

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

Cyberterrorism : A New Tool in the Hands of Terrorist Organizations

ملياني عبد الوهاب

جامعة عمار ثليجي-الاعواط-الجزائر

مخبر بحث الحقوق والعلوم السياسية

Abdel.meliani@lagh-univ.dz

هاشمي رشيدة*

جامعة عمار ثليجي-الاعواط-الجزائر

مخبر بحث الحقوق والعلوم السياسية

r.hachemi@lagh-univ.dz

تاريخ نشر المقال: 2025/03/20

تاريخ قبول المقال: 02/03/2025

تاريخ إرسال المقال: 2025/03/01

الملخص:

تهدف هذه الدراسة إلى إلقاء الضوء على الإرهاب الإلكتروني باعتباره ظاهرة خطيرة تهدد سلامة الأفراد والجماعات وأمنهم مما يجعله من أهم المواضيع التي تستدعي اهتماما فوريا، من خلال التعرف على الإرهاب الإلكتروني وخصائصه، مروراً بدوافع ممارسته وأشكاله المختلفة، وصولاً إلى استراتيجيات الوقاية من هذه الظاهرة.

الكلمات المفتاحية: الإرهاب، التنظيمات الإرهابية، أسباب الإرهاب الإلكتروني، أشكال الإرهاب

الإلكتروني

Abstract:

This study aims to shed light on the phenomenon of cyberterrorism as a serious threat to the safety, security, and well-being of individuals and communities, making it a subject that demands immediate attention. By exploring the concept of cyberterrorism, its characteristics, motivations, and various forms, this study seeks to contribute to the development of effective strategies for preventing and mitigating this threat.

Keywords: terrorism, terrorist organizations, motivations for cyberterrorism, forms of cyberterrorism

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

المقدمة:

مع ظهور الثورة الرقمية وازدياد التطور التكنولوجي بشكل متسارع ظهر شكل جديد من الارهاب يعتمد على الوسائل التكنولوجية الرقمية والانترنت، فتغير بذلك وجه الإرهاب بشكل جذري من الإرهاب التقليدي الى الإرهاب في الفضاء الإلكتروني مشكلا ظاهرة خطيرة تهدد أمن الدول والمجتمعات، حيث سهلت التكنولوجيا الرقمية ارتكاب الأعمال الإرهابية من أي مكان وزمان، وأضحت الجماعات الإرهابية تستخدم تقنيات حديثة لإدارة عملياتها والتواصل فيما بينها وتجنيد الأعضاء الجدد وجمع الأموال بل وتحولت هجماتها من الفضاء العادي الى الفضاء الإلكتروني من خلال إنشاء المواقع الإلكترونية واختراقها، ونشر برامج التجسس وبرامج تدمير المواقع والنظم والمعلومات.

تأتي أهمية دراسة هذا الموضوع نظرا لازدياد عدد المواقع الإلكترونية التي تديرها المنظمات الإرهابية على الإنترنت، مما يسهل انتشار المعلومات والأفكار المتطرفة بين مختلف فئات المجتمع، ويزيد من صعوبة تتبع الأنشطة الإرهابية عبر الإنترنت، لذلك من الضروري دراسة الإرهاب الإلكتروني للتعرف على مفهومه وأسباب انتشاره وكذا تحليل مظاهره وتقديم حلول للوقاية منه.

وتثير هذه الدراسة تساؤلات جوهرية حول تأثير الثورة الرقمية على طبيعة التهديدات الإرهابية التي أدت الى التحول من العنف المادي إلى العنف الافتراضي والحلول الكفيلة لمواجهة هذه الظاهرة؟

للإجابة على الإشكالية المطروحة اعتمدنا في دراستنا على المنهج الوصفي التحليلي من خلال استعراض تعاريف الإرهاب الإلكتروني وخصائصه، ومن ثم تحليل الأسباب التي ساهمت في انتشار هذه الظاهرة ومن ثم إبراز اشكال وسبل الوقاية من الإرهاب الإلكتروني، وقصد إضفاء موضوع الدراسة الى المقصود، ارتأينا تقسيم هذه الدراسة الى بحثين، نتناول في المبحث الأول مفهوم الإرهاب الإلكتروني واسبابه، ومن ثم تسليط الضوء بموجب المبحث الثاني على مظاهر الإرهاب الإلكتروني وسبل الوقاية منه.

المبحث الأول: تحليل أسباب التحول من الإرهاب المادي الى الإرهاب الإلكتروني

يعد الإرهاب الإلكتروني ظاهرة حديثة تعتمد على استخدام التكنولوجيا الرقمية والانترنت لنشر الخوف والتهديد، لتحقيق أهداف سياسية أو دينية أو أيديولوجية مما يشكل تهديدا متزايدا للبنى التحتية والأنظمة الإلكترونية وزعزعة للاستقرار السياسي والاقتصادي والاجتماعي.

بناءا على ما سبق قسمنا المبحث الى مطلبين تناولنا في المطلب الأول مفهوم الإرهاب الإلكتروني، ثم ستم دراسة أسباب الإرهاب الإلكتروني بمقتضى المطلب الثاني.

المطلب الأول: تحديد مفهوم الإرهاب الإلكتروني

من خلال هذا المطلب سيتم التطرق الى تعريف الإرهاب الإلكتروني بمقتضى الفرع الأول، ثم خصائص الإرهاب الإلكتروني بموجب الفرع الثاني

الفرع الأول: تعريف الإرهاب الإلكتروني

عرفته اللجنة الدولية للصليب الأحمر على انه استخدام تقنيات المعلومات والاتصالات لشن هجمات على أنظمة الحاسوب والشبكات، من خلال اختراق النظام المعلوماتي او جمع او نقل او تشفير او تغيير البيانات او التلاعب بها بهدف احداث اضرار او تعطيل أو تدمير البنى التحتية الحيوية او الخدمات الأساسية او البيانات¹.

اما مكتب التحقيقات الفيدرالية الأمريكي FBI يعرفه على انه استخدام القوة او العنف بشكل غير قانوني من قبل جماعة او جماعات، ضد الأشخاص او الممتلكات بهدف تخويف الحكومة او السكان المدنيين او فئة معينة والزامهم بتحقيق اهداف سياسية او اجتماعية محددة لمصلحة الجماعة مرتكبة العنف².

¹ سعيد غريب المزروعى، الإرهاب الرقمي من منظور جنائي (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2022، ص22

² هالة احمد الرشيدى، الإرهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2021، ص24.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

ومن جانب آخر عرفت وزارة الدفاع الأمريكية الإرهاب الإلكتروني بأنه هجمات أو تهديدات تستهدف الأنظمة الحاسوبية، بهدف ترهيب أو فرض السيطرة على الحكومات أو المجتمعات سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، ولا بد أن يكون الهجوم كافياً لإحداث الخوف مقارنة بالتأثير الذي تسبب فيه الأشكال الأخرى المادية للإرهاب.³

أما التعريفات الفقهية نذكر منها تعريف Barry C. Colin الباحث في معهد الامن والاستخبارات في كاليفورنيا وهو أول من استعمل مصطلح الإرهاب السيبراني في ثمانينات القرن الماضي⁴ وعرفه على أنه هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب.⁵

أما Pollitt فقد جمع بين تعريف Collin وتعريف وزارة الخارجية الأمريكية فعرّف الإرهاب السيبراني على أنه هجوم متعمد، ذو دوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات، التي تؤدي إلى أعمال عنف ضد أهداف غير مقاتلة من قبل مجموعات دون وطنية أو عملاء سريين.⁶

كما عرف James Lewis الإرهاب الإلكتروني بأنه: استخدام أدوات شبكة الكمبيوتر لتدمير أو تعطيل البنى التحتية الوطنية الحيوية مثل الطاقة والنقل والعمليات الحكومية، أو لإكراه أو ترهيب حكومة ما أو سكان مدنيين.⁷

أما Keith Lourdeau بصفته نائب مساعد مدير لقسم الجرائم الإلكترونية بمكتب التحقيقات الفيدرالي الأمريكي خلال جلسة استماع أمام اللجنة الفرعية القضائية بمجلس الشيوخ المعنية بالإرهاب

³ هالة احمد الرشيدى، المرجع نفسه

⁴ Mohammad iqbal, Defining Cyberterrorism, UIC John Marshall Journal of Information technology & privacy law, vol 22, issue 2, winter 2004, pg 402.k

⁵ ولد يوسف مولود، الإرهاب الإلكتروني والطرق الحديثة لتكوين التنظيمات الجهادية عبر شبكة الانترنت، مجلة الدراسات القانونية، المجلد 03، العدد 02، الجزائر، ص04.

⁶ Maura Conway, Cyberterrorism :Hype and Reality, pg06
<https://doras.dcu.ie>

⁷ James A.Lewis, Assessing the Risks of Cyber Terrorism Cyber war and Other Cyber Threats, center for strategic and international studies, december 2002 ،
<https://www.steptoe.com>

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

والتكنولوجيا وأمن الوطن، حيث ذكر أن الإرهاب الإلكتروني بأنه عمل إجرامي يتم ارتكابه باستخدام أجهزة الكمبيوتر وقدرات الاتصالات السلكية واللاسلكية، مما يؤدي إلى العنف والدمار و / أو تعطيل الخدمات، بهدف زرع الخوف والارتباك وعدم اليقين بين أفراد المجتمع، من أجل التأثير على الحكومة أو مجموعة سكانية معينة لدفعها نحو تبني توجهات سياسية أو اجتماعية أو إيديولوجية معينة.⁸

من خلال التعريفات السابقة يمكننا القول بأن الإرهاب الإلكتروني هو استخدام التكنولوجيا الرقمية والشبكات الحاسوبية في تنفيذ هجمات أو تهديدات مادية أو معنوية ضد الأفراد أو المنظمات أو الدول لدوافع سياسية أو دينية أو إيديولوجية.

الفرع الثاني: خصائص الإرهاب الإلكتروني

من خلال التعاريف السابقة يتبين لنا أن الإرهاب الإلكتروني يتميز بمجموعة من الخصائص التي تميزه عن غيره من الجرائم لاسيما الارهاب التقليدي.

أولاً: الإرهاب الإلكتروني جريمة عابرة للحدود

تتميز جريمة الإرهاب الإلكتروني بالطابع العابر للحدود، حيث يمكن التخطيط للجريمة في دولة ما، وتمويلها في دولة أخرى، وتنفيذها في دولة ثالثة⁹، وذلك باستخدام شبكة الانترنت التي أصبحت تسهل عملية التواصل والتخطيط والتنفيذ لجريمة الإرهاب الإلكتروني من أي مكان في العالم.

ثانياً: الإرهاب الإلكتروني جريمة ناعمة

تطلق تسمية الجرائم الناعمة على مجموعة الجرائم التي لا تتطلب اللجوء الى العنف والقوة ومن بينها جريمة الإرهاب الإلكتروني، فهذه الأخيرة تعتمد على استخدام أدوات الكترونية اذ يعد الحاسب الالى وشبكة الانترنت الأداة الرئيسية لارتكابها،¹⁰ فكل ما يحتاجه الإرهابي هو جهاز كمبيوتر شخصي

⁸Fabio Cristiano-Dennis Broeders- daan weggemans, cyber terrorism and human rights from the national to the international, and back?, The Hague Program for Cyber Norms Faculty of Governance and Global Affairs Leiden University, 2020, pg 7 .

⁹ هالة احمد الرشيدى، المرجع السابق، ص 28.

¹⁰ ايمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقاً لقانون العقوبات الجزائري، الطبعة الأولى، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، ألمانيا، 2018، ص 14.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

والاتصال بالإنترنت فلا يحتاج الإرهابيون إلى شراء أسلحة مثل البنادق والمتفجرات، بدلاً من ذلك يمكنهم إنشاء فيروسات كمبيوتر ونشرها عبر خط الهاتف أو الكابل أو الاتصال اللاسلكي.¹¹

ثالثاً: الإرهاب الإلكتروني جريمة صعبة الاكتشاف

تعد جريمة الإرهاب الإلكتروني من الجرائم صعبة الاكتشاف وذلك لسهولة إخفاء الجاني للدليل المادي وهويته وموقعه من جهة، وافتقار بعض الأجهزة الأمنية والفضائية إلى الخبرة والمهارات اللازمة للتعامل مع هذا النوع من الجرائم.¹²

رابعاً: الإرهاب الإلكتروني جريمة صعبة الإثبات

ان غياب الدليل المادي الملموس في جريمة الإرهاب الإلكتروني يجعل من هذه الأخيرة جريمة صعبة الإثبات، ذلك كون جريمة الإرهاب الإلكتروني لا تخلف عادة أدلة مادية ملموسة، وإنما تكون هذه الأدلة على شكل بيانات رقمية يسهل على المجرمين إخفاؤها أو التخلص منها.¹³

المطلب الثاني: أسباب الإرهاب الإلكتروني

لقد تنوعت أسباب ودوافع الإرهاب لجوء التنظيمات الإرهابية إلى استعمال الفضاء الإلكتروني في العمليات الإرهابية، وفهم هذه الأسباب ضروري لوضع استراتيجيات فعالة للوقاية من الإرهاب الإلكتروني ومكافحته.

من خلال هذا المطلب سنتطرق إلى الأسباب العامة للإرهاب الإلكتروني بمقتضى الفرع الأول، ثم الأسباب الخاصة للإرهاب الإلكتروني بمقتضى الفرع الثاني.

الفرع الأول: الأسباب العامة

سنتناول بموجب هذا الفرع الأسباب العامة للإرهاب الإلكتروني

¹¹Gabriel Weimann, Cyberterrorism How Real Is the Threat, United States Institute of Peace, 2004, pg 06

[United States Institute of Peace \(usip.org\)](https://www.usip.org/)

¹² حسنين شفيق، الاعلام الجديد والجرائم الإلكترونية، دار فكر وفن للطباعة والنشر والتوزيع، 2015، ص 190.

¹³ عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي، منشورات الحلبي الحقوقية، لبنان،

2020، ص70.

أولاً: الدوافع الشخصية

تتعدد الأسباب الشخصية التي تدفع الأفراد الى ارتكاب الإرهاب الإلكتروني، فقد يسعى البعض الى ارتكاب هذه الجريمة لجذب الانتباه والحصول على الشهرة، او للتعبير عن غضبهم او احباطهم من ظروف معينة، كما قد يكون الدافع الى ارتكاب جريمة الإرهاب الإلكتروني ناتج عن فشل الشخص في الحياة الاسرية والشعور بالوحدة او العزلة عن المجتمع.¹⁴

ثانياً: الدوافع النفسية

تتضافر العديد من العوامل النفسية المؤدية الى ارتكاب جريمة الإرهاب الإلكتروني فمن بينها نجد¹⁵:

- نشر محتوى العنف والعمليات الإرهابية عبر وسائل التكنولوجيا الحديثة مما يؤثر على سلوك بعض الأشخاص ذوي النفوس الضعيفة والغريزة العدوانية،
- معاناة الشباب من نقص فرص العمل وتدهور الأوضاع الاقتصادية والاجتماعية، مما ينمي مشاعر الإحباط والغضب في نفوسهم، الامر الذي يجعلهم فريسة سهلة للجماعات الإرهابية،
- غياب التربية الأخلاقية وانتشار الأفكار والقيم الجديدة عبر مختلف وسائل الاعلام والتواصل الاجتماعي مما يساهم في جعل الشباب عرضة للتأثيرات الخارجية إذا لم يتم تحصينهم بقيم أخلاقية راسخة،
- الصراع بين الأجيال الذي يفضي إلى خلق شعور بالانعزال والرفض لدى الشباب، مما يشجعهم على البحث عن مجموعات تقدم لهم الشعور بالانتماء، فتستغل الجماعات الإرهابية هذه العوامل لتجنيد الشباب في صفوفها مستخدمة أساليباً مختلفة للتأثير على عقول الشباب وعواطفهم.

ثالثاً: الدوافع السياسية

¹⁴ مصطفى يوسف كافي، ماهر عودة الشمايلية، محمود عزت اللحام، الاعلام والإرهاب الإلكتروني، دار الاعصار العلمي للنشر والتوزيع، الأردن، 2015، ص149
¹⁵ عبد الجليل إسماعيل حسن الشيخ زيني، المرجع السابق، ص 89-90.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

تنشأ ظاهرة الإرهاب الإلكتروني نتيجة عدة عوامل سياسية قد تكون داخلية أو خارجية، من ضمن العوامل الداخلية نجد:¹⁶

- السياسات غير العادلة للدول التي تهتمش دور المواطنين تنتهك حقوقهم،
- عدم تلبية متطلبات التوازن الاجتماعي وغياب دور مؤسسات المجتمع المدني،
- الإحباط السياسي في بعض البلدان العربية والإسلامية واجهت الجماعات الإسلامية التهميش والقمع، مما أدى إلى تجميد عطاءها وظهور ردود أفعال غاضبة قد تتجه نحو الإرهاب،
- غياب العدالة الاجتماعية مما أدى الى عدم المساواة في توزيع الثروة الوطنية والخدمات والمرافق الأساسية والاستيلاء على الأموال العامة وانعدام التنمية المستدامة.

اما العوامل الخارجية نجد من بينها¹⁷:

- ظلم بعض الشعوب واضطهادها والسيطرة الاستعمارية،
- انتهاك حقوق الإنسان والقوانين والمواثيق الدولية،
- غياب عقوبات دولية شاملة وراذعة على الدول التي المنتهكة لحقوق الانسان.

رابعاً: الدوافع الاقتصادية

من أبرز الدوافع الاقتصادية للإرهاب الإلكتروني¹⁸:

- الأزمات الاقتصادية والمتغيرات الاقتصادية العالمية والاستغلال غير المشروع للموارد الاقتصادية،

¹⁶ اسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني -دراسة مقارنة-، مذكرة نيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق، 2016، ص 32-33.

¹⁷ اسراء طارق جواد كاظم الجابري، المرجع نفسه.

¹⁸ مصطفى يوسف كافي، جرائم الفساد غسل الأموال السياحة الإرهاب الإلكتروني المعلوماتية، مكتبة المجتمع العربي، عمان، 2014، ص 145-146.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

- ضعف التعاون الدولي في معالجة وإيجاد الحلول للمشاكل الاقتصادية العالمية،
- معاناة الأفراد من المشاكل الاقتصادية، مثل الفقر وغلاء المعيشة وانخفاض دخل الأفراد وكذا انتشار البطالة وقلة فرص العمل، مما يجعلهم عرضة للتجنيد من قبل الجماعات الإرهابية.
- استغلال التنظيمات الإرهابية للتقدم التقني للأنظمة المصرفية العالمية في تمويل أنشطتها غير المشروعة عن طريق تحويل الأموال بين جميع أرجاء العالم.

خامسا: الدوافع الاجتماعية

تشكل الأوضاع الاجتماعية المتردية بيئة خصبة لنمو الإرهاب الإلكتروني مما يساهم في دفع الأفراد نحو التطرف، فمن أبرز الدوافع الاجتماعية لهذه الظاهرة نجد¹⁹:

- النقص الأسري وغياب التربية الحسنة،
- فقدان الهوية المجتمعية والعقيدة الصحيحة للمجتمع،
- غياب دور العلماء في النصيح والإرشاد والتوجيه،
- الفراغ النفسي والروحي والعقلي والزمني والتأثر بالأصدقاء السيئين.

سادسا: الدوافع الفكرية

- هناك عدة دوافع فكرية تساهم في ظهور الإرهاب الإلكتروني من بينها²⁰:
- الفراغ الفكري الذي يجعل صاحبه غير قادر على التمييز بين الأفكار الصحيحة والخاطئة، مما يجعله عرضة للتأثر بالأفكار المتطرفة،
 - الجهل بمقاصد الشريعة الإسلامية وقواعد الدين مما يؤدي إلى تفسيرها بشكل خاطئ،

¹⁹ عبد الجليل إسماعيل حسن الشيخ زيني، المرجع السابق، ص 85-86.

²⁰ اسراء طارق جواد الجابري، المرجع السابق، ص 31-32.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

● التشدد والغلو في الفكر، والانقسامات الفكرية بين التيارات المتنوعة والأحزاب المختلفة مما يساعد على خلق بيئة للإرهاب الإلكتروني.

الفرع الثاني: الأسباب الخاصة للإرهاب الإلكتروني

سنتناول بموجب هذا الفرع الأسباب الخاصة للإرهاب الإلكتروني

أولاً: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق

تشكل ثغرات شبكات المعلومات بيئة مناسبة للمنظمات الإرهابية، حيث تمكنها من التسلل إلى البنى المعلوماتية التحتية وممارسة العمليات التخريبية والإرهابية، لذلك من المهم اتخاذ الخطوات اللازمة لتأمين شبكات المعلومات من مخاطر الإرهاب عن طريق تعزيز الأنظمة الأمنية وتحديثها باستمرار، وكذا نشر الوعي لدى المستخدمين حول مخاطر الإرهاب الإلكتروني وطرق الوقاية منه، ومحاربة البرامج الضارة، وحماية المعلومات الحساسة وتشفيرها.²¹

ثانياً: سهولة استخدام شبكة المعلومات وقلة التكاليف

يتزايد انتشار الإرهاب الإلكتروني بسبب سهولة استخدام شبكة المعلومات من جهة وعدم الحاجة إلى مصادر تمويل كبيرة من جهة أخرى، فمن خلال شبكة المعلومات استطاعت المنظمات الإرهابية تحقيق أهدافها من خلال الوصول إلى عدد كبير من الجمهور بسهولة وفي وقت قصير، واستغلال أدوات الانترنت لنشر الدعاية الإرهابية واستغلال تقنيات التشفير لإخفاء هويتها وحماية اتصالاتها.²²

ثالثاً: غياب الحدود الجغرافية وتدني مستوى المخاطرة

ان غياب الحدود المكانية سهل على الإرهابيين الإلكترونيين شن هجمات إلكترونية من أي مكان في العالم دون مخاطرة مباشرة فهم لا يواجهون أي خطر مباشر عند تنفيذ هجماتهم الإلكترونية عكس

²¹ مصطفى يوسف كافي، ماهر عودة الشمالية، محمود عزت اللحام، المرجع السابق، ص 151.

²² مصطفى يوسف كافي، ماهر عودة الشمالية، محمود عزت اللحام، المرجع نفسه.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

الإرهاب التقليدي، ضف الى ذلك عدم وضوح الهوية الرقمية للمستخدم مما مكن الإرهابيين الإلكترونيين من التخفي وراء أسماء مستعارة.²³

رابعاً: صعوبة اكتشاف وإثبات جريمة الإرهاب الإلكتروني

تشكل سهولة إتلاف الأدلة الرقمية، وصعوبة السيطرة على المعلومات والاتصالات عبر الإنترنت، بيئة مثالية للإرهاب الإلكتروني، فالإرهابيون يستغلون هذه العوامل للتخفي وشن هجمات دون خوف من رصدهم من قبل الأجهزة الأمنية.²⁴

خامساً: الفراغ القانوني والتنظيمي وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية

يشكل الفراغ التنظيمي والقانوني في بعض الدول سببا رئيسيا في انتشار الإرهاب الإلكتروني، فغياب القوانين المجرمة بشكل متكامل سهل على المجرمين التنقل بين الدول دون خوف من الملاحقة القانونية، إضافة الى ذلك يعد غياب جهة مركزية تسيطر على محتوى الإنترنت وتراقب مداخله ومخارجه عاملا هاما في تقشي ظاهرة الإرهاب الإلكتروني، فسهولة الوصول إلى الإنترنت ونشر أي محتوى دون قيود يتيح للإرهابيين نشر أفكارهم المتطرفة والتجنيد وجمع الأموال بسهولة.²⁵

المبحث الثاني: مظاهر الإرهاب الإلكتروني وسبل الوقاية منه

يشكل الإرهاب الإلكتروني خطرا داهما يهدد أمننا واستقرارنا، حيث تتجلى خطورته في تنوع أشكاله ومظاهره بشكل هائل، من هجمات تقنية تعطل الخدمات الإلكترونية، إلى هجمات معلوماتية تسرق البيانات، وكذا هجمات نفسية تنشر الخوف والتهديد في نفوس الافراد، حيث تستهدف هذه الهجمات مختلف شرائح المجتمع، بدءاً من الأفراد الذين قد تسرق بياناتهم الشخصية أو المالية، إلى المؤسسات التي قد تعطل خدماتها أو تسرق بياناتها الحساسة، وصولاً إلى الحكومات التي قد تهدد استقرارها السياسي أو الاقتصادي أو الاجتماعي.

²³ جاسم محمد، الإرهاب الإلكتروني، دار البداية، الطبعة الأولى، عمان، 2014، ص 97

²⁴ هالة احمد الرشيد، المرجع السابق، ص34.

²⁵ عبد الجليل إسماعيل حسن الشيخ زيني، المرجع السابق، ص 100-101.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

بناء على ما سبق قسمنا هذا المبحث الى مطلبين، خصصنا المطلب الأول لدراسة أبرز مظاهر الإرهاب الإلكتروني، ومن ثم تسليط الضوء بموجب المطلب الثاني على سبل الوقاية من الإرهاب الإلكتروني.

المطلب الأول: مظاهر الإرهاب الإلكتروني

ان مظاهر الإرهاب الإلكتروني متعددة، ولعل من أبرز هذه المظاهر التهديد والترويع الإلكتروني، القصف الإلكتروني، التجسس الإلكتروني، انشاء حسابات ومواقع خاصة بالتنظيمات الإرهابية، تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، تدمير المواقع والبيانات الالكترونية والانظمة المعلوماتية، وهو ما سنتطرق اليه بموجب هذا المطلب.

الفرع الأول: التهديد والترويع الإلكتروني

تستغل المنظمات والجماعات الإرهابية وسائل الاتصال بما في ذلك الإنترنت، لنشر التهديدات، وتتنوع أساليبها وأهدافها بين بث الرعب والضغط على الأفراد والدول لتحقيق أهدافها، والحصول على التمويل وإظهار قوتها، والمقصود بالتهديد أنه إشاعة الخوف والرغبة في النفس، بهدف الضغط على إرادة الإنسان وإرغامه على الخضوع، ويستخدم الإرهابيون الإلكترونيون مختلف وسائل الاتصال والشبكات المعلوماتية لنشر التهديدات وترويع الآخرين،

²⁶ ومن بين الطرق التي تستخدمها الجماعات الإرهابية:

- إرسال الرسائل الإلكترونية المهددة،
- نشر التهديدات على المواقع الإلكترونية والمنشآت وغرف الدردشة،
- التهديد بقتل شخصيات سياسية بارزة،
- التهديد بتفجير منشآت وطنية،
- نشر الفيروسات لإلحاق الضرر بالشبكات المعلوماتية والأنظمة الإلكترونية،

²⁶ جاسم محمد، المرجع السابق، ص 133-134.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

● التهديد بتدمير البنية التحتية المعلوماتية.²⁷

الفرع الثاني: القصف الإلكتروني

يمكن تسميته أيضاً بالهجوم المعلوماتي أو الإغراق بالرسائل، وهو نوع من الهجمات الإلكترونية التي تستهدف تعطيل عمل النظام المعلوماتي، يتم من خلال إرسال كميات هائلة من البيانات إلى النظام، مما يؤدي إلى إرهابه وجعله غير قادر على العمل بالشكل الصحيح، بمعنى آخر القصف الإلكتروني هو هجوم كثيف يشنه الإرهابيون على شبكات المعلومات من خلال إطلاق مئات الآلاف من الرسائل الموجهة لموقع واحد، مما يعيق قدرته على استقبال رسائل المتعاملين معه نتيجة الضغط الهائل الذي يتعرض له مما ينتج عن ذلك تعطل الموقع بشكل تام، وحرمانه من استقبال أي رسائل أخرى، وبالتالي يتسبب بخسائر مادية ومعنوية فادحة، زعزعة ثقة المتعاملين مع أصحاب المواقع المستهدفة، خلق حالة من الارتباك والفوضى، إلحاق الضرر بسمعة الموقع الإلكتروني²⁸

الفرع الثالث: التجسس الإلكتروني

مع ازدياد انتشار شبكات المعلومات عالمياً، شهدت أساليب التجسس تحولاً هائلاً من الطرق التقليدية إلى نظيرتها الإلكترونية، حيث يستغل الإرهابيون هذه التقنيات الحديثة للتجسس على مختلف الجهات، بدءاً من الأفراد وصولاً إلى الدول والمنظمات والهيئات والمؤسسات الدولية والوطنية، ويتميز التجسس الإلكتروني بكونه أداة حديثة تعتمد على استغلال الموارد المعلوماتية والأنظمة الإلكترونية التي وفرتها حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في هذا العصر ثلاثة أهداف رئيسية:

● التجسس العسكري الذي يهدف إلى جمع المعلومات حول قدرات الدول العسكرية،

● التجسس السياسي الذي يركز على جمع المعلومات حول الأنظمة السياسية للدول،

²⁷ جاسم محمد، المرجع نفسه.

²⁸ المعتصم منجي محمود القطيشات، جريمة الإرهاب باستخدام الوسائل الإلكترونية، رسالة ماجستير في القانون العام، كلية

الحقوق، جامعة الاسراء، 2022

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

• التجسس الاقتصادي الذي يسعى إلى جمع المعلومات حول الأوضاع الاقتصادية للدول.²⁹

الفرع الرابع: إنشاء حسابات ومواقع خاصة بالتنظيمات الإرهابية

يستغل الإرهابيون الفضاء الرقمي لإنشاء مواقع إلكترونية تهدف إلى نشر أفكارهم المتطرفة وجذب المزيد من الأتباع، مستخدمين هذه المنصات لتحقيق العديد من الأهداف من بينها:

• إبراز قوة التنظيم الإرهابي،

• التعبئة الفكرية وتجنيد إرهابيين جدد،

• إعطاء التعليمات والتلقين الإلكتروني،

• التدريب الإلكتروني،

• الدخول إلى المواقع المحجوبة،

• تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، حيث تقدم بعض المواقع الإلكترونية الإرهابية تعليمات مفصلة حول كيفية صناعة القنابل والأسلحة، واختراق المواقع الإلكترونية، ونشر الفيروسات، وغيرها من الأنشطة المجرمة.³⁰

الفرع الخامس: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

تحولت الشبكة العالمية إلى أداة قوية بيد الجماعات الإرهابية، حيث تتيح لهم حرية التواصل وتبادل المعلومات فيما بينهم، فمن خلال الانترنت يمكن للجماعات الإرهابية:

• حرية التواصل وتبادل المعلومات بدون قيود،

• التخطيط والتنسيق للهجمات الإرهابية دون رقابة الأجهزة الأمنية،

²⁹ حسنين شفيق، المرجع السابق، ص 203.

³⁰ اسراء طارق جواد كاظم الجابري، المرجع السابق، ص 99.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

• كما تساهم تقنيات الانترنت في تدفق الدعم والمساعدات للجماعات الإرهابية، حيث تتيح لهم الوصول إلى جمهور ضخم من المانحين المحتملين،

• التنسيق السريع والفعال بين الجماعات الارهابية وأعضائها، مما يعزز من تنظيم نشاطاتهم ويضمن سريان سريع ومستمر للتعليمات.³¹

الفرع السادس: تدمير المواقع والبيانات الالكترونية والانظمة المعلوماتية

تشن التنظيمات الإرهابية هجمات إلكترونية تستهدف تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها ، وتعرف عملية التدمير في هذا السياق بأنها الدخول غير المصرح به الى نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام أو مجموعة نظم مترابطة شبكيا بهدف إلحاق الضرر بنقطة الاتصال أو النظام المستهدف، وتستهدف هذه الهجماتالنظم العسكرية، البنية التحتية الاقتصادية، نظم المواصلات، نظم الاتصالات، محطات توليد الطاقة.³²

المطلب الثاني: إستراتيجية الوقاية من الإرهاب الإلكتروني

من أجل وضع حد للإرهاب الإلكتروني ومنع تطوره، وجب وضع إستراتيجية شاملة من طرف الدول والحكومات للوقاية من هذه الظاهرة قبل حدوثها، وذلك من خلال:³³

تعزيز وحماية البنى التحتية لتقنية المعلومات والاتصالات لضمان مقاومة الهجمات الإلكترونية،

تطوير التشريعات القانونية المتعلقة بمكافحة جرائم الإرهاب الإلكتروني من خلال مراجعة القوانين الحالية وتعديلها لتتوافق مع التطورات التكنولوجية وسن قوانين جديدة تجرم أشكال الإرهاب الإلكتروني المختلفة.

³¹ عبد الجليل إسماعيل حسنين الشيخ زيني، المرجع السابق، ص 106

³² جاسم محمد، المرجع السابق، ص129.

³³ بن مرزوق عنترة، جريمة الإرهاب الإلكتروني الأسباب واليات العلاج، مجلة الحقوق والعلوم الإنسانية، المجلد 11، العدد 02، 2015، ص 515 و 516.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

تفعيل دور وسائل الإعلام في مواجهة الفكر الإجرامي للتنظيمات الإرهابية على شبكة الإنترنت من خلال نشر الوعي حول مخاطر الإرهاب الإلكتروني وكشف الدعاية الإرهابية على الإنترنت والتعاون مع الجهات الأمنية لتحديد المواقع المحرصة على العنف.

بث أعمال تلفزيونية تسلط الضوء على معاناة ضحايا الإرهاب الإلكتروني، وإظهار مخاطر الانضمام إلى التنظيمات الإرهابية، وتوعية الجمهور بأهمية استخدام الإنترنت بشكل مسؤول.

إقامة مؤتمرات فكرية حول مواضيع الإرهاب الإلكتروني، ودمج مفاهيم مكافحة الإرهاب الإلكتروني في المناهج الدراسية من أجل تنشئة أجيال تنبذ الإرهاب بشتى أشكاله،

غرس قيم المواطنة في المجتمع وتعزيز ثقافة التسامح والحوار، وإبراز دور المؤسسات الأمنية في حماية المجتمع من الإرهاب الإلكتروني.

الاستفادة من خبراء عاملين في مجال مكافحة الجرائم الإلكترونية من أجل المساهمة في تكوين مختصين محليين ذوي مهارات عالية لمكافحة الجرائم الإلكترونية،

الاستفادة من تجارب الدول الرائدة في مجال تحقيق الأمن السيبراني، والاطلاع على أفضل التقنيات العالمية المتبعة في مكافحة الجرائم الإلكترونية، وتطبيق التقنيات الحديثة لتعزيز الأمن السيبراني.

توعية الجمهور بمخاطر الاستخدام غير المسؤول للإنترنت، مع التأكيد على العقوبات القانونية الرادعة والتي بإمكانها منع تشجيع الانضمام للتنظيمات الإرهابية والترويج لها.

الخاتمة:

في ختام هذه الدراسة يتضح لنا انه على الرغم من ايجابيات تكنولوجيا المعلومات الا ان الاستعمال السلبي أدى الى ظهور نوع جديد من الإرهاب يعتمد على الوسائل التكنولوجية الحديثة

وعليه يمكن استخلاص النتائج التالية:

عدم وجود تعريف جامع ومانع لجريمة الإرهاب عامة والإرهاب الإلكتروني خاصة.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الإرهابية

الإرهاب الإلكتروني من الجرائم العابرة للحدود والدول والقارات، حيث يمكن ارتكاب هذه الجريمة من أي مكان في العالم.

الإرهاب الإلكتروني من الجرائم الناعمة التي لا تستدعي استخدام العنف أو القوة بل تعتمد على الوسائل التكنولوجية الحديثة وشبكة الانترنت.

صعوبة اكتشاف جرائم الإرهاب الإلكتروني ونقص الخبرة والمهارة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع هذا النوع من الجرائم.

الإرهاب الإلكتروني من الجرائم صعبة الإثبات وذلك لسهولة إخفاء واتلاف الدليل المادي الملموس للجريمة.

الأسباب العامة للإرهاب الإلكتروني هي نفسها أسباب الإرهاب بشكل عام والمتمثلة في الأسباب الشخصية، النفسية، السياسية، الاقتصادية، الاجتماعية، الفكرية.

تتمثل الأسباب الخاصة للإرهاب الإلكتروني في ضعف بنية شبكة المعلومات وقابليتها للاختراق، سهولة استخدام شبكة المعلومات وقلة التكاليف، غياب الحدود الجغرافية وتدني مستوى المخاطرة، صعوبة اكتشاف وإثبات جريمة الإرهاب الإلكتروني، الفراغ القانوني والتنظيمي وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية.

تعدد مظاهر الإرهاب الإلكتروني أبرزها التهديد والترويع الإلكتروني، القصف الإلكتروني، التجسس الإلكتروني، إنشاء حسابات ومواقع خاصة بالتنظيمات الإرهابية، تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، تدمير المواقع والبيانات الإلكترونية والأنظمة المعلوماتية. ضرورة وضع إستراتيجية شاملة من طرف الدول والحكومات من أجل الوقاية من ظاهرة الإرهاب الإلكتروني ومنع تطورها.

- على ضوء النتائج السابقة خلصت الدراسة الى مجموعة التوصيات كالآتي:

ضرورة تقديم المجتمع الدولي تعريف موحد للإرهاب بشكل عام والإرهاب الإلكتروني بصفة خاصة.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الارهابية

العمل على مواجهة أسباب ظاهرة الإرهاب الإلكتروني

تعزيز التعاون الدولي والإقليمي وتبادل الخبرات في مجال الامن السيبراني ومكافحة جرائم تقنية المعلومات وكذا تسليم المجرمين.

حجب المواقع الالكترونية التي تسعى الى نشر الإرهاب والأفكار المتطرفة للجماعات الإرهابية وسد منافذ تمويلها والحد من تجنيد الإرهابيين عن طريق شبكة الانترنت.

ضرورة توعية المواطنين بخطورة الإرهاب الإلكتروني على الاسرة والمجتمع من خلال تفعيل دور المجتمع المدني ووسائل الاعلام والمؤسسات التعليمية والمساجد.

تنظيم ملتقيات دولية ووطنية للتعريف بظاهرة الإرهاب الإلكتروني، اشكالها، وخطورتها على أمن الاسرة والمجتمع.

مراجعة التشريعات الخاصة بالجريمة الإرهابية والجريمة الالكترونية لاسيما ما يتعلق بجريمة الإرهاب الإلكتروني.

تعزيز الامن السيبراني من خلال تطوير تقنيات حماية البنية التحتية وتكوين الأجهزة الأمنية والقضائية في مجال مكافحة الجريمة الالكترونية من خلال الاستفادة من الخبراء العاملين في هذا المجال.

قائمة المصادر والمراجع

الكتب

1. ايمان بن سالم، جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري ، الطبعة الأولى، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، المانيا، 2018.
2. جاسم محمد، الإرهاب الإلكتروني، دار البداية، الطبعة الأولى، عمان، 2014.
3. حسنين شفيق، الاعلام الجديد والجرائم الالكترونية ، دار فكر وفن للطباعة والنشر والتوزيع، 2015.

الإرهاب الإلكتروني: أداة جديدة في يد التنظيمات الارهابية

4. سعيد غريب المزروعى، الإرهاب الرقمي من منظور جنائي (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2022.
5. عبد الجليل إسماعيل حسن الشيخ زيني، الإرهاب الإلكتروني في القانون الدولي ، منشورات الحلبي الحقوقية، لبنان، 2020.
6. مصطفى يوسف كافي، جرائم الفساد غسيل الأموال السياحة الإرهاب الإلكتروني المعلوماتية، مكتبة المجتمع العربي، عمان، 2014.
7. مصطفى يوسف كافي، ماهر عودة الشمايلية، محمود عزت اللحام، الاعلام والإرهاب الإلكتروني، دار الاغصار العلمي للنشر والتوزيع، الأردن، 2015.
8. هالة احمد الرشيدى، الإرهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2021.
9. المقالات
10. بن مرزوق عنتر، جريمة الإرهاب الإلكتروني الأسباب واليات العلاج ، مجلة الحقوق والعلوم الإنسانية، المجلد 11، العدد 02، 2015.
11. ولد يوسف مولود، الإرهاب الإلكتروني والطرق الحديثة لتكوين التنظيمات الجهادية عبر شبكة الانترنت، مجلة الدراسات القانونية، المجلد 03، العدد 02، الجزائر، 2017.
12. المذكرات
13. اسراء طارق جواد كاظم الجابري، جريمة الإرهاب الإلكتروني (دراسة مقارنة)، مذكرة نيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة النهرين، العراق، 2016.
14. المعتصم منجي محمود القطيشات، جريمة الإرهاب باستخدام الوسائل الإلكترونية، رسالة ماجستير في القانون العام، كلية الحقوق، جامعة الاسراء، 2022.



المراجع الأجنبية

1. Fabio Cristiano-Dennis Broeders- daan weggemans, cyber terrorism and human rights from the national to the international, and back?, The Hague Program for Cyber Norms Faculty of Governance and Global Affairs Leiden University, 2020.
2. Gabriel Weimann, Cyberterrorism How Real Is the Threat, United States Institute of Peace, 2004,
3. United States Institute of Peace (usip.org)
4. James A. Lewis, Assessing the Risks of Cyber Terrorism Cyber war and Other Cyber Threats, center for strategic and international studies, december 2002. <https://www.steptoe.com>
5. Maura Conway, Cyberterrorism : Hype and Reality,
6. <https://doras.dcu.ie>
7. Mohammad iqbal, Defining Cyberterrorism, UIC John Marshall Jornal oh Information technology & privacy law, vol 22, issue 2, winter 2004