوجيا المعلومات لدى الإرهابيين، أفراد، كانوا أو جماعات، تمكنهم من توظيف شبكة الإنترنت لخدمة أغراضهم الإرهابية علي جميع المستويات من حيث التخطيط والدعاية والتمويل والتدريب والتنفيذ .[١٤]

فالإرهابي الإلكتروني غالبًا ما يكون شخصًا يمتلك مهارات متقدمة في مجالات مثل:

- أمن المعلومات واختراق الشبكات . - التشفير والتخفي الإلكتروني (Cryptography and Anonymity Tools) . - البرمجة وهندسة البرمجيات الخبيثة (Malware) . - إدارة الخوادم ونظم التشغيل المعقدة.

5- فداحة الخسائر

من السمات الجوهرية التي تميّز الإرهاب الإلكتروني عن غيره من أنماط الجرائم الإلكترونية الأخرى، هي فداحة الخسائر التي قد تنجم عنه، سواء على المستوى المادي أو المعنوي أو السياسي. وفداحة الخسائر الناتجة عن الإرهاب الإلكترونى والتى تكاد تكون أضعاف الخسائر التى تحدثها الجرائم الإرهابية التقليدية، سواء من حيث الأرواح أو الممتلكات، خاصة فى الدول التى تعتمد بشكل كبير على تكنولوجيا المعلومات مثل الولايات المتحدة واليابان وإنجلترا . [١٥]

إضافة لما سبق يُعد حجم الخسائر الناتجة عن الإرهاب الإلكتروني من أبرز الخصائص التي تميّزه عن غيره من أشكال الإجرام التقليدي والرقمي، إذ أن الهجوم الإلكتروني الواحد قد يُحدث أضرارًا تفوق ما تحدثه عملية إرهابية تقليدية كاملة، وذلك من حيث التأثير الاقتصادي، أو تعطيل البنية التحتية، أو زعزعة الأمن القومي.

وقد تشمل هذه الخسائر:

- تعطيل القطاعات الحيوية مثل الكهرباء، والنقل، والصحة، والاتصالات، ما يؤدي إلى شلل شبه كامل في مؤسسات الدولة.

- تسريب معلومات سيادية أو حساسة قد تُهدد الأمن القومي وتعرّض حياة المواطنين للخطر.

6- صعوبة الإثبات في الإرهاب الالكتروني

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

نظراً لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره . كما إن المعلومات التى يحملها الإنترنت يسهل إخفاؤها ويتم تخزينها علي شكل رموز يصعب فكها لغير المتخصصين ، كما أن الدليل المادي يصعب إثباته لأن الجانى مرتكب هذه الجريمة لا يترك وراءه أى أثر مادى خارجى ملموس يمكن فحصه، الأمر الذى يجعل من الصعب على رجال الأمن معرفة مرتكب الجريمة ، بخلاف الجرائم التي تتم علي أرض الواقع وليس الفضاء الالكتروني، التى عادة ما تترك واراءها دليلاً مادياً أو شهادة شهود أو غيرها من أدلة الإثبات.

وتتمثل أهم مظاهر صعوبة الإثبات في النقاط الآتية:

- **سهولة إخفاء الهوية الرقمية:** للمجرم الإلكتروني باستخدام أدوات مثل الشبكات المظلمة (Dark Web)، وبرامج إخفاء العنوان الرقمي (VPN)، مما يجعل تحديد هوية الجاني بدقة أمراً شاقاً.

- **سرعة محو الأدلة** : الرقمية أو تغييرها، إذ يمكن للجاني حذف أو تعديل محتويات إلكترونية خلال ثوانٍ معدودة دون ترك أثر.

7- الإرهاب الإلكتروني جريمة عمدية

علمنا فيما سبق أن جريمة الإرهاب الإلكتروني يسبقها تخطيط واضح من الإرهابيين ، ووضع المعلومات المغلوطة والمراد بثها ، كذا تشمل التحضيرات تصوير فيديو ليتم من خلاله بث أفكار بعينها تعمل علي نشر العنف والجريمة والكراهية ، إذن فتكون من الجرائم العمدية التي يسبقها تحضير .

- ويتميز القصد الجنائي في هذه الجريمة بأنه:

- **قصد خاص** : يتجه إلى إحداث نتيجة معينة مثل: زعزعة الأمن، بث الرعب، تهديد الاستقرار، الإضرار بالبنى التحتية الحيوية للدولة.

- يُفترض فيه التخطـيط المسبق، إذ إن تنفيذ الجرائم الإلكترونية الإرهابية يتطلب معرفة تقنية وأدوات رقمية، مما يدل على توافر نية مدروسة.

المطلب الثالث

أسباب الإرهاب الإلكتروني

أصبح الإرهاب الإلكتروني في العصر الرقمي الحديث أحد أخطر التهديدات التي تواجه الأمن الوطني والدولي، وذلك نتيجة لما يمتلكه من خصائص تجعل مواجهته أكثر تعقيداً من الإرهاب التقليدي. ولا يمكن فهم هذه الظاهرة بشكل دقيق دون التطرق إلى الأسباب والدوافع التي تقف خلفها، والتي تمثل المدخل الأساسي لتحليل طبيعة الإرهاب الإلكتروني وآليات انتشاره.

وتتسم هذه الأسباب بالتعدد والتداخل، إذ تشمل جوانب تقنية، وأخرى اجتماعية، واقتصادية، وأيديولوجية، تُسهم مجتمعة في خلق بيئة خصبة لممارسة هذا النوع من الإرهاب. فقد أتاح التطور التكنولوجي أدوات رقمية متقدمة يسهل استخدامها في تنفيذ أعمال تخريبية، في ظل ضعف البنية التحتية المعلوماتية لبعض الدول، وتراجع مستوى الوعي الأمني لدى الأفراد والمؤسسات.

الفرع الأول : الأسباب التقنية للإرهاب الالكتروني

الفرع الثاني : غياب الحدود الجغرافية وتدني مستوي المخاطرة

الفرع الثالث : الأسباب الإقتصادية للإرهاب الالكتروني

الفرع الرابع : صعوبة إكتشاف وإثبات جرائم الإرهاب الالكتروني

الفرع الخامس : غياب السيطرة والرقابة علي شبكة الإنترنت

الفرع الأول

الأسباب التقنية

أولاً : ضعف البنية التحتية السيبرانية

وهي التي تتعلق بضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للإختراق من خلال الثغرات المتاحة بها فيمكن للإرهابين استغلال هذه الثغرات والتسلل للبني المعلوماتية التحتية وممارسة عملهم الإرهابي .[١٦]

والسبب فى ذلك، هو أن شبكات المعلومات مصممة فى الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها، مما يمكن أفراد الجماعات والتنظيمات الإرهابية من التسلل إلى البنية التحتية للمؤسسات والمرافق الحيوية للدولة المستهدفة وتخريبها بسهولة ، إضافة إلى صعوبة التعرف على الهوية الإلكترونية للإرهابى، حيث يقوم بشن هجومه بهوية وشخصية وهمية يتستر ورائها للتخفى عن أعين الأجهزة الأمنية، بل ويغيرها من حين إلى آخر.[١٧]

تُشير تقارير منظمة الشرطة الجنائية الدولية (Interpol) إلى أن العديد من الدول النامية تعاني من ضعف في أنظمة الحماية الإلكترونية، مما يجعلها أهدافًا سهلة للهجمات الإرهابية التي تستهدف قطاعات حيوية كالمطارات، البنوك، وشبكات الطاقة.[١٨]

ثانياً : ضعف التشفير واستخدام الشبكة المظلمة (Dark Web)

توفر الشبكة المظلمة بيئة خفية لتداول المعلومات وبيع أدوات الهجوم الإلكترونية، بعيداً عن رقابة السلطات. وقد رصدت تقارير الأمم المتحدة استخدام تنظيمات إرهابية مثل "داعش" للدارك ويب في تجنيد الأفراد وتمويل العمليات الإرهابية.

الفرع الثاني

غياب الحدود الجغرافية وتدني مستوي المخاطرة

يُعد غياب الحدود الجغرافية أحد الخصائص الجوهرية للفضاء الإلكتروني، وهو ما يمثل سبباً مباشراً في تفشي الإرهاب الإلكتروني،

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

إذ تتيح الطبيعة المفتوحة والعالمية للإنترنت إمكانية تنفيذ الهجمات الإرهابية من أي مكان في العالم، دون التقيد بحدود الدولة أو القيود السيادية.

فالمجرم الإلكتروني يستطيع، بكبسة زر، أن يُخطط ويُنفذ هجوماً يستهدف منشأة حيوية في دولة أخرى، مستخدماً أدوات وتقنيات تخفي هويته، دون الحاجة إلى التواجد المادي في مسرح الجريمة، وهو ما يقلل من احتمالية القبض عليه أو إخضاعه للمساءلة الجنائية.

ويؤدي هذا إلى تدني مستوى المخاطرة بالنسبة للجماعات الإرهابية، حيث تتيح لهم البيئة الرقمية ممارسة أنشطتهم بأمان نسبي، بعيداً عن أعين أجهزة الأمن التقليدية، مستفيدين من الثغرات القانونية، واختلاف التشريعات بين الدول، وضعف التعاون الدولي أحياناً في ملاحقة الجرائم السيبرانية.

كما إن السمة العولمية لشبكات المعلوماتية بالإضافة إلي عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئتة المفتوحة يعد فرصة مناسبة للإرهابيين ، حيث يستطيع محترف الحاسوب ان يقدم نفسه بالهوية والصفة التي يرغب بها أو يتخفي تحت شخصية وهمية ، ومن ثم يشن هجومه الإلكتروني وهو مسترح في منزله دون مخاطرة مباشرة وبعيداً عن أعين الأمن .[١٩]

وقد أشارت وكالة الشرطة الأوروبية (Europol) في تقريرها السنوي عن التهديدات السيبرانية لعام 2022 إلى أن "الإرهابيين باتوا يفضلون استخدام الإنترنت لتنفيذ أو التنسيق لهجماتهم نظراً لانخفاض الكلفة وانعدام الحاجة إلى التواجد الفعلي في مسرح الجريمة، مما يجعل التحقيقات والملاحقة أكثر صعوبة وتعقيداً[٢٠]

الفرع الثالث

الأسباب الإقتصادية للإرهاب الالكتروني

تلعب العوامل الاقتصادية دوراً جوهرياً في دفع بعض الأفراد والجماعات نحو ممارسة الإرهاب الإلكتروني، سواء بدافع تحقيق الربح المباشر أو بهدف زعزعة استقرار الاقتصاد الوطني للدول المستهدفة. ويُعد الجانب الاقتصادي من أخطر أبعاد هذه الجريمة، حيث يتداخل فيه الطمع الشخصي مع الأجندات التخريبية للمنظمات الإرهابية.

أولًا: يُمثل الحافز المالي عامل جذب رئيسي للأفراد الذين يعانون من البطالة أو الفقر، لا سيما في الدول التي تفتقر إلى فرص اقتصادية مستقرة، إذ يلجأ البعض إلى تنفيذ هجمات إلكترونية مثل الابتزاز الرقمي (Ransomware) أو سرقة البيانات البنكية للحصول على عوائد مالية غير مشروعة. وتُظهر تقارير الأمن السيبراني أن الجماعات الإرهابية بدأت تعتمد على هذا النوع من الهجمات كمصدر تمويل بديل عن الوسائل التقليدية.[٢١]

ثانيًا: تسعى بعض الجماعات الإرهابية إلى استهداف الاقتصاد القومي للدول كوسيلة لإثارة الفوضى أو الضغط السياسي. فالهجمات التي تستهدف البنية التحتية الاقتصادية كالبنوك، شركات الطاقة، والموانئ الذكية، تُحدث خسائر ضخمة للدول، سواء على مستوى المال أو الثقة في النظام الاقتصادي، ما يُعد هدفًا إستراتيجيًا للإرهابيين.

على سبيل المثال: أشار تقرير صندوق النقد الدولي لعام 2024 إلى أن الخسائر الناتجة عن الحوادث السيبرانية الشديدة قد تضاعفت أربع مرات منذ عام 2017، لتصل إلى 2.5 مليار دولار، مع تأثيرات غير مباشرة أكبر بكثير، مثل الأضرار بالسمعة وتكاليف تعزيز الأمان.[٢٢]

كما أوضح تقرير صادر عن شركة Allianz أن هجوماً سيبرانياً كبيراً على شبكة الكهرباء الأمريكية قد يتسبب في خسائر اقتصادية وتأمينية تتجاوز 240 مليار دولار، وقد تصل إلى أكثر من تريليون دولار.[٢٣]

ثالثاً : البطالة

مما لاشك أن البطالة [٢٤]والكساد وانحطاط الوضع الاقتصادي ، وتدني مستوي المعيشة وعدم التناسب بين الأسعار والأجور ، هي عوامل تصيب الأفراد بحالة من الإحباط واليأس وعدم الإهتمام بحياته أو حياة غيره ، وهو ما يجعله سهل الإنقياد إلي الجماعات الإرهابية المنظمة التي قد تبشره بالتغيير وتحسين الأوضاع، ومن ثم التورط في ارتكاب جرائم عنف .

الفرع الرابع

صعوبة إكتشاف وإثبات جرائم الإرهاب الالكتروني

نظراً لسرعة غياب الدليل الرقمى وسهولة إتلافه وتدميره، علاوة على صعوبة السيطرة على المعلومات المتبادلة والمنشورة عبر الإنترنت، وكذا صعوبة فرض الرقابة على مجمل الاتصالات التى تتم من خلال الشبكة، الأمر الذى وفر للإرهابيين ملاذات آمنة لمباشرة أنشطتهم الإرهابية عبر الفضاء الإلكترونى، دون خوف أو قلق من أن ترصدهم الأجهزة الأمنية المعنية.[٢٥]

ومن أهم أسباب صعوبة اكتشاف جرائم الإرهاب الالكتروني :

1- إستخدام تقنيات التشفير والهوية المجهولة: يلجأ العديد من الإرهابيين إلى استخدام تقنيات تشفير متقدمة، مما يجعل تتبع الأنشطة الإجرامية أكثر تعقيداً. تُستخدَم برامج التشفير لتأمين التواصل بين الخلايا الإرهابية، مما يجعل من الصعب تحديد هوية الجناة أو المواقع الجغرافية التي تُنفذ منها الهجمات. كما أن الفضاء

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

الإلكتروني يوفر أدوات تمكن الإرهابيين من إخفاء هويتهم الحقيقية، سواء من خلال استخدام الشبكات الافتراضية الخاصة (VPNs) أو شبكة الإنترنت المظلم (Dark Web).[٢٦]

2- التحديات التقنية والمعرفية: تواجه السلطات المعنية بالأمن الإلكتروني صعوبة كبيرة في مواجهة الأدوات التكنولوجية الحديثة التي يستخدمها الإرهابيون، مثل البرمجيات الخبيثة (Malware) وبرامج الفدية (Ransomware)، التي تُصمم خصيصًا للتسلل إلى الأنظمة المستهدفة دون ترك آثار واضحة. وهذا يتطلب مستوى عالٍ من الخبرة التقنية للتحقيق في الحوادث.

4- تحليل الأدلة الرقمية: تتطلب الجريمة الإرهابية الإلكترونية جمع وتحليل كميات ضخمة من الأدلة الرقمية من خلال البحث في سجلات الإنترنت أو البيانات المخزنة على الخوادم. وهذه العملية معقدة، إذ قد تحتوي على بيانات مشوشة أو معدلة، مما يجعل من الصعب إثبات الجريمة في محكمة قانونية.

الفرع الخامس

غياب السيطرة والرقابة علي شبكة الإنترنت

يُعد غياب الرقابة الفعّالة على شبكة الإنترنت من أبرز العوامل التي تُسهم في تنامي ظاهرة الإرهاب الإلكتروني، حيث يُتيح هذا الغياب بيئة خصبة لنمو وتوسع الجماعات الإرهابية في الفضاء الرقمي. تُظهر الدراسات أن العديد من الدول تعاني من قصور في البنية التشريعية والتقنية الكفيلة بالرقابة على الفضاء الإلكتروني، خاصةً في ظل التوسع الكبير في استخدام تقنيات مثل الإنترنت المظلم (Dark Web) وخدمات التشفير. ووفقًا لتقرير مجلس الأمن التابع للأمم المتحدة لعام 2023، فإن "الجماعات الإرهابية تستغل ضعف الرقابة الرقمية في بعض الدول من أجل الترويج لأفكارها واستقطاب مؤيدين جدد، بالإضافة إلى استخدام الشبكات الإلكترونية في التدريب وتنسيق العمليات.[٢٧]

وبذلك، يُسهم غياب الرقابة الفعالة على شبكة الإنترنت في تمكين الجماعات الإرهابية من استغلاله كأداة رئيسية في تنفيذ أجنداتها، الأمر الذي يستدعي من المجتمع الدولي توحيد الجهود وبناء إطار قانوني وتقني مشترك للحد من هذه الظاهرة.

المبحث الثاني

الأحكام العامة في جريمة الإرهاب الإلكتروني

تمثل جريمة الإرهاب الإلكتروني واحدة من أخطر التحديات القانونية في العصر الرقمي، حيث أصبح الفضاء السيبراني بيئة خصبة لممارسة أنماط متعددة من السلوك الإرهابي الذي يهدد أمن الأفراد والدول على حد سواء. وقد أفرز هذا النوع من الجرائم الحاجة إلى وضع إطار قانوني خاص يحدد الأحكام العامة التي تحكمها، وعلى رأسها صور الجريمة وأركانها، باعتبارها المدخل الأساسي لفهم طبيعتها القانونية.

وتتعدد صور الإرهاب الإلكتروني بتعدد الوسائل المستخدمة فيه، فقد يأخذ شكل اختراق الأنظمة الحيوية، أو تعطيل البنى التحتية للدولة، أو نشر محتوى متطرف يحرض على العنف والكراهية، أو استخدام الإنترنت في التخطيط والتنسيق للعمليات الإرهابية الواقعية.

أما من حيث الأركان، فإن جريمة الإرهاب الإلكتروني لا تختلف كثيراً في بنيتها العامة عن الجريمة التقليدية، إذ تتطلب توافر ركن مادي يتمثل في الفعل الإرهابي الموجه عبر الوسائل التقنية، وركن معنوي يتمثل في القصد الجنائي الخاص .

ومن هنا تأتي أهمية تناول الأحكام العامة لهذه الجريمة، باعتبارها خطوة أساسية نحو تحديد نطاق المسؤولية الجنائية، والتمييز بينها وبين غيرها من الجرائم المعلوماتية ذات الطابع غير الإرهابي.

المطلب الأول : صور الإرهاب الإلكتروني

المطلب الثاني : أركان الإرهاب الإلكتروني

المطلب الأول

صور الإرهاب الإلكتروني

إن الإرهاب الإلكتروني استهدف التقنية في القرن الحادي والعشرين والذي يؤثر على القوى الانتاجية والثقة بالمجتمعات مابعد الصناعية ، ويسعى ارهابي الإرهاب الإلكتروني من خلال إستغلال موارد العالم المادي والإفتراضي ، ومن خلال الوصول الى المداخل العامة والخاصة بين العالمين ، والإنتقال والتجمع والإسترداد ، الى تدمير النقاط الالتقاء الايجابية ، والتي تمثل حالة للرفاه المجتمعي والمعرفة ، بالإضافة الى عمل تغيرات أساسية في الانظمة العاملة ، كما تسعى المنظمات الارهابية من خلال الثروة التقنية تقنية المعلومات الى تدمير البنية التحتية للخصوم والاعداء وخاصة فيما يتعلق بالقوات المسلحة من حيث تدمير أنظمة الاتصال الجوية والبرية والبحرية .[٢٨]

ان إخضاع العالم المادي والإفتراضي الى سيطرة وتحكم إرهابي والإرهاب الإلكتروني يختلف تماماً عن دور القراصنة أو الهواه الذين يسعون الى الحصول على مكاسب مادية محدودة ، أو بهدف المتعة والتسلية او الازعاج أحيانا ، فأن هذه الجرائم لاتدخل ضمن مفهوم الإرهاب الإلكتروني ، وعلى الرغم ماتسببه من خسائر فهي لاتعدو أن تكون مجرد جرائم عادية إرتكبت بواسطة شبكات المعلوماتية ، ويرجع

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

سبب ذلك الى ان تلك الجرائم لم ترتكب لأغراض الإخلال بالنظام العام او الامن المعلوماتي ، أو تعريض سلامة المجتمع وامنه للخطر.[٢٩]

وعلي ذلك يتم بيان صور الإرهاب الإلكتروني علي النحو التالي :

الفرع الأول : تبادل المعلومات الإرهابية ونشرها عبر الوسائل الإلكترونية

الفرع الثاني : تدمير واختراق المواقع والبيانات الإلكترونية والنظم المعلوماتية

الفرع الثالث : التجسس الإلكترونـــي

الفرع الرابع : التهديد والترويع الإلكتروني

الفرع الأول

تبادل المعلومات الإرهابية ونشرها عبر الوسائل الإلكترونية

مع التشديدات الأمنية التي تلاحق الإرهابيين في كل مكان أصبح أمر إلتقاؤهم صعباً للغاية يكاد يكون مستحيلاً ، وهو ما جعلهم يلجأون لوسائل أخري تكون آمنه لهم ويصعب اكتشافها ، ومع التطور التكنولوجي وتطور تقنيات تكنولوجيا المعلومات أصبح الأمر يسيراً ، وجعل تبادل المعلومات ونشرها عبر الوسائل الإلكترونية هو الخيار الأول لراغبي الجريمة بشكل عام والإرهابيين بشكل خاص .

لذلك اعتبرنا أن أولي صور الإرهاب الإلكتروني هي استخدام الوسائل الإلكترونية لتنفيذ الأهداف الإرهابية . علي النحو الآتي :

1- إنشاء المواقع الإلكترونية الإرهابية

يعرف الموقع الإلكتروني بأنه : مجال أو مكان افتراضي له عنوان محدد علي شبكة معلوماتية ، يهدف إلي إتاحة بيانات ومعلومات للعامة أوالخاصة .[٣٠]

ويقوم الإرهابيون بإنشاء وتصميم مواقع لهم علي شبكة الإنترنت بهدف بث أفكارهم الضاله والمتطرفه والدعوة إلي مبادئهم الغير سوية ، وإبراز قوة التنظيم الإرهابي ، والتعبئة الفكرية وتجنيد إرهابيين جدد ، وإعطاء التعليمات والتلقين الإلكتروني والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد علي القيام بهجمات إرهابية .[٣١] كما تهدف هذه المواقع إلي إحداث خلل بالأمن العام من خلال إظهار الإرهابيين بصورة الجيش القوي ذو العتاد الذي لا مثيل له وبالتالي يحدث حالة من الإهتزاز لدي جموع المواطنين وينتابهم شعور بالخوف تجاه حياتهم ، وآخرين ينتابهم إحساس بالفخر تجاه الإرهابيين وهو هدفهم المنشود .

ومع تزايد عدد مستخدمي الإنترنت حول العالم زيادة غير متوقعة كما انه وفقاً للاتحاد الدولي للاتصالات، فقد بلغ عدد مستخدمي الإنترنت عالمياً 5.35 مليار شخص في تقرير صدر في أوائل العام الجاري 2024 .

2- الإتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة شبكة الإنترنت للمعلومات في الإتصال والتنسيق فيما بينهم ، نظراً لقلة تكاليف الإتصال والرسائل بإستخدام شبكة الانترنت مقارنة بالوسائل الأخري كما انها كما ذكرنا الأكثر آمناً ، إضافة لذلك فإنها توفر للإرهابيين فرصة ثمينة في الإتصال والتخفي وذلك عن طريق البريد الإلكتروني أو المواقع والمنتديات دون ان يضطر الإرهابيين الإفصاح عن هويتهم[٣٢]

3- جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها ، كما - انها تعتبر موسوعة الكترونية شاملة متعددة الثقافات ، ومتنوعة المصادر ، وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها ، ، كمواقع المنشأة النووية ، ومصادر توليد الطاقة ، وأماكن القيادة والسيطرة والاتصالات ، ومواعيد الرحلات الجوية الدولية ، والمعلومات المختصة بسبل مكافحة الارهاب ، ونحو ذلك من المعلومات التي تعتبر بمثابة الكنز الثمين بالنسبة للإرهابيين نظراً لما تحتويه من معلومات تفصيلية مدعمة بالصورة الضوئية .[٣٣]

4- التخطيط والتنسيق للعمليات الإرهابية

العمليات الإرهابية عمل على جانب من التعقيد - والصعوبة ، فهي تحتاج الى تخطيط محكم ، وتنسيق شامل ، تعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الاهمية للجماعات الاهابية ، حيث تتيح لهم هوية التخطيط الدقيق والتنسيق الشامل لشن الهجمات الإرهابية المحددة في جو مريح ، وبعيدا عن اعين الناظرين مما يسهل على الارهابيين ترتيب تحركاتهم ، وتوقيت هجماتهم .[٣٤]

5- التعبئة وتجنيد الإرهابيين

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية - العالمية في نشر ثقافة الإرهاب والترويج لها ، وبث الأفكار والفلسفات التي تنادي به ، كما تسعى جاهدة الى توفير أكبر عدد ممكن من الإرهابيين في تبني افكارها ومبادئها . ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدى من لديهم ميول واستعداد للإنخراط في الأعمال التدميرية والتخريبية ، مما يوفر لديها قاعدة ممن تجمعهم نفس الافكار والتوجهات ، فيسهل تجنيدهم لتنفيذ هجمات إرهابية في المستقبل .[٣٥]

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

ويعد تجنيد الأفراد عبر الإنترنت من بين أخطر نماذج وصور الإرهاب الإلكتروني نظراً للتأثير الفعال للوسائل التقنية المعتمد عليها في عملية التجنيد وسرعة فعاليتها علي الأفراد في تكوين قناعات فكرية متطرفة ، والتي يتطلب لها سوي جهاز حاسوب أو هاتف محمول موصول بشبكة الإنترنت ، مع ضرورة وجود احترافية تقنية وفكرية لدي القائم بالتجنيد ، ولديه من الأسلوب والذكاء في الحوار ما يمكنه من التأثير علي المستهدف وذلك بهدف تكويت جيوشاً افتراضية من مختلف الأنحاء حول العالم . [٣٦]

جديراً بالذكر ان الفئات المستهدفه هي التي تنتمي لأفكار بعينها لاتقبل النقاش فيها ، فمن يجادل شخص لإقناعه بأراءه لابد ان يعلم توجهه جيدا حتي يستطيع السيطرة عليه ، وغالباً ما يستخدم الارهابيين الدين سلاحاً لضم أكبرعدد من الشباب بإقناعم ان ذلك الانضمام له فائدة عظمي في نصر الدين .

6- التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية الى تدريب خاص ، ويعد التدريب - من أهم هواجس التنظيمات الارهابية ، وقد انشأت معسكرات تدريبية سرية لكن مشكلة معسكرات تدريب الإرهابيين انها دائما معرضة للخطر ، ويمكن اكتشافها ومداهمتها في أي وقت ، ولذا فأن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي ، كما قامت بعض الجماعات الإرهابية بأنتاج ادلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي ، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل الى الإرهابيين في مختلف أنحاء العالم . [٣٧]

الفرع الثاني

تدمير واختراق المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الارهابية بشن هجمات الكترونية من خلال الشبكات المعلوماتية ، بقصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية ، والحاق الضرر بالبنيه المعلوماتية التحتية وتدميرها ، وتستهدف الهجمات الارهابية في عصر المعلومات ثلاثة اهداف اساسية غالبا ، وهي الاهداف العسكرية والسياسية والإقتصادية . [٣٨]

ويستطيع قراصنة الحاسب الالي التوصل الى المعلومات السرية والشخصية ، واختراق خصوصية سرية المعلومات بسهولة ، وذلك يرجع الى أن التطور المذهل في عالم الحاسب الألي والشبكات المعلوماتية يصحبه تقدم أعظم في الجرائم المعلوماتية وسبل ارتكابها ولاسيما أن مرتكبيها ليسوا مستخدمين عاديين ، بل قد يكونون خبراء في مجال الحاسب الألي . كما أن عملية الإختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة وبرامج شبكة الانترنيت ، نسبة كبيرة من الإختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الالي والشبكات المعلوماتية . [٣٩]

ومن الممكن تصور هجوم الالكتروني على أحد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل ، حيث يمكن أن يقوم الارهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية ، والحاق الشلل بأنظمة القيادة والسيطرة والإتصالات ، ومحطات توليد الطاقة والماء ، ومواقع الاسواق المالية ، بحيث ي دي توقفها عن العمل الى تحقيق آثار تدميرية تفوق ماتحدثة القنابل والمتفجرات من آثار . [٤٠]

ويمكن أن يكون الهجوم الإلكتروني علي المواقع بهدف الإستيلاء علي محتوياتها مثل ما يحدث مع المواقع المالية للبنوك من سرقة أموالهم عن طريق اختراق حساباتهم .

وبالتالي فإن ارتكاب جرائم الإتلاف والتشوية للبيانات والمعلومات وبرامج الحاسب الألي في إطار جرائم الإرهاب الإلكتروني ، يتم بإستخدام الفيروسات الإلكترونية بهدف الحصول علي معلومات تتعلق بالآماكن والمنشآت الحيوية لإستهدافها بالعمليات الإرهابية أو من أجل تدمير أو تعطيل برامج الحواسيب . [٤١]

وهناك العديد من الأمثلة علي هذه الجرائم ومنها قيام الجماعات الإرهابية بمهاجمة نظم التحكم بوسائل المواصلات المختلفة مما يؤدي إلي تعطيل وإرباك حركة الطيران وإحداث تصادمات فيما بين الطائرات أو القطارات أو اختراق مواقع المنشآت الحيوية كمؤسسات الكهرباء أو الغاز والبترول من أجل إلحاق الأذي بها وإضعاف الثقة بالإقتصاد الوطني والمؤسسات الحكومية . [٤٢]

الفرع الثالث

التجسس الإلكتروني

يُعد التجسس الإلكتروني (Cyber Espionage) من أخطر صور الإرهاب الإلكتروني، لما ينطوي عليه من تهديد مباشر للأمن القومي للدول، والمؤسسات السيادية، والقطاعات الحيوية كالدفاع والطاقة والمصارف. إذ تعتمد الجماعات الإرهابية وبعض الدول الراعية لها على تقنيات التجسس الرقمي للحصول على معلومات سرّية أو حساسة، تُستخدم لاحقًا إما في تنفيذ عمليات إرهابية دقيقة، أو للابتزاز السياسي والاقتصادي.

ومع الثورة المعلوماتية وانتشار شبكات الإتصالات وتزاوجها مع شبكات المعلوماتية وظهور شبكة الإنترنت ، جعل من المعلومات

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

المخزنة علي تلك الشبكات هدفاً للمحتالين والتنظيمات الإرهابية وذلك بإستخدام التكنولوجيا المعلوماتية ، حيث تمكن العديد من الجواسيس التابعين للتنظيمات الإرهابية من اختراق الكثير من أجهزة الحاسب والشبكات المؤمنة الخاصة بالدول والشركات والأفراد دون أن يغادروا أماكن تواجدهم ودون أن يتركوا أثر يذكر .

ومع وجود هذه التقنيات الحديثة فأن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي ، وقد تحولت وسائل التجسس من الطرق التقليدية الى الطرق الإلكترونية ، وخاصة مع ظهور الشبكات المعلوماتية وانتشارها عالميا ، ومع توسع التجارة الالكترونية عبر الشبكة العالمية للمعلومات تحولت مصادر المعلومات التجارية الى اهداف للتجسس الاقتصادي . [٤٣]

وتتمثل الخطورة في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ، ولايمكن حتماً الإعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية فهي ليست أمنية ، ولايمكن الإطمئنان لها تماماً . وتجدر الإشارة الى أن الطرق الفنية للتجسس المعلومات سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية ، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية ، وخصوصاً العسكرية والسياسية والإقتصادية ، وهذه المعلومات اذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن [٤٤] .

ويتزايد خطر التجسس الإلكتروني في ظل الاعتماد المتزايد على الفضاء الرقمي، مما يجعل من الصعب أحياناً التمييز بين الهجمات ذات الطابع الاستخباراتي والهجمات الإرهابية، خاصة عندما تُستخدم المعلومات المسروقة في تنفيذ عمليات ميدانية دقيقة ضد أهداف مدنية أو عسكرية.

وبناءعليه، يُمكن اعتبار التجسس الإلكتروني من الأدوات الاستراتيجية التي تُستخدم في الإرهاب الحديث، حيث لا يقل خطره عن الهجمات التخريبية، بل يُعد تمهيداً خطيراً لها.

الفرع الرابع

التهديد والترويع الإلكتروني

يُعد التهديد والترويع الإلكتروني (Cyber Intimidation and Threats) من أبرز صور الإرهاب الإلكتروني، حيث تلجأ الجماعات الإرهابية إلى استخدام الوسائل الرقمية لبث الرعب والخوف في نفوس الأفراد والمجتمعات، دون الحاجة إلى تنفيذ هجمات فعلية، مما يُحقق لهم أثراً نفسياً واجتماعياً بالغ الخطورة. وتتمثل هذه الصورة في إرسال رسائل تهديد عبر البريد الإلكتروني، أو منصات التواصل الاجتماعي، أو اختراق الحسابات الشخصية وبث محتوى مرعب أو تحريضي، أو حتى التهديد بتفجير منشآت أو استهداف أفراد بعينهم.[٤٥]

حيث تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الإتصالات ومن خلال الشبكة العالمية للمعلومات ، وتتعدد أساليب التهديد وتتنوع طرقه ، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب محاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية ، ومن أجل الحصول علي التمويل المالي لإبراز قوة التنظيم الإرهابية من ناحية أخري . [٤٦]

والأخطر أن هذه التهديدات، وإن لم تُترجم إلى فعل إجرامي مادي، تُحدث أثراً قانونياً واجتماعياً حقيقياً، وقد تؤدي إلى إغلاق مؤسسات، تعطيل الخدمات، أو حتى اتخاذ قرارات أمنية على أساس "تهديدات مزعومة"، مما يُسهم في تحقيق أهداف الإرهابيين دون تكبدهم خسائر فعلية.

جديراً بالذكر انه تتعدد الأساليب والأهداف الإرهابية في التهديد فأحياناً يكون التهديد بالقتل أو التخريب والقيام بأساليب العنف والتي منها التفجيرات الإرهابية للأماكن العامة أو المنشأت والمرافق العامة .

المطلب الثاني

أركان جريمة الإرهاب الإلكتروني

تُعد جريمة الإرهاب الإلكتروني من الجرائم المركبة والمعقدة التي تتطلب توافر مجموعة من العناصر القانونية والواقعية حتى يُمكن القول بقيامها. ونظراً للطبيعة الخاصة لهذه الجريمة، والتي تمزج بين الطابع المعلوماتي والأسلوب الإرهابي في التنفيذ، فقد أصبح من الضروري الوقوف على أركانها الأساسية التي تميزها عن غيرها من الجرائم الإلكترونية التقليدية أو جرائم الإرهاب التقليدي.

فكما هو الشأن في الجرائم الجنائية بوجه عام، لا تُعاقب القوانين على مجرد الأفكار أو النوايا، بل يجب توافر ركن مادي يتمثل في فعل إيجابي يُشكّل تهديداً لأمن الدولة أو الأفراد باستخدام وسائل تقنية، إلى جانب ركن معنوي يتمثل في القصد الجنائي الخاص، والذي يتطلب توجّه الإرادة نحو تحقيق غاية إرهابية.

الفرع الأول : الركن المادي لجريمة الارهاب الالكتروني

الفرع الثاني : الركن المعنوي لجريمة الارهاب الالكتروني

الفرع الأول

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

الركن المادي لجريمة الارهاب الالكتروني

يُعد الركن المادي لجريمة الإرهاب الإلكتروني من أهم عناصر قيامها، إذ لا يكفي مجرد وجود النية أو القصد الجنائي، بل يجب أن يتحقق فعل مادي ملموس يتخذ شكل استخدام غير مشروع لوسائل التكنولوجيا الحديثة بهدف إحداث الرعب أو الإخلال بالأمن أو النظام العام. ويتمثل هذا الركن في السلوك الإجرامي المرتبط بالوسائل الإلكترونية، والنتيجة الإجرامية التي تسفر عن تهديد حقيقي أو فعلي، بالإضافة إلى علاقة السببية بين الفعل والنتيجة.

أولاً : السلوك الإجرامي

إن السلوك الإجرامي بوصفه عنصراً في الركن المادي للجريمة التقليدية يمكن رؤيته بشكل ملموس والتأكد منه كفعل القتل أو السرقة، ولكن صعوبة الجريمة الإلكترونية، أن الجريمة ترتكب عن طريق معلومات تتدفق عن طريق الحاسب الآلي والتي لا يمكن الإمساك بها مادياً .[٤٧]

والنشاط الإجرامي في جريمة الإرهاب الإلكتروني يتطلب بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الإنترنت، فيقوم المجرم مثلاً بتحميل برامج اختراقية، أو تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، وكما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها، ويصعب الفصل بين العمل التحضيري والبدء في نشاط إجرامي في جرائم الإرهاب الإلكتروني، فشراء برامج اختراق، ومعدات لفك شفرات وكلمات المرور تمثل جريمة في حد ذاتها .[٤٨]

وقد يتخذ السلوك الإجرامي في جريمة الإرهاب الإلكتروني صوراً تكون عبارة عن أفعال العنف أو التهديد التي تهدف الى إلقاء الرعب بين الناس أو تعريض حياتهم وحرياتهم وامنهم للخطر وتعريض أموالهم وممتلكاتهم للتخريب وذلك تنفيذاً لمشروع إرهابي منظم فردي أو جماعي . وكذلك استخدام المواقع الإلكترونية لنشر الأخبار التي تدعو للعنف والترويج للأفكار الإرهابية وغيرها من أعمال العنف التي تنشر الكترونياً .

إضافة لما سبق قد يتخذ السلوك الإجرامي أيضاً معاونة الأفراد علي صنع الأسلحة والإتصالات اللاسلكية والإلكترونية

ويمكن التفرقة بين نوعين من السلوك الأول إيجابي والثاني سلبي :[٤٩]

- السلوك الإيجابي

وهو استخدام نظم المعلومات أو شبكة الإنترنت أو إنشاء موقع الكتروني لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم يكون هدفة الأساسي القيام بأعمال إرهابية أو الترويج لأفكار هذا التنظيم ، أو القيام بأي أفعال هدفها تعريض حياة المواطنين للخطر .

كما أن حيازة جهاز حاسب آلي موصول بشبكة الإنترنت هو فعل مشروع ولكن يتحول الأمر حين يظهر الهدف لإستخدام جهاز الكمبيوتر وتحوله لتصرفات وأفعال غير مشروعة تهدف لزعزعة الأمن ونشر الفزع بين الناس .

- السلوك السلبي

ويقصد به الامتناع عن أداء واجب قانوني مفروض على الجاني، شريطة أن يكون هذا الامتناع قد ساعد أو سهّل ارتكاب جريمة إرهابية عبر الوسائل الإلكترونية. ومن أمثلة ذلك: امتناع مسؤول تقني عن تعطيل قناة إلكترونية يُبث من خلالها محتوى إرهابي، أو عدم الإبلاغ عن أنشطة مشبوهة تتعلق بالتحضير لهجوم إلكتروني إرهابي رغم علمه بها، متى كان ملزماً بالإبلاغ بمقتضى القانون أو طبيعة وظيفته.

والإحجام عن إتيان أمر، أوجب القانون القيام به فقد ألزم المشرع المصري كل من يعلم بقيام جريمة إرهابية أو التحضير لها ضرورة إبلاغ الجهات الأمنية عن ما يعلم ، وعاقبه بالحبس ثلاثة أشهر في حال أحجم عن الإبلاغ .[٥٠]

ثانياً : النتيجة الإجرامية

تُعد النتيجة الإجرامية إحدى ركائز الركن المادي لجريمة الإرهاب الإلكتروني، إذ لا يكفي تحقق الفعل الإجرامي أو السلوك المنهي عنه لقيام الجريمة، بل يجب أن يُسفر هذا السلوك عن نتيجة تُهدد أحد القيم المحمية قانوناً، وعلى رأسها أمن الدولة واستقرارها، أو سلامة الأفراد، أو النظام العام، أو حتى السلم المجتمعي.**وتتخذ النتيجة الإجرامية إحدي الصور الاتيه :**

- تعطيل أو شلل في البنية التحتية الرقمية أو الحيوية للدولة (مثل الهجوم على أنظمة الكهرباء أو الاتصالات أو المطارات الذكية).
- إحداث حالة من الذعر أو الفوضى المجتمعية نتيجة بث تهديدات أو معلومات مضللة عبر الإنترنت.
- التأثير في الرأي العام أو دفع الحكومات لاتخاذ قرارات استثنائية نتيجة الضغط الإلكتروني الإرهابي.

ثالثاً : علاقة السببية

تعد علاقة السببية أحد الأركان الأساسية في الركن المادي لجريمة الإرهاب الإلكتروني، حيث يتعين أن تكون النتيجة الإجرامية ناتجة بشكل مباشر عن الفعل المادي الذي قام به الجاني. وهي تمثل الرابط القانوني والواقعي بين السلوك الإجرامي الذي ارتكبه الجاني، وبين الأثر الضار أو الخطر الذي لحق بالضحية أو المجتمع. في السياق

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

الإلكتروني، قد تتخذ علاقة السببية طابعاً معقداً، بالنظر إلى الطبيعة الرقمية والمتشابكة للأدوات والتقنيات المستخدمة.

وفي جريمة الإرهاب الإلكتروني، يتطلب القانون أن يكون الفعل الذي ارتكبه الجاني قد أدى مباشرة إلى النتيجة التي تُهدد الأمن أو النظام العام أو الحياة الاقتصادية أو الاجتماعية للدولة. فإذا قام شخص باختراق أنظمة حكومية أو بنية تحتية حيوية باستخدام الإنترنت، فإن السببية تكون واضحة، حيث أدى هذا الفعل إلى تعطيل النظام أو إحداث حالة من الفوضى أو الاضطراب.[٥١]

الفرع الثاني

الركن المعنوي لجريمة الإرهاب الالكتروني

يعد الركن المعنوي أو القصد الجنائي من الركائز الأساسية في تكييف جريمة الإرهاب الإلكتروني، إذ يتعين أن تكون إرادة الجاني متجهة إلى تحقيق هدف إرهابي من خلال استخدام الوسائل الإلكترونية. ويتسم القصد الجنائي في هذه الجرائم بتعقيد خاص نتيجة لطبيعة الفعل الإلكتروني والنية الموجهة نحو إحداث ضرر جسيم باستخدام التقنيات الحديثة، سواء كانت تهدف إلى الإخلال بالنظام العام أو إحداث حالة من الذعر، أو تحقيق غايات سياسية أو دينية.

يتألف الركن المعنوي في جريمة الإرهاب الإلكتروني من عنصرين أساسيين :

أولاً : القصد الجنائي العام (الإرادة)

يتعين أن يكون لدى الجاني نية واضحة لتحقيق غاية إرهابية باستخدام الوسائل الإلكترونية. لا يُشترط أن يتعرف الفاعل على جميع تفاصيل جريمته الإلكترونية، بل يكفي أن يكون قد اتخذ السلوك الذي أدى إلى ارتكاب الفعل الإرهابي بإرادته الحرة، مع علمه بأن هذا الفعل سيؤدي إلى تهديد الأمن أو الاستقرار.

ثانياً : القصد الجنائي الخاص (الغرض الإرهابي)

يُعد من أهم أبعاد القصد الجنائي في جريمة الإرهاب الإلكتروني، وهو يتعلق بـ الهدف الذي يسعى الجاني إلى تحقيقه من خلال سلوكه الإجرامي. قد يكون هذا الهدف إحداث تغيير سياسي، أو تحقيق مكاسب مادية لجماعة إرهابية، أو إشاعة الرعب والذعر في المجتمع. ويجب أن يكون هذا الهدف محدداً وواضحاً، وأن يتم السعي لتحقيقه باستخدام الوسائل الإلكترونية، مثل نشر مواد تحريضية عبر الإنترنت، أو تعطيل الأنظمة الحكومية، أو تنفيذ هجمات إلكترونية على بنى تحتية حيوية.

المبحث الثالث

المواجهة الجنائية للإرهاب الإلكتروني

أفرز التطور المتسارع في تكنولوجيا المعلومات والاتصالات مظاهر جديدة من الجرائم، يأتي في صدارتها ما يُعرف بـ"الإرهاب الإلكتروني"، الذي يُمثل تحدياً حقيقياً لأمن الدول واستقرارها، نظراً لقدرة الجماعات الإرهابية على استغلال الفضاء السيبراني في التحريض، والتجنيد، والتمويل، بل وأيضاً في شن هجمات إلكترونية تستهدف البنية التحتية الحيوية للدول.

وقد فرض هذا الواقع الجديد على الأنظمة القانونية -سواء في الدول العربية أو الغربية– ضرورة الإسراع بتطوير منظوماتها التشريعية لمواجهة هذا النوع المستحدث من الإرهاب، الذي يختلف في طبيعته وأدواته ووسائل ارتكابه عن الجرائم الإرهابية التقليدية.

المطلب الأول : المواجهة الجنائية للإرهاب الالكتروني في القوانين العربية

المطلب الثاني : المواجهة الجنائية للإرهاب الالكتروني في القوانين الغربية

المطلب الأول

المواجهة الجنائية للإرهاب الالكتروني في القوانين العربية

في العديد من الدول العربية، تم تطوير تشريعات خاصة لمكافحة الجرائم الإلكترونية، بما في ذلك الإرهاب الإلكتروني، نظراً للتهديدات المتزايدة لهذه الجرائم على الأمن القومي. وتتنوع هذه التشريعات من دولة إلى أخرى، ولكن هناك نقاط مشتركة في غالبية هذه القوانين، ومن أبرزها:

الفرع الأول : التشريع المصري

الفرع الثاني : التشريع الإماراتي

الفرع الأول

التشريع المصري

- قانون مكافحة جرائم تقنية المعلومات (2018)

يُعد قانون تقنية المعلومات في مصر من أبرز التشريعات في المنطقة التي تناولت بشكل خاص الجرائم الإلكترونية، بما في ذلك الهجمات الإرهابية عبر الإنترنت.نصت المادة رقم2 من القانون تتضمن جريمة الإرهاب الإلكتروني في إطار الجرائم الموجهة ضد الأمن الوطني.."

وتم تشديد العقوبات على الأفعال التي تستخدم تقنيات المعلومات لتنفيذ عمليات إرهابية أو ترويج الفكر المتطرف علي النحو التالي :

أولًا: العقوبات المتعلقة باستخدام الإنترنت في أعمال إرهابية وفقًا لـ المادة 29 من القانون:

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

- "يعاقب بالسجن مدة لا تقل عن خمس سنوات كل من أنشأ أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية بهدف الترويج لأفكار داعية إلى ارتكاب أعمال إرهابية أو لتسهيل التواصل مع قيادات أو أعضاء الجماعات الإرهابية، أو تمويلها، أو ترويج المواطنين، أو الإخلال بالنظام العام أو السلام الاجتماعي."

- وإذا كانت الجريمة تهدف إلى الإخلال بالنظام العام أو تعريض أمن المجتمع للخطر أو الإضرار بالأمن القومي، تكون العقوبة السجن مدة لا تقل عن عشر سنوات.

ثانياً: العقوبات الخاصة بتمويل الإرهاب الإلكتروني

العقوبات الخاصة بتمويل الإرهاب الإلكتروني يمكن بيانها فيما يلي [٥٢]:

"يعاقب بالسجن مدة لا تقل عن عشر سنوات كل من استخدم شبكة معلوماتية أو وسيلة تقنية المعلومات، بغرض تمويل أو جمع أموال بأي وسيلة لتمويل جماعات إرهابية أو أشخاص مرتبطين بها."

ثالثًا: العقوبات التكميلية[٥٣]

تضمن القانون عقوبات تكميلية إلى جانب الحبس، ومنها:

- مصادرة الأجهزة والبرامج والوسائط المستخدمة في ارتكاب الجريمة.

- إغلاق المواقع أو الحسابات التي استُخدمت في ارتكاب الأفعال الإجرامية.

- الحرمان من بعض الحقوق المدنية والسياسية في بعض الحالات.

الفرع الثاني

القانون الإماراتي للجرائم الإلكترونية (2012)

تم إقرار قانون مكافحة الجرائم الإلكترونية في الإمارات بهدف حماية أمن الدولة وحماية البيانات الشخصية والأنظمة الحكومية من التهديدات الإلكترونية

- القانون الإماراتي لمكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012 وتعديلاته (2021)[٥٤]

أولاً: العقوبات المرتبطة باستخدام الإنترنت في الإرهاب والتحريض عليه

وفقًا للمادة (26) من القانون:

- "يعاقب بالسجن المؤبد أو السجن المؤقت وغرامة لا تقل عن 500,000 درهم ولا تجاوز 1,000,000 درهم كل من أنشأ أو أدار موقعًا إلكترونيًا أو أشرف عليه أو نشر معلومات على الشبكة المعلوماتية بقصد تسهيل الاتصال بقيادات أو أعضاء تنظيم إرهابي، أو الترويج لأفكارهم، أو تمويل أنشطتهم."

- وتُشدّد العقوبة إذا اقترنت الجريمة بالتحريض على ارتكاب أفعال إرهابية أو كانت تهدف إلى زعزعة أمن الدولة أو الإضرار بالنظام العام.

ثانياً: العقوبات المتعلقة بنشر أو تخزين محتوى إرهابي

تنص المادة (28) على:

- "يعاقب بالسجن مدة لا تقل عن عشر سنوات كل من حاز أو حصل أو استعمل أو نشر محتوىً إلكترونيًا يتضمن موادّ مخصصة لتسهيل ارتكاب عمل إرهابي، أو محتوى يهدف إلى التحريض أو التدريب عليه."

- وتُعد حيازة هذا النوع من المحتوى جريمة قائمة بذاتها، حتى في حال عدم استخدامه الفعلي في تنفيذ جريمة.

ثالثًا: العقوبات التكميلية والإدارية[٥٥]

- إغلاق المواقع والمنصات التي تستخدم لأغراض إرهابية.

- مصادرة الأدوات التقنية المستخدمة في الجريمة.

- إمكانية سحب الترخيص أو الإقامة إذا كان الجاني من غير المواطنين.

المطلب الثاني

القوانين الجنائية المتعلقة بالجرائم الإلكترونية في الدول الغربية

مع التطور المتسارع في تكنولوجيا المعلومات والاتصالات، ظهرت الجرائم الإلكترونية كأحد أبرز التحديات التي تواجه الأنظمة القانونية في الدول الغربية، سواء على مستوى الأمن الوطني أو الاستقرار الاجتماعي والاقتصادي. ولأن هذه الجرائم غالبًا ما تتسم بالتعقيد التقني، وعبر الحدود، فقد كان من الضروري أن تتبنى الدول الغربية أُطرًا تشريعية مرنة وفعالة تُمكِّنها من مواجهة هذه التهديدات بأسلوب يتماشى مع طبيعة الجريمة الرقمية.

وقد قامت العديد من هذه الدول بإصدار قوانين جنائية متخصصة أو بتعديل تشريعاتها القائمة، مثل قوانين العقوبات والإجراءات الجنائية، لاستيعاب صور جديدة من الجرائم مثل القرصنة، التجسس الإلكتروني، الاحتيال الرقمي، والإرهاب السيبراني. كما تبنّت تشريعاتها مبادئ جديدة تتعلق بالمسؤولية الجنائية للكيانات الاعتبارية، والاختصاص القضائي الدولي، وتبادل المعلومات عبر شبكات التعاون الأمني.

الفرع الأول : قانون مكافحة الإرهاب الأمريكي (The USA PATRIOT Act)

الفرع الثاني : قانون الجرائم الإلكترونية البريطاني (The Computer Misuse Act 1990)

الفرع الأول

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

قانون مكافحة الإرهاب الأمريكي (The USA PATRIOT Act)[٥٦]

يهدف هذا القانون إلى منح السلطات الأمريكية القدرة على مكافحة الإرهاب، بما في ذلك التهديدات الإلكترونية. ويتضمن القانون بنوداً تتعلق بتوسيع صلاحيات التحقيقات الإلكترونية، بما في ذلك مراقبة الاتصالات الإلكترونية، وتتبع الأنشطة الإرهابية عبر الإنترنت.

أولاً: تجريم تقديم الدعم المادي للمنظمات الإرهابية

يُجرّم هذا النص تقديم أي دعم مادي، مالي، تقني أو تكنولوجي لمنظمة إرهابية، سواء بشكل مباشر أو غير مباشر. ويشمل ذلك استخدام الإنترنت لتوفير خدمات مثل:

- التدريب التقني.
- خدمات الاستضافة أو النشر الإعلامي.
- تصميم أو إدارة المواقع الإلكترونية الإرهابية.

وتكون العقوبة السجن حتى 20 سنة، وقد تصل للمؤبد إذا نتج عنها وفاة.

ثانياً: تجريم استخدام نظم الاتصالات لأغراض إرهابية

- يجيز للجهات المختصة مراقبة الأنظمة والشبكات عندما يُستخدم أي نظام معلوماتي في ارتكاب جريمة إرهابية.
- يوسّع من مفهوم "الاعتراض المشروع" ليشمل مراقبة الاتصالات الخاصة بشبكات يُشتبه في استخدامها من قبل إرهابيين.

ثالثاً: تجريم التمويل الإلكتروني للإرهاب[٥٧]

- يُلزم المؤسسات المالية بالكشف عن التحويلات المشبوهة.
- يُجرّم استخدام الأدوات الرقمية مثل العملات المشفرة أو الحسابات الوهمية لتمويل الإرهاب.

الفرع الثاني

قانون الجرائم الإلكترونية البريطاني (The Computer Misuse Act 1990)[٥٨]

يُعد من أول القوانين التي وضعت إطاراً قانونياً لمكافحة الجرائم الإلكترونية في المملكة المتحدة. بينما لم يحدد هذا القانون الجرائم الإرهابية بشكل صريح، فإنه يُعاقب أي سلوك يُعرض الأنظمة المعلوماتية للخطر، بما في ذلك الجرائم ذات الصلة بالإرهاب. ورغم أن القانون لا يستخدم لفظ "الإرهاب" صراحة، إلا أنه يُستخدم كإطار قانوني لمحاسبة الأفراد أو الكيانات التي تستخدم الحواسيب أو الشبكات في الهجمات التخريبية.

وقد جرم هذا القانون كل الصور التي تساعد في جرائم الإرهاب الالكتروني علي النحو التالي :

أولاً : الوصول غير المصرح به إلى أنظمة الكمبيوتر[٥٩]

يُجرم الدخول إلى أي نظام معلوماتي بدون إذن. و يشمل ذلك الاستخدام غير القانوني لأجهزة الآخرين أو الشبكات.

وتكون العقوبة: الحبس حتى 12 شهراً أو غرامة، أو كليهما.[٦٠]

ثانياً : الوصول غير المصرح به بنيّة ارتكاب جريمة أخرى[٦١]

يُعاقب من يخترق الأنظمة بنية:

(سرقة بيانات، الابتزاز، التجسس أو أي جريمة جنائية أخرى) بعقوبة الحبس حتى 5 سنوات وغرامة مالية .

ثالثاً : التعديل غير المصرح به للمحتوى

تشمل(حذف أو تعديل البيانات. إطلاق فيروسات إلكترونية.تعطيل أو تشويش الخوادم أو البرامج.)

تكون العقوبة الحبس مدة تصل إلى 10 سنوات حبس، وتُضاعف إذا كان الفعل يُعرض الأمن القومي للخطر.

الخاتمة

ختاماً، يُعدّ الإرهاب الإلكتروني من أخطر التحديات التي تواجه الأمن القومي للدول في العصر الرقمي. لقد شهدت السنوات الأخيرة تزايداً ملحوظاً في استخدام الشبكات الإلكترونية من قبل الجماعات الإرهابية، ما استدعى تدخلاً عاجلاً من قبل التشريعات الوطنية والدولية لتأطير هذه الظاهرة. وعلى الرغم من أن العديد من الدول قد أدرجت الجرائم الإلكترونية الإرهابية ضمن قوانينها الجنائية، إلا أن التعامل مع هذه الجرائم لا يزال يواجه العديد من الصعوبات، سواء من حيث تحديد المسؤولية الجنائية أو التعاون الدولي.

وقد أظهرت هذه الدراسة أن التشريعات الوطنية في الدول العربية والغربية قد وضعت أسساً قانونية لمكافحة الإرهاب الإلكتروني، لكن هذه التشريعات بحاجة إلى تحديث مستمر لمواكبة التقدم التقني السريع.

في الختام، يُظهر البحث أن المواجهة الجنائية للإرهاب الإلكتروني بحاجة إلى إصلاحات قانونية شاملة، وتعزيز التعاون بين الدول، إلى جانب تطوير الأدوات التقنية لمكافحة هذا النوع من الجرائم. إن مواجهة الإرهاب الإلكتروني تتطلب تعاوناً من جميع الأطراف: السلطات القضائية، الجهات الأمنية، والمؤسسات التشريعية.

النتائج

توصل هذا البحث إلى مجموعة من النتائج المهمّة، أبرزها:

1. تنامي خطر الإرهاب الإلكتروني يمثل تهديداً حقيقياً للأمن القومي للدول، نظراً لاعتماده على تقنيات متقدمة، وقدرته

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

على تجاوز الحدود الجغرافية التقليدية بسهولة، دون الحاجة إلى وجود مادي على أرض الواقع.

2. الركن المادي لجريمة الإرهاب الإلكتروني يمكن أن يتحقق من خلال مجموعة متنوعة من الأفعال الإجرامية، كالتجسس، التهديد، التحريض، الاختراق، أو تعطيل البنى التحتية الرقمية، وتتم أغلبها عبر الوسائط الإلكترونية والشبكات.

3. الركن المعنوي لهذه الجريمة يتطلب توافر القصد الجنائي الخاص، ويتمثل غالبًا في نية إرهابية واضحة، مثل زعزعة الاستقرار، بث الرعب، أو الضغط السياسي على الدول أو المجتمعات.

4. صعوبة الإثبات تُعد من أبرز التحديات في مواجهة هذه الجرائم، نظرًا لاعتماد الجناة على تقنيات متطورة لإخفاء هويتهم، وتشفير اتصالاتهم، واستخدام شبكات مظلمة لا تخضع للرقابة.

5. تشريعات الدول العربية والغربية متباينة في معالجتها للإرهاب الإلكتروني؛ إذ تختلف في تعريف الجريمة، وتحديد الأركان، وتقدير العقوبة، مما يُضعف التنسيق الدولي لمكافحة هذا النوع من الإرهاب.

6. بالرغم من وجود قوانين مثل قانون مكافحة جرائم تقنية المعلومات المصري (2018) أو قانون مكافحة الجرائم الإلكترونية الإماراتي (2012)، إلا أن بعضها لا يزال يفتقر إلى نصوص صريحة تتناول الإرهاب الإلكتروني كجريمة قائمة بذاتها

التوصيات

1- تحديث التشريعات الوطنية:

ضرورة تحديث القوانين الجنائية في الدول العربية والغربية لتواكب التطورات التكنولوجية المتسارعة في مجال الجرائم الإلكترونية، بما يتماشى مع التحديات التي يفرضها الإرهاب الإلكتروني.

2- تعزيز التعاون الدولي:

يجب تطوير وتعزيز آليات التعاون الدولي في مكافحة الإرهاب الإلكتروني، من خلال اتفاقيات دولية مُلزمة وتفعيل دور منظمة الأمم المتحدة والشرطة الدولية (الإنتربول) في تسهيل تبادل المعلومات وتنسيق الجهود بين الدول.

3- التوسع في برامج التدريب:

ضرورة تنظيم برامج تدريبية للقضاة والمحامين والعاملين في الأجهزة الأمنية على التعامل مع الأدلة الرقمية، وفهم الطرق الحديثة للتحقيق في الجرائم الإلكترونية.

4- وضع ضوابط قانونية جديدة:

إنشاء إطار قانوني عالمي ينظم المسؤولية الجنائية للأفراد والكيانات في حال ارتكابهم للجرائم الإلكترونية الإرهابية، مع التركيز على حماية حقوق الأفراد وعدم المساس بحرية التعبير عبر الإنترنت.

5- الاستفادة من التقنيات الحديثة:

يجب على الدول الاستثمار في تقنيات الذكاء الاصطناعي وتحليل البيانات للكشف عن الأنشطة الإرهابية عبر الإنترنت، وتحسين القدرة على تحديد هوية المجرمين والمتورطين في هذه الجرائم.

قائمة المرجع

أولا : المراجع العربية :

[1] إيمان بن سالم – جريمة التجنيد الالكتروني للإرهاب وفقاً لقانون العقوبات الجزائري – ط 1 – المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية – برلين – المانيا 2018

[2] حسن بن أحمد والعسيري، محمد بن عبد الله آل فايع 2012 - الإرهاب الإلكتروني وبعضا من وسائله والطرق الحديثة لمكافحته، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5 / 2011 ، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض

[3] خالد حنفي علي – الانترنت وتصدير الارهاب – مجلة السياسه الدولية – السنه 41 – العدد 162 – اكتوبر 2005

[4] ذياب موسي البداينة – جرائم الحاسب الدولية – بحث مقدم الى أكاديمية نايف للعلوم الأمنية – الرياض – المملكة العربية . السعودية – ١٩٩٨

[5] صالح السدلان:اسباب الارهاب والعنف والتطرف- دار روز للطباعة-- الجزائر ١٩٩٩

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

[6] عادل عبدالصادق - الإرهاب الالكترونى القوة فى العلاقات الدولية: نمط جديد وتحديات مختلفة (القاهرة: -مركز الدراسات الاستراتيجية والسياسية 2009

[7] عبدالرحمن السند – وسائل الإرهاب الإلكتروني – حكمها في الإسلام وطرق مكافحتها – السجل العلمي لمؤتمر موقف الإسلام من الإرهاب – الجزء الأول – الرياض 2004 –

[8] عبدالفتاح بيومي حجازي- مكافحة جرائم الكمبيوتر والإنترنت- دار الفكر الجامعي- الإسكندرية

[9] عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية – دار الثقافة للطباعة والنشر – 1999

[10] عفيفي كامل عفيفي- جرائم الكمبيوتر وحق وق المؤلف والمصنفات الفنية ، دار الثقافة - للطباعة والنشر

[11] علي عدنان الفيل – الإجرام الالكتروني دراسة مقارنه – ط 1 – مكتبة زين الحقوقية – بيروت 2011

[12] علي عسيري - الإرهاب والانترنت - الطبعة الأولى - الرياض - 2006-

[13] مايا خاطر – الاطار القانوني لجريمة الارهاب الالكتروني – مجلة العلوم الاقتصادية والقانونية والادارية – المركز القومي للبحوث – دولة فلسطين – مايو 2018

[14] محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسوب الالكتروني ، دار الثقافة للطباعة والنشر

[15] محمد عبد الله منشاوي – جرائم الانترنت من منظور شرعي وقانوني – مطبعة جامعة الملك فهد – الرياض –. ١٤٢٣ هـ

[16] محمد كاسب خليفه المسافري – الإرهاب الالكتروني وسبل مواجهته – المجلة المغربية للإدارة المحلية والتنمية – العدد 150.151 – ابريل 2020

[17] محمود صالح العادلي –موسوعة القانون الجنائي للارهاب – دار الفكر الجامعي – الاسكندرية 2005

[18] موسى مسعود أرحومة- "الإرهاب والإنترنت"- مجلة جامعة الجلفة للدراسات والأبحاث- العدد 4 -2011

[19] نافع ابراهيم _كابوس الارهاب ،مركز الاهرام للترجمة والنشر_القاهرة ،1997

ثانيا : المراجع الأجنبية :

[1] Denning, Dorothy, Cyberterrorism, p 1, August 24, 2000-.

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

[3] For more details, see: Sarah Gordon, Richard Ford, Cyber Terrorism?, Symantec-

[4] Security Response, White paper, p. 4, at:

[5] https://www.symantec.com/avcenter/reference/cyberterrorism.pdf and see

[6] also, Barry C. Collins, The Future of Cyber Terrorism, Crime and Justice-

[7] International, March 1997, pp. 15-18.

[8] at:http://www.cjimagazine.com/archives/cji4c18.html?id=415.

[9] Lewis, A., James, “Assessing the Risks of Cyber Terrorism, Cyber War and-

[10] Other Cyber Threats”, Washington DC: Center for Strategic and

[11] International Studies, 2002, p. 1, at:

[12] https://csisprod.s3.amazonaws.com/s3fspublic/legacy_files/files/media/csis/pubs/0

[13] 21101risks of cyberterror.pdf.

[14] JomponPitaksantayothin, "Cyber Terrorism Laws in United States, the United-

[15] Kingdom and Thailand: A comparative study", March 2018, at:

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

[16] https://www.researchgate.net/publication/323748019 Cyber Terrorism Laws

[17] in the United States the United Kingdom and Thailand A Comparative

[18] KuboyeOluwafemi Samuel et al, International Journal of Computer Science-

[19] and Mobile Computing, Vol.3 Issue.5, May2014, p. 1084, at:

[20] https://ijcsmc.com/docs/papers/May2014/315201499b12.pdf.

[21] Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA.(Rising Cyber Threats Pose Serious Concerns for Financial Stability

[22] https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[23] Gabriel Weimann, Cyber Terrorism: How Real is the Threat?, United States-

[24] Institute of Peace, Special Report, December 2004, pp. 2-6, at:

[25] https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat

[26] UNODC, The Use of the Internet for Terrorist Purposes, 2012

الهوامش

[1] د : محمد عبد الله منشاوي – جرائم الانترنت من منظور شرعي وقانوني – مطبعة جامعة الملك فهد – الرياض – ١٤٢٣ هـ – ص11 .

[2] د : ذياب موسي البداينة – جرائم الحاسب الدولية – بحث مقدم الى أكاديمية نايف للعلوم الأمنية – الرياض – المملكة العربية السعودية – ١٩٩٨ – ص ٢ .

[3] د : علي عدنان الفيل – الإجرام الالكتروني دراسة مقارنه – ط 1 – مكتبة زين الحقوقية – بيروت 2011– ص 6

[4] عادل عبدالصادق - الإرهاب الالكترونى القوة فى العلاقات الدولية: نمط جديد وتحديات مختلفة (القاهرة: -مركز الدراسات الاستراتيجية والسياسية 2009)-٣٧ .

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

[6] - For more details, see: Sarah Gordon, Richard Ford, Cyber Terrorism?, Symantec Security Response, White paper, p. 4, at:
https://www.symantec.com/avcenter/reference/cyberterrorism.pdf and see also, Barry C. Collins, The Future of Cyber Terrorism, Crime and Justice International, March 1997, pp. 15-18.
at:http://www.cjimagazine.com/archives/cji4c18.html?id=415.

[7] - Lewis, A., James, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Washington DC: Center for Strategic and International Studies, 2002, p. 1, at:
https://csisprod.s3.amazonaws.com/s3fspublic/legacy_files/files/media/csis/pubs/021101 risks of cyberterror.pdf.

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

[8] د: مايا خاطر – الاطار القانوني لجريمة الارهاب الالكتروني – مجلة العلوم الاقتصادية والقانونية والادارية – المركز القومي للبحوث – دولة فلسطين – مايو 2018 – ص 58

[9] المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

[10] مايا خاطر – مرجع سابق – ص 59

[11] 1. نافع ابراهيم _كابوس الارهاب ،مركز الاهرام للترجمة والنشر_القاهرة ،1997_ص198.

[12] حسن بن أحمد والعسيري، محمد بن عبد الله آل فايع 2012 - الإرهاب الإلكتروني وبعضا من وسائله والطرق الحديثة لمكافحته، ندوة: استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين المقامة في الرياض من 9 إلى 11 / 5 / 2011 ، منشورات جامعة نايف العربية للعلوم الأمنية، الرياض، ص 225

[13] - JomponPitaksantayothin, "Cyber Terrorism Laws in United States, the United Kingdom and Thailand: A comparative study", March 2018, at: https://www.researchgate.net/publication/323748019 Cyber Terrorism Laws in the United States the United Kingdom and Thailand A Comparative Study/citations

[14] د : خالد حنفي علي – الانترنت وتصدير الارهاب – مجلة السياسه الدولية – السنه 41 – العدد 162 – اكتوبر 2005

[15] د : موسى مسعود أرحومة- "الإرهاب والإنترنت"- مجلة جامعة الجلفة للدراسات والأبحاث- العدد 4 -2011 ص 16

[16] د : عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية – دار الثقافة للطباعة والنشر – 1999 ص 83

[17] - KuboyeOluwafemi Samuel et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May2014, p. 1084, at: https://ijcsmc.com/docs/papers/May2014/315201499b12.pdf.

[18] ▪ مثال: في عام 2021، تعرّضت وزارة الصحة في أيرلندا لهجوم فدية إلكتروني (Ransomware) أدى إلى شلل في النظام الصحي، مما كشف هشاشة البنية الإلكترونية.

[19] د : صلاح الفتلاوي – جريمة الارهاب الالكتروني – دون تاريخ نشر او دار نشر – ص 55

[20] (Europol. (2022). Internet Organised Crime Threat Assessment (IOCTA.

[21] وقد أوضح تقرير صادر عن مركز الدراسات الإستراتيجية والدولية (CSIS) عام 2022 أن الجماعات المتطرفة، مثل "القاعدة" و"داعش"، لجأت إلى شن هجمات إلكترونية على بنوك وشركات مالية، بهدف سرقة الأموال واستخدامها في تمويل أنشطتها، مستغلة ضعف الرقابة المالية الإلكترونية في بعض المناطق.

[22] Rising Cyber Threats Pose Serious Concerns for Financial Stability - https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[23] متاح علي الرابط التالي - Cyber attacks on critical infrastructure - https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html? - تم الدخول في 15 ابريل 2025

[24] د : عاطف عبدالفتاح – البطالة في العالم العربي وعلاقتها بالجريمة – المركز العربي للدراسات الأمنية والتدريب – الرياض – 1986 – ص 35 ، 36

[25] - Gabriel Weimann, Cyber Terrorism: How Real is the Threat?, United States Institute of Peace, Special Report, December 2004, pp. 2-6, at: https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 . https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

[26] وأفاد تقرير الشرطة الأوروبية (Europol, 2022) أن "الإرهابيين يستخدمون الإنترنت بشكل متزايد للتخطيط والتنسيق لعملياتهم، مما يجعل من الصعب على الأجهزة الأمنية اكتشاف هذه الأنشطة قبل تنفيذها، وهو ما يعرقل فعالية مكافحة الإرهاب الإلكتروني"

[27] كما أشار تقرير منتدى الاقتصاد العالمي (WEF) حول التهديدات السيبرانية العالمية لعام 2024 إلى أن "الافتقار إلى الرقابة الدولية الموحدة على الإنترنت يجعل من الصعب على الحكومات تتبع الأنشطة الإرهابية أو حظرها، ما يفتح الباب أمام استغلال هذه الثغرات من قبل جماعات منظمة

[28] د : عبدالرحمن السند – وسائل الإرهاب الإلكتروني – حكمها في الإسلام وطرق مكافحتها – السجل العلمي لمؤتمر موقف الإسلام من الإرهاب – الجزء الأول – الرياض 2004 – ص 224

[29] المصدر السابق ص 225

[30] المادة الأولي من القانون رقم 157 لسنة 2018

[31] محمد كاسب خليفه المسافري – الإرهاب الالكتروني وسبل مواجهته – المجلة المغربية للإدارة المحلية والتنمية – العدد 150.151 – ابريل 2020 – ص 382

[32] د:صالح السدلان:اسباب الارهاب والعنف والتطرف- دار روز للطباعة-- الجزائر ١٩٩٩ _ص ٩

[33] د : صلاح الفتلاوي – مرجع سبق ذكره – ص 23

[34] د : عبدالرحمن السند – مرجع سابق – ص 224

[35] د : علي عسيري - الإرهاب والانترنت - الطبعة الأولى - الرياض - 2006- ص 63

[36] إيمان بن سالم – جريمة التجنيد الالكتروني للإرهاب وفقاً لقانون العقوبات الجزائري – ط 1 – المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية – برلين – المانيا 2018 – ص 37

[37] د : عبدالرحمن السند – مرجع سبق ذكره – ص 225 – دكتور : محمود صالح العادلي –موسوعة القانون الجنائي للارهاب – دار الفكر الجامعي – الاسكندرية 2005 – ص 183

[38] المرجع السابق – ص 225

[39] د : محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسوب الالكتروني ، دار الثقافة للطباعة والنشر – ص 53

[40] د : عبدالرحمن السند – مرجع سابق – ص 225

[41] د : مايا خاطر – مرجع سابق – ص 60

[42] محمد كاسب خليفه المسافري – مرجع سابق – ص 384 - 385

[43] د : عفيفي كامل عفيفي- جرائم الكمبيوتر وحق وق المؤلف والمصنفات الفنية ، دار الثقافة - للطباعة والنشر – ص 107

[44] د : صلاح الفتلاوي – مرجع سابق – ص28

[45] كما أوضح تقرير صادر عن المنتدى العالمي لمكافحة الإرهاب (GCTF) أن "الرسائل التحريضية والمرعبة التي تُنشر إلكترونياً تمثل تهديداً متصاعداً، خاصة مع انتشار منصات التواصل الاجتماعي التي تُستخدم لتخويف فئات مجتمعية معينة أو بث الكراهية، مما يجعلها أداة فعّالة في يد الجماعات المتطرفة"- متاح علي الموقع التالي https://www.thegctf.org/ تم الدخول في2 ابريل 2025

[46] تقرير ورقة العمل التابعة للأمم المتحدة بتنفيذ تدابير مكافحة الارهاب – استخدام الانترنت في أغراض ارهابية – قسم اللغة الانجليزية والمنشورات المكتبية – مكتب الأمم المتحدة في فينيا – حزيران 2013

[47] د : عبدالفتاح بيومي حجازي- مكافحة جرائم الكمبيوتر والإنترنت- دار الفكر الجامعي- الإسكندرية- ص ١١٤

[48] المرجع السابق – ص 113

[49] وقد أكّدت دراسة للأمم المتحدة بشأن استخدام الإنترنت في الإرهاب أن "الجماعات الإرهابية تعتمد بشكل متزايد على سلوكيات إيجابية كالنشر والتخطيط، وأحياناً على الامتناع المتعمد عن حذف المحتوى أو إبلاغ السلطات، مما يُعزز من فرص انتشار الأيديولوجيا المتطرفة"

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 . https://doi.org/10.36371/port.2025.3.8

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 8, issue 3. 2025

.(UNODC, The Use of the Internet for Terrorist Purposes, 2012)

[50] مادة 33 من قانون مكافحة الارهاب المصري لسنة 2015

[51] وقد أكدت دراسة للشرطة الفيدرالية الأمريكية (FBI) أن "التهديدات الإلكترونية الإرهابية تزداد تعقيداً نظرًا لاستخدام أساليب متقدمة تُصعب إثبات علاقة السببية بين الفعل والنتيجة، مما يفرض تحديات قانونية خاصة في التحقيقات"

[52] المادة 28 - من قانون مكافحة جرئم تقنية المعلومات المصري

[53] قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018

[54] صدر القانون في عام 2012 في دولة الإمارات العربية المتحدة تحت عنوان "قانون مكافحة جرائم تقنية المعلومات"، ويهدف إلى مواجهة كافة أشكال إساءة استخدام الوسائل الإلكترونية، وخاصة تلك التي تهدد الأمن القومي والسلم العام، أو تُستخدم لأغراض إرهابية أو تخريبية.

[55] قانون مكافحة جرائم تقنية المعلومات - دولة الإمارات

[56] صدر هذا القانون في أعقاب هجمات 11 سبتمبر 2001، ويُعرف رسميًا باسم:
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism "Act of 2001"
ويُختصر إلى: USA PATRIOT Act.

[57] U.S. Code Title 18 - Crimes and Criminal Procedure

[58] صدر هذا القانون في المملكة المتحدة عام 1990، ويُعد من أوائل القوانين في العالم التي تناولت الجرائم الإلكترونية بشكل صريح. وقد جاء كردّ فعل على تصاعد حوادث الاختراق والقرصنة الإلكترونية في الثمانينيات، وتم تعديله عدة مرات لاحقًا، خصوصًا لمواكبة تطور الجريمة السيبرانية.

[59] المادة 1 من القانون السابق

[60] (تُرفع العقوبة في القضايا الجسيمة إلى الحبس حتى سنتين بعد التعديلات اللاحقة).

[61] المادة 2

S. A. Shehata. 2025, Criminal Confrontation with Cyber Terrorism: (A Comparative Analytical Study). *Journal port Science Research*, 8(3), pp.300 -321 .
https://doi.org/10.36371/port.2025.3.8