بسم الله الرحمن الرحيم

JournaL of the Faculty of Sharia & Law(FSLJ)
مجلة كلية الشريعة و القانون
https://journal.oiu.edu.sd/index.php/JFSL

ISSN: 5442-1858

2020; 13 ; 114 – 95

https://doi.org/10.52981/jfsl.v13i1.2891

الإرهاب الإلكتروني

The electronic terrorism

د. محمد الطيب عبدالله خالد،قسم القانون، كلية إدارة الأعمال ،جامعة المجمعة –المملكة العربية السعودية

البريد الالكتروني: mo26102006@gmail.com

المستخلص :

يُعد الإرهاب الإلكتروني من أخطر أنواع الجرائم في العصر الحاضر، وذلك نتيجة لظهور الحاسبات الآلية التي غيرت شكل الحياة، حيث أصبح الاعتماد على وسائل تقنية المعلومات الحديثة في ازدياد في شتى المجالات الحياتية، إلا وأنه إن كان لهذه الوسائل الحديثة منافع، إلا أن الوجه الآخر يتمثل في الاستخدامات الضارة، منها كالإرهاب الإلكتروني (الإرهاب الرقمي) الذي أصبح سلاحاً خطراً يهدد العالم بأكمله، وذلك لسهولة استخدامه مع شدة أثره المدمر، وابتكار أساليب وطرق إجرامية مستحدثة، ولقد سعت العديد من الدول لسن الأنظمة والتدابير والاحترازات لمواجهته؛ إلا أن هذه الجهود المبذولة مازالت قليلة وبحاجة إلى المزيد من الجهود لمواجهة هذا السلاخ الخطير.

هدف البحث وسعى إلى محاولة استكشاف وتحديد معالم الإرهاب الإلكتروني، ولذا اقتصر على بيان ماهية الإرهاب الإلكتروني، وبيان أنواعه وأسبابه ودوافعه، وخصائصه وأهدافه، وإبراز أهم مظاهره وأشكاله، مع توضيح آلية وطرق التصدي له. ولذا اعتمدت الدراسة على المنهج الاستقرائي والمقارن والوصفي التحليلي لمناسبة ذلك لموضوع البحث.

وأخيرا ذيل البحث بخاتمة تضمنت النتائج والتوصيات، حيث كانت من النتائج: محدودية الدراسات والبحوث في مجال الإرهاب الإلكتروني، ومن التوصيات: ضرورة اتفاق الباحثين على تعريف موحد للإرهاب، وضرورة التوعية المستمرة بمخاطر الإرهاب الإلكتروني.

الكلمات المفتاحية: الارهاب ، الالكتروني ، الرقمي

Abstract :

Electronic terrorism is one of the most dangerous types of crimes in the present era, as a result of the rise of computers that have changed the style of life, as reliance on modern information technology has become on the increase in various areas of life, but if these modern means have benefits, the other side

is In harmful uses, including electronic terrorism (digital terrorism), which has become a dangerous weapon that threatens the entire world, This is because of its ease of use with the severity of its devastating impact, and the invention of new criminal methods, and many countries have sought to enact regulations, measures and precautions to confront it; However, these efforts are still few and more efforts are needed to confront this dangerous breach.

The aim of the research is to try to explore and define the features of electronic terrorism, and therefore it was limited to explaining the nature of electronic terrorism, clarifying its types, causes and motives, its characteristics and objectives, and highlighting its most important manifestations and forms, besides an explanation of the mechanism and methods of addressing it.

Therefore, the study adopted the comparative inductive and descriptive-analytical method to suit the topic of the research. Finally, the research was appended with a conclusion that included the results and recommendations. Among the results: the limited studies and research in the field of electronic terrorism, and among the recommendations: the need for researchers to agree on a unified definition of terrorism, and the need for continuous awareness of the dangers of electronic terrorism.

Keywords: digital terrorism , electronic

مقدمة:

الحمد لله الذي بعث محمداً بالهدى ودين الحق ليظهره على الدين كله وكفى بالله شهيداً. وأشهد ألا إله إلا الله وحده لا شريك له، وأشهد أن محمداً عبده ورسوله، صلى الله عليه وعلى آله وصحبه وسلم تسليماً مزيدا. ... أما بعد.

يشهد العالم ويعيش تطوراً في وسائل الاتصالات وتقنية المعلومات؛ حتى أصبح يطلق عليه عصر الثورة المعلوماتية؛ لأن جوانب الحياة المعيشية طغت عليها التغيرات السريعة والمتلاحقة المترتبة على التقدم العلمي والتقني.

وأصبح الإرهاب من الكلمات الأكثر تداولاً وترددًا في وسائل الإعلام المقروءة والمسموعة، ويشهد العالم أجمع موجات إرهابية كثيرة وخطيرة ومتنوعة، فليس من دولة في العالم إلا وقد اكتوت بنار هذا الداء، حيث تباينت أشكاله وتنوعت صوره، حتى أصبح مشكلة عالمية شغلت فكر العالم بأجمعه.

ولقد أنتجت هذه الثورة الكبيرة والتقدم الهائل الذي جلبته التقنية المعلوماتية ظهور مصطلح الإرهاب الإلكتروني (الإرهاب الرقمي)، وانتشر استخدامه، مما أدى إلى بروز الجرائم الإرهابية وتعقيدها، سواء من حيث تسهيل الاتصالات وتنسيق العمليات بين الجماعات الإرهابية، أو من حيث ابتكار أساليب وطرق إجرامية متقدمة، الأمر الذي دعا دول العالم إلى التنبه لقضية الإرهاب الإلكتروني وخطورته ودفعها للقيام بتشريع الأنظمة التي تساعدها على مكافحة ومحاربة هذه الجرائم المستحدثة.

أهمية البحث:

1. حداثة مصطلح الإرهاب الإلكتروني، وشيوع استخدامه.
2. يُعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب في العصر الحاضر.
3. معرفة أسباب الإرهاب الإلكتروني وطرق مكافحته.
4. قلة الدراسات والبحوث ذات الصلة بالإرهاب الإلكتروني في الدول العربية والافريقية.

أهداف البحث:

1. تسليط الضوء على ماهية الإرهاب الإلكتروني.
2. التعرف على أنواع الإرهاب الإلكتروني.
3. تسليط الضوء على مخاطر الإرهاب الإلكتروني .
4. الخروج برؤية علمية تسهم في إيجاد الحلول تحد من تزايد الإرهاب الإلكتروني.

مشكلة البحث:

يكمن الإشكال في صعوبة محاربة الإرهاب الإلكتروني، وفي خطورته على الأفراد والجماعات لأنه يضر بكافة النواحي الحياتية، كما يُعد الإرهاب من الظواهر العالمية الخطيرة التي أضحت تمثل معضلة من المعضلات لدى دول العالم كافة، كما أنه يمثل عقبة كؤود أمام تطور الدول وتقدمها.

منهج البحث:

اتبعت في هذا البحث المنهج الوصفي والتحليلي، والاستقرائي والمقارن من خلال استخلاص المعلومات من كتب الفقه الإسلامي والقانوني، والرسائل العلمية، والأبحاث والمقالات والدوريات المتخصصة التي تناولت موضوع البحث، فقمت بالتحليل والمقارنة، وبوضع النتائج والتوصيات في نهاية البحث.

حدود البحث:

أحب أن أشير إلى أنني لن أطيل في هذه الدراسة؛ لأنني لو أردت استقصاء جرائم الإرهاب الإلكتروني لطال بي البحث، ولكني أقصر البحث على تعريف جرائم الإرهاب الإلكتروني وبيان خطورتها، وأسباب انتشارها، وطرق مكافحتها وعقوبتها.

هيكل البحث:

تقوم هيكلة البحث على مستخلص ومقدمة، وأربعة مباحث، ناقش المبحث الأول مفهوم الإرهاب الإلكتروني، أما المبحث الثاني فتناول دوافع وأسباب وخصائص الإرهاب الإلكتروني، ويتركز المبحث الثالث على أنواع الإرهاب الإلكتروني، وأخيراً المبحث الرابع ناقش طرق مكافحة الإرهاب الإلكتروني، والخاتمة تضمنت أهم نتائج البحث والتوصيات، وذيل البحث بفهارس عامة.

1 المبحث الأول

1.1 مفهوم الإرهاب الإلكتروني

1.2 المطلب الأول: تعريف الإرهاب الإلكتروني في اللغة.

مصطلح الإرهاب الإلكتروني يتألف من كلمتين وللوقوف على معناه اللغوي يتطلب الأمر معرفة معنى كل كلمة على حده.

وقد جاء معنى كلمة (الإرهاب) من مصدر أرهب يرهب إرهاباً وترهيباً، وأصله مأخوذ من الفعل الثلاثي رهب بالكسر يرهب رهبة ورهبا وبالضم وبالفتح وبالتحريك أي خاف، ورهب الشيء خافه، وأرهبه وسترهبه أخافه، وترهبه توعده، والرهبة الخوف والفزع [1].

والإرهاب بالكسر الإزعاج والاخافة [2]، وقد ذكر مجمع اللغة العربية في القاهرة أن الإرهابيين وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم السياسية.

ومن هذا يتبين أن معنى الإرهاب في اللغة يدل على الإخافة والتفزيع والترويع.

وجاء معنى (إلكتروني) [مفرد]: والجمع إلكترونيات: اسم منسوب إلى إلكترون؛ حاسب إلكتروني، عقل إلكتروني، حاسبة إلكترونية، كمبيوتر، والعقل الإلكتروني جهاز إلكتروني يشتمل على مجموعة من الآلات التي تنوب عن الدِّماغ البشريّ في حل أعقد العمليّات [3] .

وعلم الإلكترونيات: فرع من الفيزياء يتناول الإلكترونات وآثارها واستخدام الأدوات الإلكترونية (البرمجة الإلكترونية –البريد الإلكتروني –البطاقة الإلكترونية–التِّقنيّات الإلكترونية–الحضارة الإلكترونية–الفضاء الإلكتروني–تكنولوجيا الإلكترونيات–عصر وسائل التعبير الإلكترونية–وسائل إعلام إلكتروني) [4].

وبناء على ما تقدم يتبين أن مصطلح الإرهاب الإلكتروني، معناه في اللغة يعني: الإخافة والتفزيع والترويع التي تتم بواسطة استخدام الأدوات الإلكترونية واستخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.

• المطلب الثاني: تعريف الإرهاب الإلكتروني في القانون:

جاء تعريفه في القانون بأنه: :(كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني تنفيذاً لمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو المواصلات أو بالأموال أو المباني أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لأعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح)[5].

---

(1) تاج العروس من جواهر القاموس، محمّد بن محمّد بن عبد الرزّاق الحسيني، الملقب بمرتضى الزبيدي، تحقيق على هلالي، ط2، الكويت: وزارة الإعلام، (1407 هـ–1987م) مادة (رهب)، ج78/10.

(2) معجم مقاييس اللغة، أحمد *بن فارس* بن زكريا القزويني الرازي، وضع حواشيه إبراهيم شمس الدين، ط1، بيروت: دار الكتب العلمية، (1420هـ–1999م)، ص132.

(3) معجم اللغة العربية المعاصرة، أحمد مختار عمر، عالم الكتب – القاهرة، (1429ه – 2008م)، الطبعة الأولى (د.ت)، ج121/1.

(4) معجم اللغة العربية المعاصرة، أحمد مختار عمر، مرجع سابق، ج123/1.

(5) المواجهة القانونية للإرهاب، د. أحمد فتحي سرور، ط1، دار النهضة العربية، القاهرة، 2008م، ص32.

كما عرفه مجمع البحوث الإسلامية بالأزهر بأنه:(ترويع الآمنين، وتدمير مصالحهم ومقومات حياتهم، والاعتداء على أموالهم وأعراضهم وحرياتهم، وكرامتهم الإنسانية، بغياً وإفساداً في الأرض)[6].

وعرفه مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي بأنه:(العدوان الذي يمارسه أفراد أو جماعات أو دول بغياً على الإنسان في دينه ودمه وعقله وماله وعرضه، ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق، وما يتصل بصور الحرابة وإخافة السبيل وقطع الطريق، وكل فعل من أفعال العنف أو التهديد, يقع تنفيذا لمشروع إجرامي فردي أو جماعي, ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو أموالهم للخطر، ومن صنوفه إلحاق الضرر بالبيئة أو بأحد المرافق والأملاك العامة أو الخاصة، أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها)[7].

كما عرفته الاتفاقية العربية لمكافحة الإرهاب بأنه: (كل فعل من أفعال العنف أو التهديد به أياً كانت دوافعه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر)[8].

وأيضاً جاء تعريفه في الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م بأنه:(الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة)[9].

وكذلك عرفه الاتحاد الأوربي عام 2002م بأنه: (أعمال ترتكب بهدف ترويع الأهالي أو إجبار حكومة أو هيئة دولية على القيام بعمل أو الامتناع عن القيام بعمل ما، أو تدمير الهياكل الأساسية السياسية أو الدستورية أو الاقتصادية أو الاجتماعية لدولة أو هيئة دولية، أو زعزعة استقرارها)[10].

وبإلقاء نظرة ثاقبة على هذه التعريفات يلاحظ أن هنالك تباين كبير وواضح، وهذا التباين نراه بأنه ناتج عن عدم وجود ضابط أو معيار محدد متفق عليه لمفهوم الإرهاب والمعاني التي يحتويها، وهذا من أبرز الإشكاليات التي تواجه طرق معالجة ظاهرة الإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والأيديولوجيات التي تعتنقها الدول تجاهه، فما يراه البعض إرهاباً يراه الآخر عملاً مشروعاً.

وعلى ضوء التعريفات الواردة أعلاه وبعد عقد مقارنة فيما بينها نميل إلى أن تعريف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي مناسب لتعريف الإرهاب اصطلاحاً؛ لقصر ألفاظه وإيجاز عباراته، وشموله لمختلف مظاهر وأنواع الإرهاب وأشكاله وأهدافه.

وعلى أثر ما سبق من تعريفات يمكن أن نخرج بتعريف لجرائم الإرهاب الإلكتروني ونقول بأنها: (كل عدوان أو تخويف أو تهديد مادي أو معنوي يحدث من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام التقنية

(6) راجع: بيان مجمع البحوث الإسلامية بالأزهر بشأن ظاهرة الإرهاب، القاهرة، بتاريخ 1422/8/15هـ-11/1/ 2001م).

(7) راجع: بيان مكة المكرمة الصادر عن المجمع الفقهي الإسلامي التابع لرابطة العالم الإسلامي في دورته السادسة عشرة، مكة المكرمة، 21 – 1422/10/26هـ الموافق 5-2002/1/10م.

(8) راجع: المادة (2) من الاتفاقية العربية لمكافحة الإرهاب الصادرة بتاريخ 1998/4/22م، وجريدة الجزيرة، العدد:(10605)، الصادر في يوم الخميس 1422/7/24هـ.

(9) راجع: المادة (2) من اتفاقية جنيف لمنع ومعاقبة الإرهاب الصادرة في 16/ 1937م.

(10) راجع: الاتفاقية مكافحة الإرهاب الصادرة عن دول الاتحاد الأوربي في عام 2002م.

المعلوماتية والوسائل الإلكترونية، بشتى أنواع العدوان ومظاهر الإفساد). لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي الهدف الأساسي للإرهابيين.

المبحث الثاني

دوافع وأسباب وخصائص الإرهاب الإلكتروني

المطلب الأول: دوافع وأسباب الإرهاب الإلكتروني

لم تأت جرائم الإرهاب الإلكتروني أو تنشأ من فراغ بل لها أسبابها ودوافعها، وهي أسباب متعددة ومتنوعة ومتداخلة تبعًا لاختلاف الاتجاهات السياسية، والظروف الاقتصادية، والأحوال الاجتماعية، والاختلاف الديني والعقدي، وهي عينها أسباب ظاهرة الإرهاب عموماً، كما أن هناك عوامل عدة تجعل من ظاهرة الإرهاب الإلكتروني سلاحاً سهلاً للجماعات والمنظمات الإرهابية لكونه لا يحتاج لاستعمال العنف والقوة، وقد تعددت الاتجاهات والمدارس الفكرية التي تناولت دراسة أسباب ظاهرة جرائم الإرهاب الإلكتروني، ونتناول ذلك على نحو ما يلي:

الفرع الأول: دوافع الإرهاب الإلكتروني[11]:

1. الدوافع الشخصية: تتعدد الدوافع الشخصية المؤدية لجرائم الإرهاب الإلكتروني ونذكر منها الرغبة في الظهور وحب الشهرة بالعدوان والتخريب والخروج عن النظام وخصوصاً من الافراد الغير مؤهلين أكاديمياً، والمخفقين عملياً، أو معيشياً، وكذلك الإحباط في تحقيق بعض الأهداف والرغبات.
2. الدوافع الفكرية: تعدد وتتنوع مثل هذه الدوافع ولكن نذكر أهمها والتي تتمثل في الفهم والتفسير الخاطئ للدين وذلك بجهل قواعده ومبادئه وأحكامه مما يقود الي الاختلاف في التيارات والأحزاب والتشدد والغلو في الآراء والأفكار.
3. الدوافع السياسية: أن الغموض في المنهج السياسي والتخطيط في العمل وتهميش دور المواطن، وعدم تلبية متطلبات التوازن الاجتماعي، وانعدام تفعيل دور مؤسسات المجتمع المدني، وغياب العدالة الاجتماعية، وإهمال الرعية أو التقصير في أمورهم وما يصلحهم، هذا من شأنه أن يولد المنظمات والأحزاب، وردود الأفعال الغاضبة التي لا تجد ما تصب فيه غضبها سوى الإرهاب.
4. الدوافع الاجتماعية: التفكك الأسري والاجتماعي، مما يؤدي إلى انتشار الأمراض النفسية والانحراف والإجرام والإرهاب، لذلك فإن المجتمع المترابط والأسرة المتماسكة تحيط الأشخاص بشعور التماسك والتعاون، ومن شذ عنهم استطاعوا احتواءه ورده عن الظلم، فالمجتمعات ذات الترابط الأسري لا تظهر بينهم الأعمال الإرهابية بالقدر نفسه الذي تظهر فيه عند المجتمعات المفككة اجتماعياً، فانتشار المشكلات الاجتماعية والتفكك الأسري يدفع الفرد إلى الانحراف في السلوك، والتطرف في الآراء، والغلو في الأفكار، وغياب التربية الحسنة التي توجه الأشخاص لمكارم الأخلاق ومحاسنها, وانعدام التربية الإيمانية القائمة على مرتكزات

(11) الإرهاب الإلكتروني في عصر المعلومات، د/ عبد الله بن عبد العزيز العجلان، بحث مقدم إلى المؤتمر الدولي الأول حول (حماية أمن المعلومات والخصوصية في قانون الإنترنت)، القاهرة، يونيو 2008م، ص13. وراجع: أسباب الإرهاب والعنف والتطرف دراسة تحليلية، د. أسماء الحسين، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الثالث، الطبعة الأولى، الرياض، جامعة الإمام محمد بن سعود الإسلامية، (1425هـ – 2004م)، ص21.

ودعائم قوية من نصوص الوحي، واستبصار المصلحة العامة ودرء المفاسد الطارئة، بالإضافة إلى قلة القدوة الناصحة المخلصة التي تعود على المجتمع بالنفع والخير وإرضاء الله سبحانه وتعالى وحب الدين والوطن[12].

5. الدوافع التجارية: نتيجة للتنافس الشرس بين الشركات التجارية الكبرى متعددة الجنسيات والعابرة للقارات، فإنها تلجأ لاختراق مواقع بعضها البعض، وتشير الكثير من البحوث والدراسات في مجال علم المعلومات أن هنالك أكثر من (٥٠) شركة حول العالم تتعرض للاختراق بشكل يومي فعلى سبيل المثال لا الحصر الاختراق الذي تعرض له شركتي(البيبسي، والكوكا كولا).

الفرع الثاني: أسباب الإرهاب الإلكتروني:

1. ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: لقد صممت شبكات المعلومات والأنظمة الإلكترونية بشكل مفتوح رغبة في التوسع وتسهيل دخول المستخدمين، مما جعلها تحتوي على ثغرات معلوماتية، يمكن للمنظمات الإرهابية استغلالها في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية.
2. صعوبة اكتشاف وإثبات الجريمة الإرهابية الإلكترونية: في كثير من أنواع الجرائم المعلوماتية لا يعلم بوقت وقوع الجريمة وخاصة في مجال جرائم الاختراق، وهذا ما يشجع الإرهابي على أن ينفذ جريمته في اطمئنان، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تعطي المجرم الامل في الإفلات من العقوبة[13].
3. سهولة استخدام التقنية وقلة التكلفة: إن السمة التي تميز شبكات التواصل المعلوماتية تتمثل في سهولة الاستخدام، وقليلة التكلفة والجهد والوقت، مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة، ومن دون الحاجة إلى مصادر تمويل ضخمة، فالقيام بشن هجومٍ إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة.
4. الفراغ النظامي والرقابي على الشبكة المعلوماتية: إن الفراغ التنظيمي والقانوني لدى بعض الدول النامية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعتبر من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر توجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق، وكذلك عدم وجود جهة مركزية تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها يعدُّ سبباً مهماً في تفشي ظاهرة جرائم الإرهاب الإلكتروني

لكل هذه الأسباب والدوافع التي ذكرت أصبحت جرائم الإرهاب الإلكتروني هي الوسيلة الأمثل والخيار الأفضل للمنظمات والجماعات الإرهابية وذلك لما تحققه من مزايا من حيث قلة التكلفة والجهد والوقت.

(12) أسباب الإرهاب والعنف والتطرف، د. صالح السدلان، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الطبعة الأولى، الرياض: جامعة الإمام محمد بن سعود الإسلامية، (1425هـ-2004م)، ج/3/22.

(13) دور الآليات الحديثة للحد من الجرائم المستحدثة-الإرهاب الإلكتروني وطرق مواجهته، أيسر محمد عطية القبسي، ملتقى الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، كلية العلوم والدراسات الاستراتيجية، المملكة الأردنية الهاشمية، 1435ه، ص17. وأيضاً: جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، د/ ناصر بن محمد البقمي، ط1، الرياض، (1430ه-2009م)، ص45.

المطلب الثاني: خصائص وأهداف الإرهـــاب الإلكتروني:

أن جرائم الإرهاب الإلكتروني تتميز بعدة خصائص تختلف عن خصائص الجرائم الإرهابية التقليدية، وتختلف عن الكثير من الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق عدد من الأهداف والأغراض غير المشروعة، وفي هذا المطلب نبين أهم خصائص الإرهاب الإلكتروني، ثم نبين أبرز أهدافه وأغراضه.

الفرع الأول: خصائص جرائم الإرهاب الإلكتروني:

يتميز الإرهاب الإلكتروني بعددٍ من الخصائص والسمات التي يختلف فيها عن بقية الجرائم، وتحول دون اختلاطه بالإرهاب العادي، ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يلي:

1. لا يحتاج في ارتكاب جرائم الإرهاب الإلكتروني إلى العنف والقوة، بل يتطلب توافر حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.
2. تتسم الجريمة الإلكترونية بأنها جريمة متعدية الحدود الاقليمية، وغير خاضعة لنطاق إقليمي محدود.
3. الصعوبة في اكتشاف وإثبات جرائم الإرهاب الإلكتروني والتحقيق فيها لعدم توافر الدليل لسرعة اتلافه وتدميره، أو لعدم توافر الإمكانيات لاكتشافه، وعدم وضوح التشريعات القانونية والإجراءات القضائية في بعض الدول للتعامل مع مثل هذا النوع من الجرائم.
4. أن مقترف جريمة الإرهاب الإلكتروني يكون في الغالب من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية مما يمكنه من إخفاء الدليل أو تتبعه[14].

الفرع الثاني: أهداف جرائم الإرهاب الإلكتروني:

مما لا شك فيه أن مرتكبي جرائم الإرهاب الإلكتروني يسعون إلى تحقيق كثير من الأهداف الغير المشروعة والتي لا حصر لها، ولكن يمكننا بيان أبرز تلك الأهداف في ضوء النقاط الآتية:[15]

1. السعي إلى الإخلال بالنظام العام والطمأنينة، والأمن المعلوماتي.
2. تدمير وإتلاف البنى المعلوماتية التحتية وتسبيب الإضرار بوسائل الاتصالات.
3. التهديد والترويع عبر نشر الصور المفزعة والأفكار الضالة.
4. سرقة الأموال إلكترونياً لتمويل العمليات الإرهابية.
5. إثارة الراي العام وخلق الفوضى وتهديد الدول والأشخاص وزعزعة الأمن وسلامة المجتمع.

ونخلص إلى أن هذه الأهداف التي ذكرت على سبيل المثال وليس الحصر وتعدد أساليب التهديد وطرقه وذلك لخلق ما يسمى بتوازن الرعب، وإحداث الصدمة، وترويع الأفراد والدول.

---

(14) دور الآليات الحديثة للحد من الجرائم المستحدثة-الإرهاب الإلكتروني وطرق مواجهته، أيسر محمد عطية القبسي، ملتقى الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، مرجع سابق، ص 17. راجع: السياسية الجنائية، في مواجهة جرائم الانترنت، د/ موسى مسعود أرحومة، بحث مقدم إلى المؤتمر الدولي جامعة الطفيلة التقنية، حول (التنمية البشرية والامن في عالم متغير)، الأردن، 10-2007/7/12م، ص8.

(15) جرائم المساس بأمن الدولة والانترنت، د/ حسني الجندي، ورقة بحثية قدمت في ندوة الأمن والانترنت، القاهرة، أكاديمية الشرطة، 2003م، ص16.

المبحث الثالث

أنواع الإرهاب الإلكتروني وأشكاله

نتناول في هذا المبحث أبرز وأهم أنواع الإرهاب الإلكتروني وأشكاله، ولذا نقسم هذا المبحث إلى مطلبين، نتناول في الأول استخدام الوسائط المعلوماتية، وفي الثاني استهداف الوسائط الإلكترونية وذلك على النحو الآتي:

المطلب الأول: الجرائم المرتكبة باستخدام الوسائط المعلوماتية:

الفرع الأول: التهديد والتخويف الإلكتروني:

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات، ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب ومحاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي ولإبراز قوة التنظيم الإرهابي من ناحية أخرى.

والمقصود بالتهديد: الوعيد بشر، وزرع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أن ضرراً ما سيلحقه أو سيلحق أشخاصاً أو أشياء له بها صلة.

وقد يلجأ مجرمي الإرهاب الإلكتروني إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية؛ بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية.

ولقد تعددت الأساليب الإرهابية في التهديد، فتارة يكون بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، وتارة بنشر الصور ومقاطع الفيديو ونحو ذلك[16].

الفرع الثاني: التعبئة والتجنيد وتبادل المعلومات ونشرها:

إذا كانت الجرائم التقليدية تتطلب لقاء الإرهابيين والمجرمين في مكان معين للتخطيط ولمعرفة كيفية التنفيذ وتبادل الآراء والأفكار والمعلومات، فأصبح في العصر الحاضر الأمر سهلاً وميسراً إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي وزمن معين، وتبادلوا الحديث والاستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم أتباعاً لنشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية، وبواسطة استخدام البريد الإلكتروني، حيث إن كثيراً من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها، ويقومون كذلك باستغلال البريد الإلكتروني والاستفادة منه في نشر أفكارهم والترويج لها، والسعي للتعبئة ولتجنيد الأتباع والمتعاطفين[17].

---

(16) جرائم نظم المعلومات، د/ حسن طاهر داود، الطبعة الأولى، الرياض، جامعة نايف العربية للعلوم الأمنية، (1420هـ -2000م)، ص27. وأيضاً راجع: جرائم الاعتداء على الأشخاص والأموال، د. رؤوف عبيد، القاهرة: دار الفكر العربي,1985م، ص23.

(17) تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها، د/ محمد مؤنس محب الدين، مرجع سابق، ص122. راجع: بحث بعنوان: (الإطار القانوني للإرهاب الإلكتروني واستخدام الانترنت للأغراض الإرهابية)، منشور ضمن كتاب بعنوان: (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية)، كلية العلوم الاستراتيجية، المملكة الأردنية الهاشمية، 1435ه، ص17.

ونخلص إلى أنه بات من خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة، والتي تتعارض مع مصلحة المجتمع، نظراً لقلة تكاليف الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى، حيث يمكن وضع رسائل مشفرة تأخذ طابعاً لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته، كما أنها لا تترك أثراً لتعقبه، وكما أنها تعتبر موسوعة إلكترونية شاملة لنواحي الحياة، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية وغيرها، مما يوفر لهم المعلومات التي تساعدهم على التخطيط والتنسيق لنشر أفكارهم وشن العمليات الإلكترونية.

الفرع الثالث: إنشاء المواقع الإرهابية الإلكترونية:

أصبح من السهل قيام الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات لاستغلالها في البث والدعوة لأفكارهم الضالة ومبادئهم المنحرفة, ولإبراز قوة التنظيم الإرهابي, وللتعبئة الفكرية وتجنيد إرهابيين جدد, ولإعطاء التعليمات والتلقين والتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشئت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات، والأسلحة الكيماوية, ولشرح طرق اختراق البريد الإلكتروني، وكيفية اختراق وتدمير المواقع الإلكترونية، والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات, ونحو ذلك[18].

وقد أصبح الآن متاحاً للجماعات الإرهابية نقل المعلومات والأفكار والتوجيهات من الرؤوس المدبرة إلى الأتباع والأنصار عبر مواقعهم الإلكترونية من خلال الرسائل النصية، أو رسائل الوسائط، أو المحادثات الفورية، وتستطيع هذه العصابات حماية مواقعهم واتصالاتهم بنظم مشفرة وحيل تصعب كشفهم وملاحقتهم.

ونذكر على سبيل المثال بعض المواقع الإلكترونية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية، فمن حيث المواقع الغربية نذكر موقع (المقاومة الإريانية البيضاء)، التي أسسها توم ميتزقر (Tom Metzger) المتطرف الأمريكي، حيث أسس مجموعة بريدية إلكترونية لبث أفكاره المتطرفة وللتواصل مع أتباعه، ومن أمثلة المواقع الإلكترونية العربية، (موقع النداء) وهو الموقع الرسمي لتنظيم القاعدة، ومن خلاله تصدر البيانات الإعلامية، و(صوت الجهاد) وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وهي تصدر بصيغتي (word),(pdf) ، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم، وقد استطاع كذلك تنظيم (داعش) من توظيف الفضاء الإلكتروني[19].

ونخلص إلى أن التنظيمات الإرهابية والجماعات المتطرفة قد استفادوا من هذه الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، فأصبح لهم العديد من المواقع على الشبكة العالمية للمعلومات، وصارت تلك المواقع من أبرز مظاهر وأشكال الإرهاب الإلكتروني.

الفرع الرابع: السعي للحصول على التمويل:

(18) بحث بعنوان: (استخدام شبكة الانترنت في مجال الاعلام الأمني العربي)، د/ فايز بن عبد الله الشهري، مجلة البحوث الأمنية، مركز الدراسات، كلية الملك فهد الأمنية، الرياض، المجلد (10)، العدد (19)، نوفمبر 2001م، ص182.

(19) المرجع السابق، ص182. وانظر: الفضاء المعلوماتي، د/ حسن مظفر الرزو، الطبعة الأولى، بيروت، مركز دراسات الوحدة العربية، 2007م، ص23.

مما لا شك فيه أن الجماعات والمنظمات الإرهابية قد استغلت الشبكة العنكبوتية كمصدر لجمع الأموال لاستغلالها في تمويل جرائمها الإرهابية، مستقلة الفرص التي وفرتها التقنية الرقمية في حقل الاستثمار الرقمي والتواصل مع المستخدمين من شتى الدول.

حيث تقوم التنظيمات الإرهابية بالاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية، ومن خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي العاطفة، والقلوب الرحيمة، ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، وقد يتم ذلك بواسطة رسائل البريد الالكتروني، أو من خلال وسائل الحوار الإلكترونية، ويكون بطريقة ذكية وأسلوب مخادع بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية[20].

وتأخذ مصادر التمويل أشكالاً متنوعة فتارة تكون مباشرة بالأموال النقدية والعينية كالتي يقدمها الافراد أو الشركات والمؤسسات، وتارة أخرى في شكل تدريب على الاعمال التدميرية والتخريبية، أو الحصول على التمويل بواسطة التهديد والترويع والابتزاز، أو الاستيلاء على الأموال بالسطو المسلح على البنوك والشركات، أو عن طريق الفدية وغيرها من الطرق الغير مشروعة[21].

المطلب الثاني: جرائم استهداف الوسائط المعلوماتية:

الفرع الأول: تدمير واختراق المواقع والبيانات الإلكترونية:

تستهدف الجرائم الإلكترونية الإرهابية في عصر المعلومات في الغالب ثلاثة أهداف رئيسية، وهي الأهداف العسكرية، والسياسية، والاقتصادية، مستهدفةً مراكز القيادة والتحكم فيها، ثم المؤسسات والمنافع المدنية كالكهرباء والمياه والصحة، والقطاعات الاقتصادية كالمصارف والأسواق المالية، مستهدفة البنية المعلوماتية التحية، والبيانات الإلكترونية والنظم المعلوماتية لهذه المواقع بقصد إلحاق الضرر بها وتدميرها، وذلك لإخضاع إرادة الدول والشعوب للحصول على مطالب غير مشروعة[22].

وقد أصبح تدمير المواقع وقرصنة البيانات هاجساً يقلق دول العالم أجمع لما له من تأثير على زعزعة الثقة والطمأنينة الواجب توافرها في التعاملات الإلكترونية في عصر العولمة الرقمية، ويحول بينها وبين قيام الحكومة الإلكترونية التي توجبها النواحي الحياتية العصرية.

وقد بات من شبه المؤكد أنه لا تتوافر حتى الآن تقنية أو نظام أو تطبيق يمكن أن تحول كاملاً دون تدمير المواقع أو اختراقها أو سرقة البيانات بشكل دائم، فالمتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح للأجزاء، سواء كان ذلك في مكونات نقطة الاتصال، أو في النظم أو في الشبكة أو في البرمجة، تجعل الحيلولة دون حصول القرصنة أمراً غير ممكن، بالإضافة إلى أن المنظمات الإرهابية من ضمن أهدافها الرغبة في الاختراق وتدمير المواقع بما لديها من الإمكانات والقدرات التي لا تتوافر للأفراد[23].

ولقد قام خبراء الجرائم الإلكترونية والأمن المعلوماتي بوضع بعض من السيناريوهات المحتملة للجرائم الإلكترونية الإرهابية، نذكر منها استهداف النظم العسكرية، وذلك باختراق منظومة الأسلحة الاستراتيجية، ونظم الدفاع الجوي، والصواريخ النووية، فقد تتوافر للمنظمات الإرهابية المعلومات الخاصة بفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية، والأسلحة الفتاكة، فيحدث ما لا

(20) تجفيف مصادر تمويل الإرهاب، د/ محمد السيد عرفة، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، 1430هـ، ص73.
(21) دور الآليات الحديثة للحد من الجرائم المستحدثة-الإرهاب الإلكتروني وطرق مواجهته، د/ أيسر محمد عطية القبسي، مرجع سابق، ص 22.
(22) الأحكام الفقهية للتعاملات الإلكترونية، د/ عبد الرحمن بن عبد الله السند، الطبعة الثالثة، الرياض، دار الوراق، (1427هـ -2006م)، ص282.
(23) الإرهاب والإنترنت، د/ علي عسيري، الرياض، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، (1427هـ -2006م)، ص43.

يحمد عقباه على المستوى العالمي.، أو استهداف محطات الطاقة الكهربائية والمياه المعلوماتية وذلك بشن هجمات على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية والمياه، أو استهداف البنية التحتية الاقتصادية بإحداث خلل كلي أو جزئي في نظم الشبكات التي تتحكم بسريان أنشطة المصارف وأسواق المال العالمية، أو باستهداف نظم المواصلات والاتصالات[24].

ونخلص إلى أن هذا السيناريوهات على سبيل المثال وليس الحصر، ولا يتوقف الأمر عند هذا الحد، بل هناك العديد من الأهداف الأخرى التي يمكن للمجرمين الإرهابيين أن يشيعوا الفساد، وينشروا الفوضى في العالم، وقد أوجب الواقع على جميع الدول العمل على تطوير برامجها ونظمها الإلكترونية بحيث تحول أو تحقق أعلى درجات من الأمن المعلوماتي، وذلك للحيلولة دون اختراق أو قرصنة أو تدمير أجهزتها الإلكترونية العسكرية أو الاقتصادية أو السياسية.

الفرع الثاني: التجسس الإلكتروني:

أدى عصر التقنية وتوفر وسائل الاتصال الحديثة إلى انعدام الحدود الدولية، وأصبحت مساحات الدول مستباحة بأقمار التجسس والبث الفضائي، وتحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية، وبقصد بمفهوم بالتجسس الإلكتروني الاطلاع على معلومات خاصة بالغير ومؤمنة في جهاز آخر، وليس مسموحاً لغير المخولين الاطلاع عليها [25].

ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة من أجل الحصول على أسرار ومعلومات الدولة، ومن ثم إفشائها لدول أخرى معادية، أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة، وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق، ومن أشهرها البريد الالكتروني، حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة مجهولة أو إخفاء المعلومات داخل المعلومات، ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في إن هناك معلومات حساسة يتم تهريبها[26].

ويرمي الارهابيون من خلال التجسس الإلكتروني إلى هتك الأسرار والاطلاع على المعلومات والبيانات والتجسس عليها لمعرفة المراسلات والمخاطبات والاستفادة منها في عملياتهم الإرهابية، أو التهديد لحملهم على إتيان أفعال غير مشروعة.

وتجدر الإشارة إلى أن الطرق الفنية للتجسس على المعلومات سوف تكون أكثر الطرق استخداماً في المستقبل من قبل التنظيمات الإرهابية، نظراً لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصاً العسكرية والسياسية والاقتصادية، وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن.

(24) حماية الشبكات الرئيسية من الاختراق والبرنامج الضارة، زكريا أحمد عمار، رسالة ماجستير غير منشورة، جامعة النيلين، السودان، 2011م، ص20. وايضاً: الإرهاب الإلكتروني في عصر المعلومات، د/ عبد الله بن عبد العزيز العجلان، مرجع سابق، ص24.

(25) جرائم الانترنت والاحتساب عليها، د/ محمد عبد الرحيم سلطان، ورقة بحثية قدمت في مؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، 2000م، ص88.

(26) الاجرام الإلكتروني، د/ علي عدنان الفيل، ط1، دمشق، منشورات زين الحقوقية، 2011م، ص96. وانظر: جرائم الكمبيوتر والانترنت، د/ محمد أمين الرومي، دار المطبوعات الجامعية، 2003م، ص136.

الفرع الثالث: سرقة الأموال إلكترونياً:

انتهزت المنظمات الارهابية التطور التقني الذي انتظم التعاملات المالية والذي قاد بدوره إلى تقدم وتنامي التجارة الإلكترونية، حيث أمكنها شن هجوم إلكتروني على المواقع الإلكترونية بقصد الاستيلاء على محتوياتها، أو بشن هجوم الكتروني عن طريق الشبكة المعلوماتية على أحد البنوك والمصارف المالية بقصد السرقة والاستيلاء على الأموال وذلك من أجل تمويل ذلك التنظيم الإرهابي [27].

وقد ازداد الأمر خطورةً في الوقت الحاضر مع توفر سهولة الاستيلاء على بطاقات الائتمان، حيث يمكنهم سرقة أرقام بطاقات الائتمان من خلال شبكة الانترنت ثم القيام ببيع هذه المعلومات للغير [28].

كما تتم عمليات التحويل الإلكتروني غير المشروعة من خلال إيهام المجني عليه بمشروع كاذب، أو بالحصول على ربح مالي، أو الاحتيال بواسطة بطاقات الدفع الإلكتروني من خلال شبكة التسوية الإلكترونية الدولية، مثل بطاقات هيئة الفيزا كارد، أو الماسترد كارد [29].

وخلاصة القول نجد أنه من خلال هذه الوسائل والطرق استطاعت الجماعات والمنظمات الإرهابية سرقة الأموال الكترونياً وتوظيفها في تمويل الجرائم الإرهابية التقليدية أو الإلكترونية، وفي إطار هذه المخاطر المتزايدة وجب على دول العالم التصدي لهذه الجرائم وقطع سبل التمويل عن هذه المنظمات الإرهابية.

1.3 المبحث الرابع

1.4 طرق مكافحة الإرهاب الإلكتروني

تعد الجرائم الإلكترونية الإرهابية من أكثر الجرائم المعاصرة خطورةً وتعقيداً، وذلك لكونها نتاج عوامل متداخلة سواءً أكانت سياسية، أو اقتصادية، أو اجتماعية، أو ثقافية، أو إيديولوجية، ولكونها جرائم ذات صعوبة بالغة في الضبط والتحقيق، حيث يجمع الإرهابي الإلكتروني بين سهولة الحصول على أداة الجريمة المتمثلة في الحاسب الآلي وخدمة الانترنت، وخطورة الاضرار المترتبة عن الجريمة، بالرغم من أن الجريمة الإرهابية الإلكترونية تهدف بالأساس إلى الترويع والتخويف وإعلام العالم الخارجي، وتعود هذه الصعوبة إلى سهولة محو أثارها، وإلى السرية التي يعمل بها الارهابيون، بالإضافة لصعوبة تعقب الجريمة والمجرم، حتى اعتبرها البعض من الجرائم النظيفة[30].

وعلى ضوء هذه المعطيات، تُعد الجرائم الإلكترونية بحق من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت، لذا يمكن ترتيب سُبل مواجهة هذا النمط من الإرهاب وَفقَ الطرق الآتية:

الطريقة الأولى: التدابير السياسية والتنظيمية: وتشمل ما يأتي:

أ. السياسات السيبرانية: إن سياسة الدولة على المستويين المحلِّي والدَّولي تحدِّد توجُّهاتها في الفضاء السيبراني، ويبدو أن بعض الدول الكبرى الناشطة في الفضاء الإلكتروني مثل الصين وروسيا لديها تحفظاتٌ تتعلَّق بهذا الفضاء؛ إذ رأت في العولمة السيبرانية تعدِّيًا على سيادة الدولة القومية، ولا يمكن لأي دولة في ظلِّها أن تسيطرَ على المضمون المتداوَل بين مواطنيها عبر شبكة الإنترنت. لذلك

(27) عولمة الجريمة الاقتصادية، د/ عباس أبو شامة عبد المحمود، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007م، ص20.

(28) البطاقات الائتمانية المستخدمة الأكثر انتشاراً في البلاد العربية، عمر الشيخ الأصم، ورقة بحثية مقدمة ضمن أعمال ندوة تزوير البطاقات الائتمانية، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1، 2002م، ص12.

(29) المرجع السابق، ص13.

(30) دور الآليات الحديثة للحد من الجرائم المستحدثة–الإرهاب الإلكتروني وطرق مواجهته، د/ أيسر محمد عطية القبسي، مرجع سابق، ص 17.

أقامت كلٌّ منهما الحواجزَ اللازمة، وأنشأت شبكاتها القوميةَ الخاصَّة ضمن إطار شبكة الإنترنت العالمية، وبحسَب ضوابطها الخاصَّة. ونجحت كلا الدولتين في تحقيق ذلك، إضافة إلى تبنِّي معظم الدول الكبرى جماعاتٍ سيبرانيةً وسيطة تعمل لصالحها مثل الجيوش أو ما أُطلق عليه الذباب الإلكتروني.

ب. الجوانب التنظيمية والتشريعية: إن التشريعاتِ القانونيةَ التي تراعي الجوانبَ الموضوعية والشكلية مهمَّة في مواجهة الإرهاب الإلكتروني على صعيد الدول؛ إذ يجب أن تنظمَ التشريعات العمل في المجال الرَّقْمي بإنشاء مؤسسات متخصِّصة بموجب قوانين خاصَّة، وتحديد طبيعة الجرائم والعقوبات الملائمة والرادعة لها، وشمول جميع الجوانب المتعلِّقة بالتجريم والعقوبات، والإجراءات الشكلية كالضبط والتحقيق والتوقيف وما شاكلها. وفعلاً قد تصدت كافة دول العالم وما زالت للجرائم الإلكترونية بعد التطور الهائل لتقنية المعلومات، وذلك بالاستفادة من التقنية الحديثة في الحماية من الاعتداءات الإلكترونية، مثل فرض الرقابة الكافية على كل ما يقدم من خلال الشبكة المعلوماتية، ومنع وحجب الدخول على بعض المواقع التي تبث الفكر الإرهابي المنحرف، واستخدام كلمات سر الدخول للحواسب الآلية، وبرامج الحماية من الفيروسات وتحديثها بصفة مستمرة [31].أما الأنظمة القانونية التي شرعت على المستوى الداخلي للدول فنشير إلى أنظمة بعض الدول على سبيل المثال، حيث نجد منها أن الولايات المتحدة تعتبر أول من أصدرت تشريعاً لمكافحة الجرائم الإلكترونية في شهر أكتوبر من عام 2001م، وقد كون البنتاغون لجنة من عباقرة الاختراق الإلكتروني لتأمين وتحصين الفضاء الإلكتروني ([32]).

كما أصدرت المملكة العربية السعودية نظام مكافحة الجرائم المعلوماتية في عام 1428ه ([33])، مجرماً الإرهاب الإلكتروني بكافة مظاهره وأشكاله، وأصدرت أيضاً نظام جرائم الإرهاب وتمويله بتاريخ 1435ه، ويهدف هذا النظام إلى تعقب مرتكبي الجرائم المعلوماتية لو كانوا خارج الوطن ([34]) وقد توالت التشريعات في كل دول العالم لتجرم الإرهاب الإلكتروني، فلم تجد دولة صغيرة أو كبيرة لم تسن قانوناً لمكافحة هذه الجريمة العصرية.

ج. الاستراتيجيات السيبرانية: الاستراتيجية السيبرانية للدولة تحدِّد توجُّهها في هذا المجال، وتشمل كلَّ السياسات والجوانب الأخرى ذات الصلة، مثل المؤسَّسات المخوَّلة بتنظيم النشاطات الرَّقْمية وضبطها، ومواكبة التشريعات للتطوُّر الحاصل في هذا المجال، والاهتمام بتوعية المستخدِمين بالمخاطر المحتمَلة.

ح. الاتفاقيات الإقليمية والتعاون الدَّولي: تشمل الاتفاقياتُ الثنائية بين الدول الجوانبَ القانونية اللازمة للتعاون في مجال التحقيق في حوادث الفضاء الإلكتروني، أمَّا التحالفاتُ السيبرانية بين الدول، أو مع القطاع الخاصِّ؛ فهي مهمَّة في عمليات التتبُّع والتحقيق في الحوادث، وتبادل المعلومات عن أبرز الطرق الإجرامية المتَّبعة، وأهمِّ الأختام الرَّقْمية والبصَمات الإلكترونية الخاصَّة بالتنظيمات الإرهابية، وأحدث البرمجيَّات والأسلحة السيبرانية المستخدَمة، ما يساعد على تحديد هُويَّة الجهة التي تنفِّذ الهجَمات الإرهابية السيبرانية، ويسهِّل استهدافها. فقد ساهمت منظمة الأمم المتحدة في اصدار العديد من الاتفاقيات المناهضة للجرائم الإلكترونية التي

(31) استراتيجية مكافحة الإرهاب، عزالدين أحمد جلال، مجلة الفكر الشرطي، الامارات العربية المتحدة، المجلد (8)، العدد (2)، ص237.
(32) قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، محمد سيد سلطان، دار ناشري للنشر الإلكتروني، (1433ه–2012م)، ص42.
(33) أنظر: نظام مكافحة الجرائم المعلوماتية السعودي الصادر بموجب المرسوم الملكي السامي رقم (17) بتاريخ 1428/7/8ه .
(34) أنظر: نظام جرائم الإرهاب وتمويله السعودي، الصادر بموجب المرسوم الملكي السامي رقم (16) بتاريخ 1435/2/24ه .

تصدت للجرائم الإرهابية الإلكترونية، وسارعت غالبية الدول بالتصديق على هذه الاتفاقيات والتزمت بالعمل على منع الجـــرائم الإرهابية والقضاء عليها من خلال التعاون فيما بينها ([35]). كما قامت دول الاتحاد الأوربي بتوقيع اتفاقية بودابست لمكافحـــة الجرائم المعلوماتية في 2001/11/23م والتي اعتبر اطاراً مرجعياً لمكافحة جرائم الإرهاب الإلكتروني ([36]).

الطريقة الثانية: التدابير الأمنية والاستخبارية السيبرانية

يبرز أثرُ الجهات الأمنية السيبرانية في مجال التوعية والقيام بإجراءات الاستخبارات السيبرانية المضادَّة؛ لكشف ثُغرات الأنظمة المحلِّية ومعالجتها، ووضع التدابير لمواجهة الهجَمات، والقيام بالتحقيقات الفنية اللازمة، والتنسيق مع مؤسَّسات إنفاذ القانون والجهات الأخرى ذات العَلاقة. فضلًا عن متابعة النشاطات السيبرانية الحديثة، والأسلحة السيبرانية المستحدَثة، ومراقبة الفضاء الرَّقْمي، ومدى التزام المستخدمين بالمعايير المرعية محليًّا ودَوليًّا، والتعاون مع الجهات المناظرة لها إقليميًّا ودَوليًّا، ويمكنها توظيف القراصنة المحلِّيين واستقطابهم ليكونوا جيوشًا إلكترونية لصالحها.

الطريقة الثالثة: التدابير الفنية:

تتضمَّن هذه المرحلةُ تطوير البرمجيَّات والتطبيقات والأدوات والبنية التحتيَّة الإلكترونية اللازمة للمواجهة، وتشمل ما يأتي:

1. نشاء جُدران الحماية (Firewalls): لتكونَ خطَّ الدفاع الأول للأنظمة والمعلومات، وهي برمجيَّات لحماية الأنظمة والبيانات وكشف الهجَمات.
2. اجراءات أمن حسابات المستخدِمين وطرق التحقُّق من الهُوية: تتضمَّن حمايةَ الحسابات الرسمية والمصنَّفة، ويُعَدُّ الفرد هو العنصرَ الأهمَّ في هذا الجانب؛ إذ على مديري الأنظمة وضعُ الوسائل الآلية واليدوية اللازمة للتحقُّق من هُويَّة المستخدم.
3. تعمية البيانات: وهي من وسائل حماية البيانات عند إرسالها في الإنترنت أو عند تخزينها، بوصف ذلك عنصرَ إعاقة في حال حصلت جهةٌ غير مخوَّلة على البيانات، ما قد يمنع أو يؤخِّر استفادةَ هذه الجهة من البيانات.
4. قنية المفتاح العام: وهي تعتمد تعمية (تشفير) البيانات وتقسيمها إلى أجزاء، وتوزيعها إلى عدَّة خوادم في مناطقَ مختلفة من العالم، من قِبَل المرسِل، ولا يتمكَّن المستقبِلُ من جمعها إلا باستعمال مفتاح التشفير (مثل تقنية Freenet).
5. تقنيَّة القفز المشفَّر: وهي تقنيَّة تعتمد انتقالَ البيانات المشفَّرة من المرسِل عبر عدَّة عُقَد متتالية في الشبكة، بأن تضيفَ كل عُقدة تشفيرًا حتى تصلَ إلى المستقبِل، وهذه هي التقنيةُ المستخدَمة في شبكة (Tor) السرِّية المظلمة.
6. الشبكة الافتراضية الخاصَّة: وهي شبكة افتراضية فرعية عن شبكة الإنترنت، مصنَّفة كما هو حالُ شبكة (Linknet) الأمريكية، شبكةً سرِّية خاصَّة، تربط الأجهزة الأمنية والاستخباراتية والحكومية ذات العَلاقة بمواجهة الإرهاب السيبراني، وتستخدم المنظماتُ والدول بعضَ الشبكات الخاصَّة والمـُعَدَّة للاستخدام الخاص بين موظفيها ومديريها، وتكون معزولةً جزئيًّا عن الإنترنت، وتخضع لرقابة المختصِّين الدائمة لحمايتها.
7. تقنيَّة الفجوة الهوائية (Air-gapping): وهي تقنيَّة تستخدمها أنظمةُ التحكم والإشراف والحوسبة للبُنى التحتية الحسَّاسة وإدارة البيانات فيها، بأن تجعلَ الأنظمة معزولة كليًّا عن شبكة الإنترنت، بإعداد فجَوات فنية، تُزال فقط وَفقَ إجراءات سرِّية محدَّدة وبأوقات سرِّية أيضًا.

(35) راجع: قرارات منظمة الأمم المتحدة بهذا الشأن على موقعها الإلكتروني: (http:www.un.org).

(36) اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا د/ هلالي عبد الله أحمد، دار النهضة العربية، القاهرة، ط8، 2011م، ص43.

8. مسجِّل لوحة المفاتيح (Key logger): تقنيَّة تستخدمها الاستخباراتُ السيبرانية، وتُستخدَم للتجسُّس على أجهزة الجهات الإجرامية والمتطرفة، باستخدام البرمجيات اللازمة لاختراق أنظمة هذه المنظمات وإرسال برمجية التجسُّس للجهة المستهدَفة في الفضاء الرَّقْمي.
9. تقنيَّة خلية العسَل (Honey-cell) أو الطُّعم: وهي تقنيَّة تستخدمها الاستخباراتُ السيبرانية بوضع معلومات غير حقيقية على أحد الخوادم لتكونَ طُعمًا للإرهابيين، وَفقَ خطة مُحكَمة، بهدف معرفة نشاطات الإرهابيين وإمكاناتهم، وتحديد مواقعهم.
10. تقنية استمرار الأعمال : أي أن يستمر استعمالُ البيانات باستخدام النُّسَخ الاحتياطية(Backup) ؛ إذ عادةً ما يُحتفَظ بنُسَخ احتياطية آليًّا وَفقًا لبرمجة محدَّدة تديرها إدارةُ النظام أو الجهة الأمنية المسؤولة.

ونشير إلى ما ذهب مختصون ومحللون في مجال مكافحة الإرهاب والجرائم الإلكترونية إلى أن الحلول التقنية والقانونية قد لا تكون كافيةً لوحدها في التصدي للجرائم الإلكترونية بل يجب أن تصاحبها حلولاً أخرى مثل نشر ثقافة الحوار والتسامح على كافة المستويات التعلمية والثقافية والدينية، وتعزيز الانتماء الوطني[37].

وفى نهاية المطاف نرى أن دور مصممي البرامج في ملاحقة هذا الإرهاب قبل وقوعه يعد بمثابة الإنذار؛ فإنه لا شك فيه أن مطوري تكنولوجيا المعلومات وخبراء الإنترنت مطالبون بملاحقة أنشطتهم التوسعية بأنشطة حماية وسد ثغرات لحماية هذا الفضاء الحيوي من أن يصبح ساحة إرهاب دامية. ويجب تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الإلكترونية، وتوفير التقنيات اللازمة لمواجهتها، عبر تطوير أمن شبكات الحاسب باستخدام أنظمة التشفير المتقدمة والجدران النارية في الشبكات، وأنظمة اكتشاف المخترقين عالية الدقة، والبرامج المضادة للفيروسات، وإنشاء إدارات لمكافحة الإرهاب الإلكتروني في أنظمة الأمن، خصوصاً في الدول التي تشهد تقدماً مطرداً في اعتمادها على تكنولوجيا المعلومات أمر حيوي، خاصة وأن التطور الحاصل في هذا المجال يتسارع، والثغرات التكنولوجية فيه تتسع، وهو الأمر الذي يستلزم مواجهة كفؤة متخصصة للحد من احتمالات نجاح التهديدات الإلكترونية الإرهابية في هذا المجال.

وأخيرا نرى أن العالم قد أصبح أمام تحدٍ كبير، يتطلب تنسيقاً إلكترونياً عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلاً عن تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذا المشكلة وبخاصة الإنتربول لمواجهة كافة أشكال جرائم الإرهاب على الإنترنت.

(37) دور التربية في مواجهة الإرهاب، د/ نهى حامد عبد الكريم، ورقة بحثية قدمت في المؤتمر الثاني لكلية الشريعة والقانون، (الإرهاب في ضوء الشريعة والقانون)، جامعة إربد الأهلية، الأردن، 2002م، ص31. وأنظر: المواطنة ودورها في مكافحة الإرهاب في المملكة العربية السعودية، د/ نهاد فاروق عباس محمود، مجلة الفكر الشرطي، المجلد (23)، العدد (89)، ابريل 2014م، ص151.

2 الخاتمة

إن القضاء على ظاهرة الإرهاب الكتروني بمختلف أشكالها وصورها وأساليبها المتنوعة، أمر مربوط في المقام الأول بالوقوف على الأسباب والدوافع الكامنة ورائه، إلى جانب تحديد أهم وأبرز الآثار المترتبة على ظاهرة الإرهاب، الأمر الذي يُعد دافعاً كبيراً لدفع الدول والمنظمات الدولية والإقليمية إلى العمل بكل ما أوتيت من قدرات وإمكانات لمحاربة هذه الجرائم العصرية، وقد استعرض هذا البحث موضوع الإرهاب الإلكتروني، وقد خلص هذا البحث إلى مجموعة من النتائج والتوصيات الهامة، وهي:

أولاً: النتائج:

1. الإرهاب الإلكتروني هو الخطر المستقبلي لذا يجب رسم سياسة إلكترونية وتشريعية لمواجهته.
2. الإرهاب الإلكتروني غير محصور بمكان وزمان معينين لذا يجب على الدول متابعته باستمرار.
3. يمكن القول بأن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، بشتى صنوف العدوان وصور الإفساد.
4. كل تطور جديد يطرأ على الساحة التقنية يقابلها أشكال جديدة من الإرهاب الإلكتروني.
5. إن أسباب الإرهاب الإلكتروني ودوافعه متعددة ومتنوعة، ولكن هي عينها أسباب ظاهرة الإرهاب التقليدي عموماً.
6. سهولة تنفيذ الجرائم الإرهابية من خلال التقنيات الحديثة المتطورة.
7. إن أبرز وأهم مظاهر الإرهاب الإلكتروني وأشكاله تتمثل في تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، وإنشاء المواقع الإرهابية الإلكترونية، وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والتهديد والترويع الإلكتروني، وترويج الأفكار المتطرفة.
8. تقوم التنظيمات الإرهابية بشن الهجمات الإلكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالباً، وهي الأهداف العسكرية، والسياسية، والاقتصادية، الأمر الذي يتطلب إنشاء قاعدة بيانات مركزية حديثة مع العمل على تبادل المعلومات للمحافظة عليها من الاختراق والتلف.

ثانياً: التوصيات:

1. ضرورة السعي إلى عقد مؤتمر دولي بإشراف هيئة الأمم المتحدة يتم من خلاله وضع وتحديد تعريف شامل للإرهاب يتفق عليه الجميع، وتحديد خطة عملية دولية لمكافحته بجميع صوره وأشكاله، مع احترام سيادة الدول الأعضاء.
2. التشديد والتأكيد على أن الإرهاب لا ينتمي لدين معين، أو جنس، أو جنسية أو منطقة جغرافية محددة، وفي هذا السياق ينبغي التأكيد على أن أي محاولة لربط الإرهاب بأي منها سيساعد في حقيقة الأمر الإرهابيين، ومن ثم الحاجة إلى منع التسامح حيال اتهام أي دين، وإلى تهيئة جو من التفاهم والتعاون المشترك يستند إلى القيم المشتركة بين الدول المنتمية إلى عقائد مختلفة.

3. التأكيد على أهمية دور وسائل الإعلام والمؤسسات المدنية ونظم التعليم في بلورة استراتيجيات للتصدي لمزاعم الإرهابيين، وتشجيع وسائل الإعلام لوضع قواعد إرشادية للتقارير الإعلامية والصحفية بما يحول دون استفادة الإرهابيين منها في الاتصال أو التجنيد أو غير ذلك.
4. الدعوة إلى زيادة التعاون على المستوى الوطني والإقليمي للتنسيق بين الأجهزة المختصة بمكافحة الإرهاب الإلكتروني، لتبادل الخبرات والتجارب، بما في ذلك التدريب لضمان الفعالية في محاربة الإرهابيين وصلاتهم بالجريمة المنظمة.
5. الدعوة إلى استخدام وسائل المكافحة التقنية والقانونية، وإنشاء وتطوير الأنظمة الأمنية، بحيث تتواكب باستمرار مع التطور النوعي للعمليات الإرهابية.
6. السعي إلى إنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب عبر الشبكات المعلوماتية والأنظمة الإلكترونية وتشجيع قيام اتحادات عربية تسعى للتصدي لجرائم الإرهاب الإلكتروني.
7. حث الدول إلى الإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.
8. التأكيد على أهمية نشر القيم الإنسانية الفاضلة، والولاء للأوطان، وإشاعة روح التسامح والتعايش، وحث وسائل الإعلام على الامتناع عن نشر المواد الإعلامية الداعية للتطرف والعنف.
9. التأكيد على السعي للمعرفة والالمام بصناعة المعلومات، وإلا ستظل الشبكات المعلوماتية الحكومية، والخاصة، في بلداننا تحت رحمة من يعرف أسرارها ويحيط بنقاط الضعف في بنائها سواء كان المخرّب إرهابيا مستقلا، أو عميلا يتبع حكومات وأجهزة معادية.
10. التحذير من تزايد الإرهاب الإلكتروني، والتأكيد على أنه على الرغم من التزايد المطرد للجرائم المعلوماتية إلا أن العالم لم يشهد بعد إرهابا إلكترونياً من نوع مُشابه للإرهاب العادي والواقعي، والتنبيه إلى ضعف البنية التحتية للشبكة العالمية للمعلومات، مما يُمهد لهجمات إرهابية ربما تؤدي إلى نتائج كارثية على المجتمعات الدولية والاقتصاد العالمي.

وصلى الله على سيدنا محمد وعلى آله وصحبه وسلم.

3 الهوامش

1. أساليب إجرامية بالتقنية الرقمية، ماهيتها، ومكافحتها، موسى، د. مصطفى، دار الكتب القانونية، المحلة الكبرى، مصر، 2005م.
2. أسباب الإرهاب والعنف، دراسة تحليلية، الصافي، الحسيني، د. أسماء، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ط1، الرياض، جامعة الامام محمد بن سعود، (1425ه-2004م).
3. أسباب الإرهاب والعنف والتطرف، السدلان، د. صالح، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، ط1، الرياض، جامعة الامام محمد بن سعود، (1425ه-2004م).
4. استراتيجية مكافحة الإرهاب، جلال، د. عزالدين أحمد، مجلة الفكر الشرطي، الامارات المتحدة، المجلد (8)، العدد (2).
5. اتفاقية بودابست لمكافحة جرائم المعلوماتية، معلقاً عليها، أحمد، د. هلالي عبد الله، ط1، دار النهضة العربية، القاهرة، 2011م.
6. استخدام شبكة الانترنت في مجال الاعلام الأمني العربي، الشهري، د. فايز بن عبد الله، مجلة البحوث الأمنية، مركز الدراسات، كلية الملك فهد الأمنية، المجلد (10)، العدد (19)، 2011م.
7. الإرهاب الإلكتروني في عصر المعلومات، العجلان، د. عبد العزيز بن صالح، بحث مقدم إلى المؤتمر الدولي الأول حول (حماية أمن المعلومات والخصوصية في قانون الانترنت)، القاهرة، 2008م.
8. المواجهة القانونية للإرهاب، سرور، د. أحمد فتحي، الطبعة الأولى، القاهرة، 2008م.
9. السياسة الجنائية في مواجهة جرائم الانترنت، أرحومة، د. موسى مسعود، بحث مقدم للمؤتمر الدولي، حول (التنمية البشرية والأمن في عالم متغير)، جامعة الطفيلة، الأردن، 2007م.
10. الإطار القانوني للإرهاب الإلكتروني واستخدام الانترنت للأغراض الارهابية، عرب، د. يونس محمد، بحث منشور في كتاب بعنوان (استعمال الانترنت في تمويل الإرهاب وتجنيد الارهابين)، نشر مركز البحوث والدراسات، جامعة نايف العربية، الرياض، 1435ه.
11. البطاقات الائتمانية المستخدمة الأكثر انتشاراً في البلاد العربية، الأصم، عمر الشيخ، ورقة بحثية مقدمة ضمن أعمال ندوة تزوير البطاقات الائتمانية، جامعة نايف العربية للعلوم الأمنية، ط1، الرياض، 2002م.
12. المواطنة ودورها في مكافحة الإرهاب في المملكة العربية السعودية، محمود، د. نهاد عباس فاروق، مجلة الفكر الشرطي، المجلد (23)، العدد (89)،2014م.
13. الفضاء المعلوماتي، الرزو، د. حسن مظفر، ط1، بيروت، مركز دراسات الوحدة العربية، 2007م.
14. الأحكام الفقهية للتعاملات الإلكترونية، السند، د. عبد الرحمن بن عبد الله، ط3، الرياض، دار الوراق، (1427ه-2006م).
15. الإرهاب والانترنت، عسيري، د. علي، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، (1427ه-2006م).
16. الاجرام الإلكتروني، الفيل، د. علي عدنان، ط1، دمشق، منشورات زين الحقوقية، 2011م.
17. تاج العروس من جواهر القاموس، الزبيدي، محمد بن محمد بن عبد الرازق الحسيني، تحقيق على هلالي، ط2، الكويت، وزارة الاعلام، (1407ه-1987م).
18. تجفيف مصادر تمويل الإرهاب، عرفة، د. محمد السيد، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، 1430ه.
19. تحديث أجهزة مكافحة الإرهاب وتطوير أساليبها، محب الدين، د. محمد مؤنس، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، 1427ه.

20.جرائم المعلوماتية ومكافحتها في المملكة العربية السعودية، البقمي، د. ناصر بن محمد، ط1، الرياض، (1430ه-2009م).
21.جرائم المساس بأمن الدولة والانترنت، الجندي، د. حسني، ورقة بحث مقدمة في (ندوة الأمن والانترنت)، القاهرة، أكاديمية الشرطة. (د.ط)، 2003م.
22.جرائم نظم المعلومات، داؤود، د. حسن الطاهر، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، (01420ه-2000م).
23.جرائم الاعتداء على الأشخاص والأموال، عبيد، د. رؤوف، (د.ط)، القاهرة، دار الفكر العربي، 1985م.
24.جرائم الانترنت والاحتساب عليها، سلطان، د. محمد عبد الرحيم، بحث قدم في مؤتمر القانون في الكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، 2000م.
25.جرائم الكمبيوتر والانترنت، الرومي، د. محمد أمين، (د.ط)، دار المطبوعات الجامعية، 2003م.
26.حماية الشبكات الرئيسية من الاختراق والبرنامج الضارة، عمار، زكريا أحمد، رسالة ماجستير غير منشورة، جامعة النيلين، السودان، 2011م.
27.دور الآليات الحديثة للحد من الجرائم المستحدثة – الإرهاب الإلكتروني وطرق مواجهته، القبسي، د. أيسر محمد عطية، ملتقى الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، كلية العلوم الاستراتيجية، الأردن، 1435ه.
28.دور التربية في مواجهة الإرهاب، عبد الكريم، د. نهى حامد، بحث قدم في المؤتمر الثاني لكلية الشريعة والقانون، (الإرهاب في ضوء الشريعة والقانون)، جامعة إربد، الأردن، 2002م.
29.عولمة الجريمة الاقتصادية، عبد المحمود، د. عباس أبو شامة، الرياض، جامعة نايف العربية للعلوم الأمنية، 2007م.
30.قضايا قانونية في أمن المعلومات وحماي البيئة الإلكترونية، سلطان، محمد سيد، دار ناشري للنشر الإلكتروني، (01433ه-2012م).
31.معجم مقاييس اللغة، الرازي، أحمد بن فارس، وضع هوامشه: أبراهيم شمس الدين، ط1، بيروت، دار الكتب العلمية، (1420ه-1999م).
32.معجم اللغة العربية المعاصرة، عمر، أحمد مختار، ط1، القاهرة، (1429ه-2008م).
33.مستقبل الإرهاب في هذا القرن، العموش، د. أحمد فلاح، ط1، الرياض، جامعة نايف العربية للعلوم الأمنية، 1427ه.
34.نظام مكافحة الجرائم المعلوماتية السعودي الصادر بموجب المرسوم الملكي السامي بالرقم (17) سنة 1428ه.
35.نظام جرائم الإرهاب وتمويله السعودي الصادر بموجب المرسوم الملكي السامي بالرقم (16) سنة 1435ه