وسائل الارهاب الالكتروني وآليات مواجهتها
(دولة الامارات نموذجا) دراسة مقارنة

د. مؤتمن الفاتح طه[1]

DOI: https://doi.org/10.52981/jfsl.v12i1.2186

المقدمة

الحمد لله الذي خلق الإنسان وعلمه البيان، وكرمه فجعله سميعاً بصيراً وحباه عقلاً مميزاً ليعي العلم ويتفكر في الخلق، ويهتدي إلي الحق فيحقق سعادة الدارين فله الحمد والشكر، فبحمده تتم الصالحات وبشكره تدوم النعم، أنعم علينا برسالة الإسلام العظيم، وأرسل لنا أعظم رسله، ليكون حجة على كافة خلقه.

والصلاة والسلام علي مصباح العدالة والسلام، سيدنا محمد الذي اصطفاه من بين خلقه ليكون للعالمين نذيرا، الذي قال عنه ربه جل في علاه: " وَمَا أَرْسَلْنَاكَ إِلَّا رَحْمَةً لِلْعَالَمِينَ" [2] ورضي الله عن صحابه رسول الله وآل بيته الغر الميامين، أعظم الناس إيمانا وأكثرهم جهاداً، فكانوا بحق، خير أمة أخرجت للناس.

يعد الإرهاب الإلكتروني من أخطر أنواع الإرهاب في العصر الحاضر، نظرًا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم، لذا من الأهمية بمكان مدارسة أسبابه، وطرق مكافحته. ومصطلح "الإرهاب الإلكتروني" الذي ظَهر وشَاع استخدامه عقب الطفرة الكبيرة التي حقَّقتها تكنولوجيَا المعلومات واستخدامات الحواسب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، وهو الأمر الذي دعا 30 دولة إلى التوقيع على "الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت"، في بودابست، عام 2001 م، والذي يُعد وبحق من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت، ويتضح هذا جليًّا من خلال النظر إلى فداحة الخسائر التي يمكن أن تسببها عملية ناجحة واحدة تندرج تحت مفهومه.

وقد جرَّم علماءُ المسلمين هذا الإرهاب الإلكتروني بل جميع أنواع الإرهاب بأشكاله المختلفة، ورفضُوا لصق التُّهمة بالإسلام ووسم المسلمين بالإرهابيين.

1/ أستاذ مساعد/ جامعة الفجيرة

2/سورة الأنبياء: الأية 107

وكان حقًّا علينا وحتمًا مقضيًّا أن تحشدَ الأمَّة كلّ إمكاناتهَا اللازمَة لمحاربةِ هذه الظَّاهرة التي لا دين لها ولا حدود.

اهمية الدراسة: لقد اصبحت جرائم الكمبيوتر و الانترنت ظاهرة اجرامية جديدة –تتطور باستمرار بتطور الحاصل في مجال التقنية و نظم المعلومات– تقرع في جنباتها أجراس الخطر لتنبه المجتمع المعاصر لحجم المخاطر و هول الخسائر الناجمة عنها، و التي تستهدف اولاً الاستيلاء على المعطيات بدلاتها التقنية الواسعة ثم تنفيذ المخطط الإجرامي بعد ذلك، و قد عبر عن ذلك الفقيه الفرنسي ميلر بالآتي:"ان الكمبيوتر بشراهته كوسيلة لجمع المعلومات على نحو لا يمكن وضع حد لها ، و ما يتصف به من دقة و عدم نسيان ما يخزن فيه قد يقلب حياتنا رأساً على عقب ، يخضع فيه الأفراد لنظام رقابة صارم ، و يتحول المجتمع الى عالم شفاف، تصبح فيه بيوتنا و معاملاتنا المالية و حياتنا العقلية و الجسمانية عارية لأي مشاهد."

ومن تلك الجرائم الالكترونية ظهرت أخطارها نوعاً: جرائم الإرهاب الإلكتروني التي لا تقل في خطورتها عن خطر الإرهاب الواقعي الذي يستهدف التفجير والخطف والترويع والتخويف،والإرهاب الإلكتروني يرتبط بعلاقة طردية مع زيادة التقدم، فيزداد خطورة وفتكاً وضرراً بزيادة التقدم في المجال المعلوماتي.

وقد استغلت الجمعات الإرهابية هذا التقدم، كما استغلت ارتباط البشرية بالعالم الالكتروني لتحقق أغراضها عن طريق الإنترنت ببث معلومات وبيانات مغلوطةلاجتذاب أعداد ليست بالقليلة في كل دول العالم للمحاربة في صفوفها. كما استغلت تلك الجماعات الإرهابية وسائل التواصل الاجتماعي كتويتر وفيسبوك ويوتيوب لتمرير أهدافها خاصة في بلدان يعتمد معظم سكانها على التواصل عن طريق هذه الوسائل.

مما سبق كله: برزت أهمية التعرض لموضوع وسائل الارهاب الالكتروني وآليات مواجهتها (دولة الامارات نموذجا).

اشكالية الدراسة: لا شك أن ممارسة الإرهاب الالكتروني عبر الشبكة العنكبوتية أصبح أمراً واقعاً لا يمكن إنكاره ولا تجاهله حاضراً ومستقبلاً.لذلك من خلال هذا البحث نحاول الإجابة على التساؤلات الاتية:

ا–ماهية جرائم الإرهاب الإلكتروني، وما هي وسائلها.

2–هل توجد نصوص شرعية إسلامية تجرم وسائل الإرهاب الالكتروني.

3–ماهي الاليات القانونية الدولية التي وضعت لمكافحة الجرائم الالكترونية الإرهابية.

4–ماهي التشريعات القانونية التي وضعها المشرع الاماراتي لمواجهة الجرائم الالكترونية الإرهابية.

أهداف الدراسة: تتمثل الأهداف في الآتي:

1- إزالة الغموض حول تعريف وتوصيف جرائم الإرهاب الالكتروني وتحديدها بدقة، والوصول إلى كيفية مواجهتها وشرح ملابساتها وتشريعات مواجهتها دولياً وشرعيا ومحلياً.

2- التوصل لحقيقة: هل القواعد القانونية التي وضعها الشارع الاماراتي في كافية ومتطورة للحد من الجرائم الالكترونية.

3- الاستفادة القانونية للدول العربية عامة ودولتي السودان من التجربة التشريعية الإماراتية.

منهجية الدراسة: سوف نتبع على مدار دراستنا مجموعة من المناهج؛اهمها**المنهج المقارن:** فالحاجة تدعو الى ضرورة التطلع الى النظم القانونية المختلفة العربي منها والأجنبي التي تناولت جرائم الارهاب الإلكتروني بالمعالجة ، للاستفادة من اخر ما توصلت اليه تلك النظم لأثراء البحث وتعظيم الفائدة منه وقد اتخذنا القانون المصري كقانون رئيسيللمقارنة مع التعرض سريعاً لبعض القوانين الاخرى اذا ما وجد فيها جانب لإثراء البحث او الاستفادة من أحدث ما توصلت اليه، ولعل ما يبرر ذلك المنهج المقارن والتعرض له اكثر: ان تلك الجرائم غير مرتبطة بدوله ما، فكرتها المادي يحدث فيبيئة افتراضيه(الشبكةالعنكبوتية) تتطال اكثر من دوله ، لذا لابد كان لابد من التعرض للمنهج المقارن لضرورة تشابك وتناسق القوانين والنظم المختلفة لتوحيد مبدأ المواجهة.

كذلك سوف نتبع المنهج التأصيلي والتحليلي.

<u>خطه الدراسة:</u>

المبحث التمهيدي: مفاهيم جوهريه لجريمه الارهاب الإلكتروني

المبحث الاول: وسائل الإرهاب الإلكتروني وحكمها في الشريعة الإسلامية

البحثالثاني: الجهود الدولية في التصدي لجرائم الإرهاب الإلكتروني.

المبحث الثالث: آليات المواجهة التشريعية في تشريع دولة الإمارات المتحدة.

الخاتمة

- نتائج الدراسة
- التوصيات

المبحث التمهيدي: ماهية الإرهاب الإلكتروني

المطلب الأول: تعريف الإرهاب الإلكتروني

الفرع الأول: تعريف الإرهاب الإلكتروني في اللغة والاصطلاح.

تعريف الإرهاب في اللغة:

الإرهاب لغة يعني: العمل الذي يُحدث الإخافة، والفزع، والذعر. والإرهابي هو الذييُحدث الخوف والفزع والذعر عند الآخرين، بعمل مفزع ومخيف.

قال ابن منظور في كتابه " لسان العرب ": رَهِبَ، بالكسر، يَرْهَبُ رَهْبَةًورُهْباً بالضم، ورَهَباً بالتحريك؛ أي خاف. ورَهِبَ الشيء رَهْباً ورَهْبَةً: خافه.[1]

قال ابن فارس: (الراء والهاء والباء أصلان: أحدهما يدل على خوف والآخر على دقة وخفة).[2]وجاء في تاج العروس: (الإرهاب –بالكسر–الإزعاج والإخافة). [3] وقد ذكر مجمع اللغة

1/ ابن منظور، لسان العرب، تصحيح أمين محمد عبد الوهاب ومحمد الصادق العبيدي، الطبعة الثالثة، (بيروت: دار إحياء التراث العربي, 1419هـ–1999م) 337/5

2/ ابن فارس: أحمد بن فارس بن زكريا أبو الحسين، معجم مقاييس اللغة، تحقيق الدكتور: محمد عوض مرعب –الآنسة: فاطمة محمد أصلان، دار إحياء التراث العربي – لبنان، الطبعة الأولى 1422 هـ –2001 م، 2 / 401.

3/ محمد بن محمد بن عبد الرزاق المرتضى الزبيدي، تحقيق مجموعة من المحققين، دار الهداية طبعة الكويت، تاج العروس 538/2

العربية في القاهرة أن الإرهابيين وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم السياسية.[1]

ومن خلال ما تقدم يتبين أن معنى الإرهاب في اللغة يدل على الإخافة والتفزيع والترويع

تعريف الإرهاب في الاصطلاح:

لقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب؛ 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.

كما بذلت في هذا الشأن جهود مشكورة من أهل العلم والإنصاف، ومن بعض المجامع الإسلامية والعربية، وكذلك حاولت بعض الاتفاقيات الدولية أو الإقليمية تحديد المراد من هذا المصطلح،كما قامت بعض القوانين الجنائية الوطنية بتعريف الإرهاب، ويمكننا ذكر أهم التعاريف لهذا المصطلح فيما يلي:

عرف مجمع البحوث الإسلامية بالأزهر الإرهاب بأنه: (ترويع الآمنين، وتدمير مصالحهم ومقومات حياتهم، والاعتداء على أموالهم وأعراضهم وحرياتهم، وكرامتهم الإنسانية، بغياً وإفساداً في الأرض).[2]

وعرف مجمع الفقه الإسلامي التابع لرابطة العالم الإسلامي الإرهاب 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

1/ مجمع اللغة العربية: المعجم الوسيط، (إبراهيم مصطفى / أحمد الزيات / حامد عبد القادر / محمد النجار)، مكتبه الشروق الدولية
الطبعة الرابعة، 2004 1/ 376

2/ بيان مجمع البحوث الإسلامية بالأزهر بشأن ظاهرة الإرهاب، (القاهرة: 15/8/هـ1422-11/1/ 2001م).

الخاصة, أو تعريض أحد الموارد الوطنية أو الطبيعية للخطر، فكل هذا من صور الفساد في الأرض التي نهى الله سبحانه وتعالى المسلمين عنها).[1]

وكذلك عرف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي الإرهاب بأنه:(العدوان أو التخويف أو التهديد مادياً أو معنوياً الصادر 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 في الأرض).[2]

وعرفت 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).[3]

كما عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م الإرهاب بأنه:(الأفعال الإجراميةالموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة).[4]

وكذلك عرف الاتحاد الأوربي عام 2002م الإرهاب 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).[5]

1/ 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).

2/ قرارات وتوصيات الدورة الرابعة عشرة لمجلس مجمع الفقه الإسلامي الذي عقد في الدوحة في الفترة من

3/ الاتفاقية العربية لمكافحة الإرهاب الصادرة عن مجلس وزراء الداخلية والعدل العرب، (القاهرة: 1998/4/22م). 11–16 كانون الثاني 2003م

4/ اتفاقية جنيف لمنع وقمع الإرهاب الدولي ومعاقبته، (جنيف: 1937م).

5/ مدحت رمضان، جرائم الإرهاب في ضوء الأحكام الموضوعيةوالإجرائية للقانون الجنائي الدولي والداخلي" دراسة مقارنة"، القاهرة–دارالنهضةالعربية، سنة 1995، ص06

إن مشكلة عدم تحديد المجتمع الدولي لمفهوم الإرهاب دفعت جميع المؤتمرات العربية والإسلامية التي بحثت موضوع الإرهاب إلى تحديد هذا التعريف واستعدادها للتعاون مع المجتمع الدولي لوضع مصطلح محدد للإرهاب، فقد نص البيان الختامي الصادر عن الدورة الطارئة التاسعة لوزراء الخارجية للدول الإسلامية المنعقد في الدوحة في 23 / 7 / 1422هـ الموافق2001/10/10م على الآتي: (انطلاقا من أحكام معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي فقد أكد المؤتمر استعداد دوله في الإسهام بفعالية في إطار جهد دولي جماعي تحت مظلة الأمم المتحدة كونها المحفل الذي تمثل فيه جميع دول العالم لتعريف ظاهرة الإرهاب بمختلف أشكاله دون انتقائية أو ازدواجية، ومعالجة أسبابه، واجتثاث جذوره، وتحقيق الاستقرار والأمن الدوليين).[1]

تعريف الإلكتروني في اللغة.

أصل كلمة إلكتروني حديثة، يعرفها بعضهم بأنها جسيمات دقيقة ذات شحنات كهربائية سالبة، وشحنتها هي الجزء الذي لا يتجزأ من الكهربائية.[2]

ويقصد الباحث بكلمة إلكتروني: الصفةَ المحددةكوسيلة للإرهاب المقصودة والمستخدمة في البحث.

تعريف الإلكتروني في الاصطلاح

في قانون المعاملات التجارية الإلكترونية بإمارة دبي عرفت المادة الثانية من هذا القانون مصطلح إلكتروني بأنه ما يتصل بالتكنولوجيا الحديثة، وذو قدراتكهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية كهرومغناطيسية أو ضوئية أو ما شابه ذلك.[3]

أورد المشرع السعودي تعريفا لمصطلح إلكتروني بقوله: تنقية وسائلكهربائية، أوكهرومغناطيسية، أو بصرية، أو أي شكل آخر من وسائل التقنية المشابهة.

1/ البيان الختامي الصادر عن الدورة الطارئة التاسعة لوزراء الخارجية للدول الإسلامية المنعقد في الدوحة في 23 / 7 / 1422هـ الموافق2001/10/10م

2/ المعجم الوسيط، مرجع سابق 42/1

3/ نظام المعاملات التجارية الإلكترونية؛ إمارة دبي رقم ٢ سنة ٢٠٠٢م المادة الثانية، نقلا عن كتاب جريمة التحريض
الإلكتروني لراشد الهاجري صـ 47

وعرف أيضا: التعاملات الإلكترونية: أي تبادل، أي تراسل، أو تعاقد، أو أي إجراء آخر يبرم أوينفذٍ بشكلكلي أو جزئي بوسيلة إلكترونية. [1]

تعريف الإرهاب الإلكتروني:

مما سبق بيانه عن معنى الإرهاب في اللغة والاصطلاح ومعنى الإلكتروني في اللغة والاصطلاح وفي ضوء التعريفات السابقة يمكن القول بأن تعريف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي يعتبر من أفضل التعاريف الاصطلاحية للإرهاب وأقربها إلى الصواب؛ لقصر ألفاظه وإيجاز عباراته، ولشموله مختلف أنواع الإرهاب وأشكاله.

وتأسيساً على ما سبق يمكننا تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد.

فالإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

1/ نظام التعاملات الإلكترونية ونظام مكافحة الجريمة المعلوماتية السعودية–الصادر عام ١٤٢٨هـ السابع من ربيع الأول، المادة الأولى فقرة ٩ –١٠، من موقع وزارة الاتصالات نقلا عن كتاب جريمة التحريض الإلكتروني لراشد الهاجريص٤٦

المبحث الاول:

وسائل الإرهاب الإلكتروني وحكمها في الشريعة الإسلامية

المطلب الأول: البريد الإلكتروني

البريد الإلكتروني خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وتعد هذه الخدمة من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما تمثله من سرعة في إيصال الرسالة وسهولة الاطلاع عليها في أي مكان، فلا ترتبط الرسالة الإلكترونية المرسلة بمكان معين، بل يمكن الاطلاع عليها وقراءتها في أي مكان من العالم.

وعلى الرغم من أن البريد الإلكتروني (E–mail) أصبح أكثر الوسائل استخدامًا في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمنا وسرعة لإيصال الرسائل إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرًا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها.

وكذلك يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية.

ومما يقوم به الإرهابيون أيضًا اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

لقد نهى الله –جل جلاله –عن التجسس، فقال سبحانه: (وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ) [1] ونهت الشريعة الإسلامية عن الاطلاع على أسرار الناس وهتك حرماتهم، ففي الحديث أن النبي صلي الله عليه وسلم قال: (إنك إن اتبعت عورات المسلمين أفسدتهم أو كدت أن تفسدهم) [2] واختراق البريد الإلكتروني هو خرق لخصوصية الآخرين وهتك لحرماتهم وتجسس على

1/ سورة الحجرات، الآية: 12.

2/ رواه أبو داود، حديث رقم (4888)، وقال عنه النووي: إسناده صحيح. (انظر: رياض الصالحين باب النهي عن التجسس، ص596).

معلوماتهم وبياناتهم التي لا يرغبون أن يطلع عليها غيرهم، والنبي صلي الله عليه وسلم يقول: (ولا تحسسوا ولا تجسسوا)[1].

فالشريعة الإسلامية كفلت حفظ الحقوق الشخصية للإنسان وحرمت الاعتداء عليها بغير حق، وهؤلاء الذين يعتدون على بيانات الآخرين ومعلوماتهم عبر اختراق رسائلهم البريدية الإلكترونية آثمون لمخالفة أمر الشارع الحكيم ومستحقون للعقاب التعزيري الرادع لهم، ولا بد من إشاعة هذا الحكم بين الناس وتوعية المتعاملين بشبكة المعلومات العالمية (الإنترنت) بخطورة انتهاك خصوصية الآخرين وحكم ذلك في الشريعة الإسلامية، وأن هذا الأمر مما استقرت الشريعة على تحريمه والنهي عنه، وقد تضافرت نصوص الكتاب والسنة على حفظ حقوق الآخرين وعدم انتهاكها، بل قد تنادت الدول إلى تجريم مخترقي البريد الإلكتروني لما فيه من ضياع للحقوق واعتداء على خصوصيات الآخرين وأسرارهم، ولاسيما إذا كان ذلك لاستغلالها في الجرائم الإرهابية والعدوان على الآخرين.

واستثناء من ذلك فقد يكون التجسس مشروعًا في أحوال معينة كالتجسس على المجرمين، فقد لا يعرفون إلا بطريق التجسس، وقد أجاز الفقهاء التجسس على اللصوص وقطاع الطريق، وطلبهم بطريق التجسس عليهم وتتبع أخبارهم [2] وكذلك يجوز التجسس في حال الحرب بين المسلمين وغيرهم لمعرفة أخبار جيش الكفار وعددهم وعتادهم ومحل إقامتهم وما إلى ذلك.

أما الجاسوس الذي يتجسس على المسلمين فقد ذهب الحنفية إلى أن يوجع عقوبة ويطال حبسه حتى يحدث توبة [3]، وذهب المالكية إلى أنه يقتل ولا يستتاب ولا دية لورثته كالمحارب لإضراره بالمسلمين وسعيه بالفساد في الأرض، وقيل: يجلد نكالًا ويطال حبسه وينفى من الموضع الذي كان فيه، وقيل: يقتل إلا أن يتوب، وقيل: يقتل إلا أن يعذر بجهل، وقيل: يقتل إن كان معتادًا

1/ رواه البخاري في كتاب الأدب، باب ما ينهى عن التحاسد والتدابر، ورواه مسلم في كتاب البر والصلة والآداب، باب: تحريم الظن والتجسس والتنافس برقم (2563).

2/ إبراهيم بن علي بن محمد، ابن فرحون، برهان الدين اليعمري (المتوفى: 799هـ)، تبصرة الحكام في أصول الأقضية ومناهج الأحكام، مكتبة الكليات الأزهرية، الطبعة الأولى، 1406هـ -1986م، 2/ 171.

3/ أبو يوسف يعقوب بن إبراهيم بن حبيب بن سعد بن حبتة الأنصاري (المتوفى: 182هـ)، الخراج، تحقيق طه عبد الرؤوف سعد، سعد حسن محمد، ط المطبعة السلفية ومكتبتها – القاهرة، ص205

لذلك [1].وذهب الشافعية [2] إلى أن الجاسوس المسلم يعزر ولا يجوز قتله، وإن كان ذا هيئة – أي سلف كريم في خدمة الإسلام–عفي عنه لحديث حاطب بن أبي بلتعة رضي الله عنه[3].

وذهب الحنابلة إلى أن الجاسوس يقتل لضرره على المسلمين [4].

وكذلك يجوز اختراق البريد الإلكتروني للمجرمين المفسدين في الأرض واللصوص وقطاع الطريق، لتتبعهم ومعرفة خططهم وأماكن وجودهم، لقطع شرهم ودفع ضررهم عن المسلمين وهذا موافق لمقاصد الشريعة الإسلامية التي جاءت بحفظ الدين والعرض والمال والنفس والعقل.

المطلب الثاني: إنشاء مواقع على الإنترنت

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة نشر الفيروسات وغير ذلك.

والموقع هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل (Hype text mark-up language (HTML ولأجل رؤية هذه الصفحات يتم طلب

1/ تبصرة الحكام لابن فرحون، مرجع سابق177/1،

أيضا: أَبُو عَبْدِ اللَّهِ مُحَمَّدُ بْنُ أَحْمَدَ بْنِ أبي بكر بن فرح الأنصاري الخزرجي شمس الدين القرطبي (المتوفى: 671هـ)، الجامع لأحكام القرآن، تحقيق: أحمد البردوني وإبراهيم أطفيش، الناشر: دار الكتب المصرية – القاهرة، الطبعة: الثانية، 1384هـ –1964 م، 52/18

2/ أحمد سلامة القليوبي وأحمد البرلسي عميرة، حاشية أحمد سلامة القليوبي، دار الفكر – بيروت، بدون طبعة، 1415هـ–1995م، 4/ 226.

3/ حديث حاطب بن أبي بلتعة أخرجه البخاري 6 143، وأخرجه مسلم 4 1941.

4/ منصور بن يونس بن صلاح الدين ابن حسن بن إدريس البهوتى الحنبلي (المتوفى: 1051هـ)، شرح منتهى الإرادات، عالم الكتبالطبعة:الأولى، 1414هـ –1993م، 138/2

استعراض شبكة المعلومات العنكبوتية (WWW Browser) ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة. [1]

وتسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الإنترنت في شهر 10 2000م إلى أكثر من 22مليون موقع. [2]

إن الشبكة العنكبوتية (World Wide Web) أو نظام الويب الذي ابتكره العالم الإنجليزي تم بيرنرس عام 1989م، يرتكز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت، ومن هنا أطلقت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجانًا عبر شبكة الإنترنت في عام 1991م، واعتمد في المرحلة الأولى عام 1993م، من خلال برامج التصفح.

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإرهاب والإجرام، وتبادل الآراء والأفكار والمعلومات صعبا في الواقع فإن الإنترنت تسهل هذه العملية كثيرًا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، ويتبادلوا الحديث والاستماع لبعضهم عبر الإنترنت، بل يمكن أن يجمعوا لهم أتباعًا وأنصارًا عبر إشاعة أفكارهم ومبادئهم من خلال مواقع الإنترنت، ومنتديات الحوار، وما يسمى بغرف الدردشة، فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلًا ممكنًا، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمنوا انتشارًا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها.

لقد وجد الإرهابيون بغيتهم في تلك الوسائل الرقمية في ثورة المعلوماتية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة المعلومات العالمية الإنترنت، فغدت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب الإلكتروني.

ولا شك أن إنشاء المواقع للعدوان وتضليل الآخرين ونشر الأفكار الهدامة محرم ولا يجوز يقول سماحة مفتي عام المملكة الشيخ عبد العزيز بن عبد الله آل الشيخ: (شبكة الإنترنت من وسائل

1/ سايمون كولن، التجارة على الإنترنت، نقله إلى العربية يحيى مصلح، بيت الأفكار الدولية بأمريكا 1999م، ص26.

2/ com.yahoo. www

الاتصالات الحديثة السريعة في إيصال المعلومات الواسعة من حيث الانتشار وسهولة الوصول إليها وهي إن استغلت في الخير والدعوة إلى الله ونشر دين الله في أصقاع الأرض من قبل الأفراد والمؤسسات الإسلامية المختلفة، فلا شك أنها من الجهاد في سبيل الله بالبيان واللسان ويجب على المسلمين استغلالها وتسخيرها لهذا الغرض الخير، أما المواقع الفاسدة المخلة والمضرة بعقائد المسلمين من خلال التلبيس والتشكيك والمضرة بأخلاقهم كذلك من خلال ما يعرض فيها من الدعوة إلى الفساد وتيسير طرقه وتعليم الناشئة لهذه الأمور، وتربيتهم عليها من خلال ما يعرض فيها... فلا ريب أن هذا من أعظم المنكرات التي يجب التصدي لها وإنكارها وفق قواعد إنكار المنكر التي جاء بها النص من الكتاب والسنة، وبينها وفصلها علماء الأمة، والله تعالى يقول: ﴿وَلْتَكُن مِّنكُمْ أُمَّةٌ يَدْعُونَ إِلَى الْخَيْرِ وَيَأْمُرُونَ بِالْمَعْرُوفِ وَيَنْهَوْنَ عَنِ الْمُنكَرِ ۚ وَأُولَٰئِكَ هُمُ الْمُفْلِحُونَ﴾[1] .

وقال صلي الله عليه وسلم كما في الحديث الذي رواه أبو سعيد الخدري رضي الله عنه(من رأى منكم منكرًا فليغيره بيده، فإن لم يستطع فبلسانه، فإن لم يستطع فبقلبه، وذلك أضعف الإيمان)[2].

المطلب الثالث تدمير المواقع

تدمير المواقع يقصد به: الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (PC–Server) أو مجموعة نظم مترابطة شبكيًا (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تمامًا دون تدمير المواقع أو اختراق المواقع بشكل دائم، فالمتغيرات التقنية، وإلمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source) سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة أو البرمجة، جعلت الحيلولة دون الاختراقات صعبة جدًا، إضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في

1/ سورة آل عمران الآية (104).

2/ مسلم الإيمان (49)، الترمذي الفتن (2172)، النسائي الإيمان وشرائعه (5009)، أبو داود الصلاة (1140)، ابن ماجه إقامة الصلاة والسنة فيها (1275)، أحمد (54/3).

الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانات والقدرات ما ليس لدى الأفراد.

يستطيع قراصنة الحاسب الآلي (Hackers) التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي يصحبه تقدم أعظم في الجريمة المعلوماتية وسبل ارتكابها، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في مجال الحاسب الآلي [1].

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي [2].

وإن من الوسائل المستخدمة لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (e-mails) من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطًا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه [3].

وفي الواقع إن هناك أسبابًا لوقوع عملية تدمير المواقع ومن هذه الأسباب ما يأتي:

1/ د سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، دولة الإمارات العربية المتحدة، العدد (91).

2/ موزة المزروعي، الاختراقات الإلكترونية خطر كيف نواجه، مجلة آفاق اقتصادية، دولة الإمارات العربية المتحدة، العدد التاسع، سبتمبر 2000م، ص54.

3/ التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني) ، د عماد علي الخليل ، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3 مايو 2000م ، ص4.

1-ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسر وتخمين الكلمات السرية من المخترق.

2-عدم وضع برامج حماية كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق للموقع.

3-استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج وأنظمة غير موثوقة أمنيًا ولا يتم تحديثها باستمرار.

4-عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية [1] تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.

5-عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة فيه، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها، ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في الآونة الأخيرة، ويعد عام 2002م من أكثر الأعوام اختراقًا، فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات [2].

<u>حكم تدمير المواقع:</u>

لقد جاءت الشريعة الإسلامية بحفظ حقوق الآخرين وصيانتها، قال الله تعالي في النهي عن الاعتداء: (*وَلا تَعْتَدُوا إِنَّ اللَّهَ لا يُحِبُّ الْمُعْتَدِينَ*)[3] فنهى الله عز وجل عن الاعتداء، وإن المواقع على شبكة المعلومات العالمية حق للآخرين لا يجوز الاعتداء عليه بأي وجه من الاعتداء، وتدمير المواقع نوع اعتداء فهو محرم ولا يجوز، وقد صدر قرار مجمع الفقه الإسلامي في دورته

1/ حذرت شركة مايكروسوفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجة، ودعت المستخدمين إلى تركيب برنامج ترقيعي لحل المشكلة. (جريدة الرياض، العدد 12542، السبت 20/ 8 /1423هـ، ص19).

2/ المرجع نفسه

3/ سورة البقرة آية: 190

الخامسة سنة 1409هـ بأن حقوق التأليف والاختراع أو الابتكار مصونة شرعًا، ولأصحابها حق التصرف فيها ولا يجوز الاعتداء عليها [1].

فالاعتداء على مواقع الإنترنت ممنوع شرعًا من باب أولى، فإذا كان حق الاختراع والابتكار مصونًا شرعًا، فكذلك الموقع على شبكة الإنترنت مصون شرعًا ولا يجوز الاعتداء عليه.

ويعتبر تدمير الموقع من باب الإتلاف وعقوبته أن يضمن ما أتلفه، فيحكم عليه بالضمان. والله أعلم.

1/ مجلة مجمع الفقه الإسلامي، العدد الخامس، المجلد الثالث، ص2267.

المبحث الثاني:

الجهود الدولية في التصدي لجرائم الإرهاب الإلكتروني

نظرا للخطر الكبير الذي تمثله الجرائم الإلكترونية، أدركت دول العالم أهمية التعاون الدولي من أجل تجاوز تحديات الجرائم الإلكترونية، فعمد الكثير منها إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسوب[1] منذ عام 1983 م، بدء مع منظمة التعاون والإنماء الاقتصادي والتي قدمت دراسة حول إمكانية تطبيق القوانين الجنائية الوطنية وتكيف نصوصها لمواجهة تحديات الجرائم الإلكترونية وسوء استخدامها. ومن ثم جاءت اتفاقية فينا عام 1988م والتي حثت دول العالم على الدخول في اتفاقيات ثنائية ضد الإرهاب الإلكتروني. وبعدها تم عقد مؤتمر الثامن للأمم المتحدة في كوريا عام 1990م للنظر في نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية واقتراح تشجيع اتخاذ اجراء دولي حيال هذه الجريمة، حيث ناشد المؤتمر الأخير في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف علي ضرورة تكثيف جهودها لمكافحة الجرائم الإلكترونية في عدة وجوه[2]، منها تحديث القوانين الإجرائية وتبادل المساعدة في المسائل الخاصة بالجرائم الإلكترونية، وعقد اتفاقيات دولية تنطوي علي نصوص تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود علي الأنظمة المعلوماتية.

وقد أصدرت الأمم المتحدة عبر جمعيتها العامة العديد من القرارات التي توضح مدي تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداما غير سلمي، وجاء ذلك عبر سلسلة من القرارات، هي قرار الجمعية العامة للأمم المتحدة في الدورة 28/55 في ديسمبر عام 2000م، والدورة 56/19 في 19 ديسمبر عام 2001م في شأن إرساء الأساس القانوني لمكافحة إساءة استعمال تكنولوجيا الاتصال والمعلومات في أعمال إجرامية، وجاءت القرارات في

1/ محمد الامين البشري، التحقيق في جرائم الحاسب ا لآي، بحث مقدم إلي مؤتمر القانون والكمبيوتر والانترنت المنعقد في الفترة منن ١ – ٣ مايو ٢٠٠٠ بكلية الشريعة والقانون بدولة الإمارات، ص١٠٧٨.

انظر: كذلك حسن طاهر داوود: جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الامنية، الطبعة الأولى، الرياض، ٢٠٠٠.

2/ انظر في ذلك محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد في القاهرة ٢٥ – ٢٨ أكتوبر، ١٩٩٣، ص ٣٦٢

الدورة 35/70 في ٤ديسمبر١٩٩٨ وفي الدورة ٥٤/٤٩ في ١ديسمبر١٩٩٩، والدورة٥٥/٢٠٢٨نوفمبر ٢٠٠٠، والدورة ٥٩/١٩ في ٢٩نوفمبر ٢٠٠١، والدورة ٥٧/٥٣ في ٢٢نوفمبر٢٠٠٣ بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي. فضلا عن قرار الجمعية العامة للأمم المتحدة في الدورة ٥٧/٢٣٩ في ديسمبر٢٠٠٢ بشأن ارساء ثقافة عالمية لأمن الفضاء الإلكتروني، و٥٥/٧٢ في ٤ديسمبر٢٠٠٠ و٥٦/١٢١ في ١٩ ديسمبر٢٠٠١، والدورة ٥٨/١٩٩٩ في ٢٣ديسمبر٢٠٠٣. كما كان قرار الجمعية العامة للأمم المتحدة بإرساء ثقافة عالمية للأمن الإلكتروني من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث وتفعيل دور المنظمات الدولية ذات الصلة، ودعوة الدول إلى وضعاستراتيجيات لتقليل حجم التعرض للأخطار التي تشكل تهديداً للبنية التحتية الحيوية للمعلومات، واتخذت الجمعية العامة للأمم المتحدة في الدورة ٥٦/٢٥٨ في ٣١يناير٢٠٠٢ قراراً يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من اجل التنمية. كما صدر قرارين من الجمعية العامة للأمم المتحدة بالدعوة إلى القمة العالمية لمجتمع المعلومات في دورتها ٥٦ في ٣١يناير٢٠٠٢ والدورة ٥٧ في ٣١يناير ٢٠٠٣. وفي ديسمبر١٩٩٨ قدمت روسيا اقتراحاً للجمعية العامة للأمم المتحدة طالبت فيه بوضع مسودة قرار يتعلق بأمن المعلومات وحمل القرار مسمى "التطورات في مال المعلومات والاتصالات في سياق الامن الدولي". وتبنتها بالإجماع الجمعية العامة للأمم المتحدة. [1]

كماتبنت الامم المتحدة اقتراحاً روسياً في مايو ٢٠٠٠ يدعو إلى " تحديد المفاهيم الدولية المرتبطة بأمن المعلومات والتي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية". وفي عام ٢٠٠١ وافق اعضاء الامم المتحدة على إنشاء " مجموعة الخبراء الحكومية GGE التي بدأت عملها في عام ٢٠٠٤ بهدف مناقشة الاخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الاسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية. وشكل الأمين العام للأمم المتحدة "كوفي عنان" في بداية عام ٢٠٠٤ فريقاً دولياً لدراسة قضية إدارة الانترنت، انتهى إلى ايجاد اربعة تصورات، يتمثل أهمها في اقتراح إقامة مجلس عالمي للإنترنت يتألف من اعضاء الحكومات ويوفر تمثيلا مناسباً عن كل منطقة ويكون

1/ الموقع الرسمي للأمم المتحدة http://www.un.org/ar/ga/

له علاقة بمؤسسات الانترنت ويتم ربطه بالأمم المتحدة، على أن يكون للقطاع الحكومي دور قيادي وللقطاع الخاص والمدني دور استشاري. [1]

لقد سعت العديد من دول العالم المتقدم إلى تبني استراتيجية قومية في مجال تامين الفضاء الإلكتروني.

وتعود اول الجهود الدولية التي هدفت لمواجهة الجريمة الإلكترونية والإرهاب إلى ثلاثة عقود ماضية، حين ناقش الانتربول الدولي امكانية ايجاد تشريع قانوني حول الجريمة الإلكترونية في عام ١٩٨١. وبدا التقدم بطيئاً ولكنه اخذ في التسارع بعد انتهاء الحرب الباردة، ولعل إنشاء معهد قانون الفضاء الإلكتروني في جامعة جورج تاون الأمريكية عام ١٩٩٥ دليل على نمط المشكلة، كما دفع ذلك إلى إنشاء العديد من المبادرات الخاصة من الهيئات التي تقدم تقارير عن تبادل المعلومات والتحذيرات ومراكز داخل الولايات المتحدة وفي الخارج.

وعلى مستوى دول العالم، ومع مواكبة التطور الهائل لتقنية المعلومات تم سن أنظمة لضبط التعاملات الإلكترونية، تضمنت عقوبات للمخالفين في التعاملات الإلكترونية ومن الأمثلة على ذلك:

- ❖ في الولايات المتحدة: قررت الإدارة الأمريكية في عهد الرئيس بيل كلينتون إجراء خطوات تنفيذية لمكافحة ظاهرة "الإرهاب الإلكتروني" Cyber terrorism"،وبناءً عليه تم عام ١٩٩٦ إنشاءلجنة حماية البنية الحساسة President's Commission on Critical Infrastructure Protection(PCCIP). [2]

وفي مارس ١٩٩٨ بدأ البنتاجون في التحري عن أخطر الهجمات على أنظمة الكمبيوتر الأمريكية فيما سمي " متاهة ضوء القمر". وفي أكتوبر ١٩٩٩ تم البدء في تدريب اخر أطلق عليه " نجم القمة" لإجراء تجارب على الدروس المستفادة من التدريب، حيث قام لصوص

1/ الدكتور رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، الدورة التدريبية بعنوان توظيف شبكات التواصل في مكافحة الإرهاب، في الفترة من 23-27/ 2/ 2013، المملكة العربية السعودية، الرياض.

2/ www.fas.org/sgp/crs/homesec/RL30153.pdf

الانترنت بمهاجمة أنظمة القوى التي تغذي عدداً من القواعد العسكرية الأمريكية وقاموا بإرباك أنظمة الطوارئ في محطات الطاقة السابق ذكرها بسيل من المكالمات عن طرق الكمبيوتر. وبعد احداث ١١سبتمر ٢٠٠١ وضع البنتاجون خطة بعنوان "خريطة طريق لعمليات المعلومات"، وهي تستهدف مراقبة الانترنت والتعامل معها "كمنظومة سلاح معادية"، وفي اكتوبر ٢٠٠١ تم عقد اجتماع ضم خبراء التقنية العالية وخبراء العديد من الشركات العاملة في تكنولوجيا المعلومات الامنية، وقام الرئيس بوش بتعيين ريتشارد كلارك كأول مستشار خاص بالأمن الرقمي وتم إنشاء مكتب الامن للفضاء الإلكتروني. كما تم إنشاء "لجنة حماية البنية الحساسة" في الولايات المتحدة والتي أسست مجموعة خاصة تتناول جوانب الإرهاب الإلكتروني وأطلقت عليها اسم: " مركز حرب المعلومات" الذي يضم نحو ألف موظف وبينهم مجموعة تعمل على مدار الساعة[1]، للرد على أي تطورات او استفسارات، كما تم إنشاء "المركز القومي لحماية البنية التحتية NIPC" و"مركز تحليل وتبادل المعلومات ISACs" وبرنامج "حراسة البنية التحتية INFRAGARD" وغيرها من المبادرات.

- ❖ سن المشرع البريطاني قانون إساءة استخدام الحاسوب لسنة ١٩٩٠ (Computer Misuse Act) وبدأ سريانه بتاريخ ٢٩ آب/ أغسطس ١٩٩٠، وقد خلق هذا القانون ثلاث جرائم جديدة لمواجهة جرائم الاختراق والتوصل غير المصرح به لتعديل معطيات الحاسوب واتلافها بشكل عام وجرائم ادخال الفيروس بشكلخاص. هذه الجرائم هي: – الدخول غير المصرح به لنظام الحاسوب (النشاط الرئيسي للعبث أو التطفل)و–نفس الفعل السابق، ولكن بقصد ارتكاب أو تسهيل ارتكاب فعل آخر. التعديل أو التحوير غير المصرح به لنظام الحاسوب بقصد اضعاف أو تعطيل النظام.

- ❖ سن المشرع الفرنسي القانون رقم ١٩–٨٨ بتاريخ ٥ كانون ثاني ١٩٨٨ الخاص ببعض جرائم المعلوماتية وضمنه قانون العقوبات الفرنسي في المادة (٤٦٢) وجرم فيه مجرد الولوج إلى نظام المعالجة الآلية أو البقاءفيه بطريق غير مشروعة (٤٦٢/٢) وشدد العقوبة في الأحوال التي ينجم عن هذا الولوج محو أو تعديل في المعطيات المعالجة آليا. ونص القانون على تجريم إتلاف المعطيات وتزوير المستندات المعالجة آليا، واستعمال هذه المستندات. وعاقب على هذه الجرائم بعقوبة الحبس او الغرامة. وقد

1/ الدكتور رائد العدوان، مرجع سابق

خضع هذا القانون لتعديلات في العام ١٩٩٣ وسعت من نطاق السلوكيات محل التجريم اضافة إلى تعديل بعض العقوبات لتحقيق مزيد من الابعاد الردعية.

- ❖ على الصعيد الأوروبي: تم إنشاء مركز الحالة الراهنة (le SITCEN) المكلف ببلورة تحليل مشترك للتهديد، وضمن هذا المركز تم إدماج مجموعات العمل الثلاث المكلفة بمتابعة مكافحة الإرهاب في الاتحاد الأوروبي: مجموعة "كوتر" (COTER مرصودة لمعالجة مسائل الإرهاب خارج حدود الاتحاد الأوروبي، لاسيما عبر إقامة الحوارات الثنائية مع شركائنا الأساسيين، ومسائل العون التقني للدول الأخرى)، و"تويغ" (TWG مسائل خاصة بالأمن الداخلي للاتحاد)، ومجموعة العمل المكلفة بمتابعة اللائحة الأوروبية المعادية للإرهاب، كما ان هناك منسق أوروبي لمكافحة الإرهاب مكلف بتنسيق النشاطات داخل الاتحاد الأوروبي في ميدان محاربة الإرهاب، وذلك منذ آذار / مارس عام ٢٠٠٤ أي غداة اعتداءات التفجير في مدريد، كما أُدخلت تحسينات على التعاون الأمني والقضائي ضمن ركيزة " العدل والشؤون الداخلية" التابعة للاتحاد الأوروبي ووكالتي "أوروبولEuropol" و"أوروجوستEurojust" ، لتقديم أعمال المساعدة التقنية لصالح دول ثالثة انخرطت فيها المفوضية أو في إطار السياسة المشتركة للخارجية والأمن.

<u>مجموعات العمل ضد الإرهاب في اوروبا:</u>

1. مجموعة الـ ٨ التي تكافح الإرهاب والجريمة المنظمة في إطار مجموعة ليون/روما. وتسمح مجموعة العمل ضد الإرهاب (GACT)، التي أنشئت في أثناء قمة إيفيان عام ٢٠٠٣ بمبادرة من الرئاسة الفرنسية لمجموعة الـ ٨،بتنسيق أفضل لتقديم المساعدة لدول ثالثة لجهة تقوية قدراتها لمكافحة الإرهاب. وتضم هذه المجموعة فضلاً عن بلدان مجموعة الـ ٨ كلاً من أستراليا وإسبانيا وسويسرا والمفوضية ووحدة التقويم المستقل ONUDC والمديرية التنفيذية للجنة مكافحة الإرهاب التابعة للأمم المتحدة.[1]
2. مجلس أوروبا الذي له دور معياري خصوصاً عن طريق لجنة الخبراء في الإرهاب CODEXTER. ولقد اعتمد الاتفاقية الأوروبية لقمع الإرهاب في كانون الثاني / يناير

1/ كريستيان سكولمان، المعايير الدولية المتعلقة بجرائم الإنترنت، (مجلس اوربا) الندوة الإقليمية حول الجرائمالمتعلقة بالكمبيوتر 19-20-يونيو 2007 المملكة المغربية.

١٩٧٧، وبروتوكولاً معدلاً لها في أيار / مايو ٢٠٠٣ وفي ٢٠٠٥ لمنع الإرهاب، واتفاقية أوروبية للوقاية منالإرهاب واتفاقية تتعلق بغسل عائدات الجريمة وكشفها وضبطها ومصادرتها وعلى تمويل الإرهاب.

3. حلفالأطلسيالذيناللمرةالأولىفي١٩٩٩اعترافابدورهفيمجالالردعلىالإرهاب.ومنذ١١أيلول/سبتمبر تعزز الاهتمام بالإرهاب أكثر فأكثرانخرطت المخابرات العسكرية أكثر في تحليل التهديد، وتقوية دور اللجنةالخاصة لتحسين تبادل المعلومات المخابراتية حول الإرهاب بين الحلفاء، وتطوير تبادل المعلومات حول العلاقة بين الإرهاب والانتشار الأسلحة النووية والإشعاعية والبيولوجية والكيميائية NRBC.

4. منظمة الأمن والتعاون في أوروبا التي أصبحت تمتلك في ٢٠٠٣ وحدة مكافحة الإرهاب. وظهر توافق منذ ١١ أيلول/سبتمبر ليخدم هذا المحفل مبادرات سياسية خصوصاً لحث أعضائه على المصادقة على اتفاقيات الأمم المتحدة، أو إلى تقوية المساعدة التقنية في هذا المجال بين الدول الأعضاء.

5. مجموعة العمل المالية GAFI التيأنشأتها منظمة التعاون والتنمية في المجال الاقتصادي OECD لمكافحة تبييض الأموال والتي توسعت ولايتها بعد ١١ أيلول/سبتمبر لكي تشمل محاربة تمويل الإرهاب، حيث أقرت لهذا الغرض ٩ توصيات خاصة.

6. الشراكة الأورو. متوسطية التي أقرت في تشرين الثاني/نوفمبر ٢٠٠٥ مدونة سلوك ضد الإرهاب.

وقد وضع المجلس الأوروبي عام ٢٠٠١ "اتفاقية بودابست"، التي تشكل نصوصها منظومة تعاون دولي تتسم بالمرونة والفعالية وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم وتكفل استخدام الوسائل الفعالة في البحث والتحقيق وملاحقة مرتكبيهاوما يتعلق بالنصوص الخاصة بالتعاون الدولي

المبحث الثالث

آليات المواجهة التشريعية في تشريع دولة الإمارات المتحدة

تعاظمت مخاطر الجريمة في العصر الحديث وتحديداً منذ حدوث الثورة التكنولوجية وما نجم عنها من إفرازات سلبية أدت إلى ظهور نوع جديد غير مألوف من الجرائم ألا وهو "الجرائم الإلكترونية" والتي تعّد أشد خطراً وأعظم ضرراً من العديد من أنماط الجرائم التقليدية لا سيما في المستوى المهارى والفني لمرتكبيها في مجال استخدام التكنولوجيا أو أدوات ارتكابها أو الحيز المكاني والزماني لها، وكونها تعّد من الجرائم العابرة للوطنية في الكثير من أنماطها وهو ما يضعف من قدرات وإمكانات وأساليب مواجهتها في حالات عدة.

ومن هذا المنطلق وفي ظل ما شهدته دولة الإمارات العربية المتحدة ولكونها منالدول الرائدة على المستوى العالمي والإقليمي في تعاظم استخدام التقنيات والإلكترونيات في مجالات عدة ووجود العديد من التطبيقات الإلكترونية حتى أصبحت الحياة تعتمد بصفة رئيسية اليوم في كثير من المؤسسات العامة والخاصة وبالغالبية من مناحي الحياة بالدولة على النظم الإلكترونية مما أدى إلى تنامي خطر الجرائم الإلكترونية في ضوء الاستخدام المتزايد للوسائل والأدوات الإلكترونية. وفي ضوء ذلك قام المشرع الإماراتي بإصدار التشريعات اللازمة للتعامل ومواجهة الجرائم الإلكترونية ولغرض حماية المجتمع من مخاطرها ومهدداتها.[1]

وعلى ذلك سوف يتم في هذا المبحث بيان تلك التشريعات وما تضمنته من الأفعال والسلوكيات التي وضع المشرع عقابًا لها، ويلي ذلك بيان التعديلات التي أجراها المشرع الإماراتي على التشريعات المتعلقة بالجرائم الإلكترونية، وأخيراً بيان اتجاه المشرع الاماراتي وسياسته اتجاه الجرائم الإلكترونية بالقانون الجديد الصادر عام 2012 م وذلك في المطالب الأتية:

المطلب الأول: التشريع الاماراتي الخاص بمواجهة الجرائم الإلكترونية

سارع المشرع الإماراتي في العام 2006 م بإصدار القانون رقم(2) لسنة 2006 م في شأن مكافحة الجرائم الإلكترونية والذي يعّد الأول على مستوى الوطن العربي والعديد من الدول الأجنبية لمواجهة الجرائم الإلكترونية، وقد تضمن القانون التعريف بالمعلومات الإلكترونية

1/ المستشار محمد أحمد محمد الحمادي، تشريعات مكافحة جرائم تقنية المعلومات في دولة الإمارات وأحكام القضاء، دولة الإمارات العربية المتحدة، أبو ظبي، شرطة أبو ظبي، مركز الدراسات الأمنية، ورقة عمل قدمت بندوة شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية، الطبعة الثانية 6-7-2006، ص 9

والبرنامج المعلوماتي ونظام المعلومات الإلكتروني والشبكة المعلوماتية والمستند الإلكتروني للموقع الإلكتروني ووسيلة تقنية المعلومات والبيانات الحكومية.

كما تضمن القانون في مواده المختلفة تحديدا للأفعال التي تشكل خطرا وضررا للنظم التقنية المستخدمة وأدواتها المختلفة، وكذلك تحديد العقوبات المتعلقة بارتكاب أي من تلك الأفعال، ومن أمثلة تلك الأفعال:[1]

1) التوصل بغير وجه حق إلى أي موقع أو نظام معلوماتي.

2) الإلغاء أو الحذف أو التدمير أو الإنشاء أو الإتلاف أو التغيير أو إعادة النشر للبيانات والمعلومات الموجودة بالموقع أو النظام المعلوماتي.

3) التزوير الإلكتروني للمستندات الإلكترونية الحكومية الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية.

4) الاستعمال للمستند الإلكتروني المزور مع العلم بتزويره.

5) الإعاقة أو تعطيل الوصول إلى الخدمة أو الأجهزة والبرامج ومصادر البيانات والمعلومات بأية وسيلة كانت.

6) الإيقاف أو التعطيل أو التدمير أو المسح أو الحذف أو الإتلاف لمحتويات الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

7) استخدام الشبكة المعلوماتية لأغراض التهديد والابتزاز للأشخاص أو للاستيلاء على إحدى وسائل تقنية المعلومات.

8) استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للوصول بدون وجه حق للبيانات والأرقام الخاصة بالبطاقة الائتمانية.

9) استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات للإساءة للشعائر الإسلامية أو أحد المقدسات الدينية.

1/ القانون الاتحادي الإماراتي رقم (2) لسنة 2006 م في شأن مكافحة الجرائم الإلكترونية وتعديلاته الصادر عام 2012 م.

منتدى قوانين الإمارات على الرابط http://www.theuaelaw.com/vb/archive/index.php/f-2.html

وقد حّدد المشرع العقوبات واجبة التطبيق في حال ارتكاب الأفعال سالفة الذكروغيرها الواردة بالقانون والتي تمثلت في الحبس والغرامة والسجن المؤقت، وكذلك بعقوبة تبعية تمثلت في الإبعاد للأجنبي. ويلاحظ مما سبق أن المشرع الإماراتي لميغفل تجريم الأفعال الماسة بالنظم التقنية والأدوات المستخدمة بها وقام بتحديد تلك الأفعال والنص على العقوبات الخاصة بها.

المطلب الثاني: التعديلات التي أجراها المشرع الإماراتي على التشريعات المتعلقة بالجرائم الإلكترونية

وبالرغم مما سبق لم يتوقف المشرع الإماراتي عند حد إصدار القانون رقم (2)لسنة 2006 مالسابق بيانه بل قام بإصدار القانون الاتحادي رقم (5) لسنة 2012 م في شأن مكافحة الجرائم الإلكترونية لغرض مواكبة المتغيرات والمستجدات سواء على الساحة المحلية أم الإقليمية أم الدولية في هذا المجال.

وفي هذا الصدد، قام المشرع الإماراتي بالإضافة والتعديل للقانون الصادر عام 2006 في العديد من الأمور، والتي تمثلت في الآتي:

1- تضمنت نصوص القانون الجديد ما يتعلق بالأفعال الخاصة بالجرائم الإرهابية والمعاملات والتجارة الإلكترونية وجرائم الإتجار بالبشر وتلك المتعلقة بالسياحة والآثار والأسلحة النارية والذخائر والمتفجرات والأمن الإلكتروني، وهي أمور لم يتم تضمينها بالقانون القديم الصادر عام 2006 م، وكان الهدف من ذلكمواكبة المتغيرات والمستجدات فيما يتعلق بأنماط الجرائم المستجدة والأنشطة التجارية والمالية المختلفة والأمن المعلوماتي.

2- تضمن القانون الجديد الصادر عام 2012 م في شأن مكافحة جرائم تقنية المعلومات إضافة بعض التعريفات الجديدة التي لم يتضمنها القانون القديم حيث شمل التعريف بـ (المنشآت المالية أو التجارية أو الاقتصادية، إلكتروني، مواد إباحية الأحداث، العنوان البروتوكولي للشبكة المعلوماتية، سري، الالتقاط، الإساءة) وكان الهدف من ذلك شمول القانون للأنشطة والأفعال الإلكترونية غير المشروعة وكذلك لما يتم من عمليات تجارية باستخدام النظم التقنية.

3- اتجاه المشرع الإماراتي إلى تغليظ العقوبات السالبة للحرية وزيادة قيمة الغرامات المالية وكذلك النص على بعض العقوبات التبعية والتكميلية والتدابير وذلك بالقانون الجديد الصادر خلال عام 2012 م خلاف ا لما كان عليه الوضع بقانون عام 2006م حيث قام بالنسبة للعقوبات السالبة للحرية بالنص على عقوبة السجن المؤبد في القانون الجديد، وهو الأمر الذي لم يكن موجوداً بالقانون الجديد. وكذلك قيامه بالنص على العقاب على الشروع بنصف عقوبة الجريمة التامة في الجنح بالمادة (40) وهو أيضا ما لم يتم النص عليه بالقانون القديم

4- أما بالنسبة لعقوبة الغرامة فقد كانت لا تزيد بالقانون القديم عن 200–ألف درهم أما بالنسبة للقانون الجديد فقد وصلت قيمتها إلى مبلغ 3 ملايين درهم.

5- وأيضا نص المشرع بالقانون الجديد على اعتبار جرائم تقنية المعلوماتولإيضاح خطورتها على الأمن والمجتمع من الجرائم الماسة بأمن الدولة.

6- وكذلك نص المشرع على اعتبار بعض الأفعال أو السلوكيات أو تكرار القيام بها ظرفاً مشّدداً مما يعني تغليظ العقوبة في حق مرتكبيها.

7- كما أضاف المشرع بالقانون الجديد عقوبة تبعية جديدة بخلاف المصادرة والإغلاق الكلي أو الجزئي للمحل أو الموقع، وهي عقوبة الإبعاد للأجنبي في حال ارتكابه إحدى الأفعال التي تم النص عليها بالقانون الجديد.

8- ونص المشرع أيضا بالقانون الجديد على بعض التدابير الاحترازية بحق مرتكبي إحدى الأفعال التي نص عليها القانون وتمثلت تلك التدابير في (الإشراف، الرقابة، الحرمان، الوضع في مأوى علاجي أو مركز تأهيل).

المطلب الثالث: اتجاه وسياسة المشرع الإماراتي تجاه الجرائم الإلكترونية بالقانون الجديد الصادر 2012م

يمكن إيجاز اتجاه وسياسة المشرع الإماراتي تجاه الجرائم الإلكترونية بالقانونالجديد الصادر عام 2012 م في ضوء ما سبق في الآتي:

1. تجريم الأفعال الخاصة بالجرائم الإرهابية والمعاملات والتجارة الإلكترونية وجرائم الإتجار بالبشر، وتلك المتعلقة بالسياحة والآثار والأسلحة النارية والذخائر والمتفجرات وما يتعلق بالأمن الإلكتروني.

2. إضافة بعض التعاريف الجديدة وهي: (المنشآت المالية والتجارية والاقتصادية، إلكتروني، مواد إباحية الأحداث، العنوان البروتوكولي للشبكة المعلوماتية، سري، الالتقاط، الإساءة).

3. النص على عقوبة السجن المؤبد.

4. النص على العقاب على الشروع بنصف عقوبة الجريمة التامة في الجنح.

5. زيادة قيمة عقوبة الغرامة المالية إلى مبلغ 3 ملايين درهم بالنسبة لبعض

الأفعال والسلوكيات المجرمة بنصوص القانون.

6. اعتبار البعض من الأفعال أو السلوكيات المتعلقة بالجرائم الإلكترونية من

الجرائم الماسة بأمن الدولة.

7. اعتبار أّي جريمة منصوص عليها بالقانون جريمة ماسة بأمن الدولة إذا ارتكبت لحساب أو مصلحة دولة أجنبيه أو جماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة.

8. النص على اعتبار بعض الأفعال أو السلوكيات التقنية من الظروف المشددة التي تستوجب تغليظ العقوبة.

9. النص على عقوبة تبعية جديدة وهي عقوبة الإبعاد للأجنبي في حال ارتكابه إحدى الأفعال أو السلوكيات المجرمة التي نص عليها القانون الجديد وذلك خلاف المصادرة والإغلاق الكلي أو الجزئي للمحل أو الموقع.

10-النص على بعض التدابير الاحترازية بحق مرتكبي الأفعال والسلوكيات المجرمة بالقانون وهي: (الإشراف، الرقابة، الحرمان، الوضع في مأوى علاجي أو مركز تأهيل)، وذلك بخلاف العقوبات الأصلية للجريمة والعقوبات التبعية أو التكميلية لها

11. تخفيف العقوبة أو الإعفاء منها في حال الإبلاغ عن أٍي من الأفعال أو السلوكيات المنصوص عليها قبل الكشف عنها أو للكشف عن مرتكبيها والمساهمة في التوصل إليهم أو القبض عليهم.

رأي الباحث:

مما سبق يتضح أن المشرع الإماراتي كان حريصا منذ البداية وعقب ظهور الجرائمالإلكترونية والتيقن من مخاطرها وأضرارها على الأمن والمجتمع على تجريمها، بل لم يكتف بذلك وقام بمواكبة كافة المتغيرات والمستجدات ذات الصلة بهذا الأمر فسارع إلى تعديل نصوص القانون الصادر عام 2006 م في شأن مكافحة جرائم تقنية المعلومات بالقانون الصادر خلال العام 2012 م. وهو الأمر الذي يدل على حرص دولة الإمارات على تحقيق الأمن والأمان بصفة مستمرة ورصد كافة الظواهر الإجرامية والعمل على الوقاية منها ومكافحتها على كافة الأصعدة المحلية والإقليمية والدولية.

الخاتمة

الحمد لله الذي بنعمته تتم الصالحات، وبشكره تدوم النعم، وباتباع منهجه تزول النقم، والصلاة والسلام علي خير البشر سيدنا محمد الذي أدي الأمانة ونصح الأمة وكشف الغمة، تركنا على المحجة البيضاء ليلها كنهارها لا يزيغ عنها إلا هالك وعلى أصحابه وآل بيته الغر الميامين.

أما بعد، فقد تم لي بحمد الله وتوفيقه الانتهاء من كتابة هذا البحث، ولا أدعي الكمال، فهو لله وحده، وإنما هو جهد متواضع في خدمة ديني وأمتي واثراء للحقائق، فما كان منه صواب وإفادة فمن الله تعالي، وما كان من غفلة أو نسيان أو خطأ فمن نفسي ومن الشيطان.

نتائج البحث:

1. أن الإرهاب في اللغة يدل على الإخافة والتفزيع والترويع، في حين لم يتوصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، مما فتح المجال لاجتهادات واسعة غير موفقة أُضطهدت بسببها الشعوب، وأُنتهكت الحقوق، وخرقت القوانين الدولية تحت ستار دعوى مكافحة الإرهاب.
2. يمكن القول بأن الإرهاب الإلكتروني هو: العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر 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.
3. الشريعة الإسلامية تجرم كافة أنواع الإرهاب الكترونيا كان ام تقليديا.
4. أن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم؛ نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى، مع توفير قدر كبير من السلامة والأمان للإرهابيين.
5. إن اعتماد الدول على وسائل الاتصالات وشبكات المعلومات سيكون عاملاً فاعلاً في فتح المجال أمام الإرهابيين لتحقيق أهدافهم وتدمير منتجات التقنية الحديثة والتي تخدم الإنسانية وتسهل التواصل المعرفي والعلمي والثقافي، ومن هنا فإن المعلومات في هذا القرن عرضة لكافة المخاطر المحتملة من هذا النمط المتجدد من الإرهاب المعاصر، فالإرهاب الإلكتروني يهدف إلى تدمير البنية التحتية المعلوماتية وتعريض المجتمعات العالمية إلى مخاطر غير محتملة وغير متوقعة.
6. اهتمام المشرع الإماراتي باتباع سياسة تشريعية جنائية هدفت الي بيان كافة الأفعال والسلوكيات التي تعد من قبيل الجرائم الإلكترونية مع وضع العقوبات اللازمة حيالها.

7. عدم اختصار المشرع الاماراتي على العقوبات الأصلية لمواجهة الجرائم الالكترونية بل تعد ذلك الي النص على عقوبات تبعية وتكميلية في حال ارتكاب بعض انماطها.

8. أبرز وأهم مظاهر الإرهاب الإلكتروني وأشكاله تتمثل في الآتي: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية، وإنشاء المواقع الإرهابية الإلكترونية، وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والتهديد والترويع الإلكتروني، والتجسس الإلكتروني.

9. تقوم التنظيمات الإرهابية بشن هجمات إلكترونية 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.

ثانياً: التوصيات:

1. ضرورة السعي إلى عقد مؤتمر دولي بإشراف هيئة الأمم المتحدة يتم من خلاله تحديد تعريف الإرهاب، وتحديد خطة عملية دولية لمكافحته بجميع صوره وأشكاله، مع احترام سيادة الدول الأعضاء.

2. التشديد على أن الإرهاب ليس له دين معين أو جنس أو جنسية أو منطقة جغرافية محددة، وفي هذا السياق ينبغي التأكيد على أن أية محاولة لربط الإرهاب بأي دين 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. إعادة النظر في مقررات كليات الشرطة ومعاهد القضاء وكليات القانون بحيث يفرد مقرر مستقل للجرائم المعلوماتية.

4. 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.

5. الدعوة إلى زيادة التعاون على المستوى الوطني والثنائي والإقليمي للتنسيق بين الأجهزة المختصة بمكافحة الإرهاب الإلكتروني، لتبادل الخبرات والتجارب، بما في ذلك التدريب لضمان الفعالية في محاربة الإرهابيين وصلاتهم بالجريمة المنظمة.

6. الدعوة إلى تطوير القوانين والإجراءات الوطنية الجنائية الكفيلة بمنع الإرهابيين من استغلال قوانين اللجوء والهجرة للحصول على ملاذ آمن أو استخدام أراضي الدول كقواعد للتجنيد أو التدريب أو التخطيط أو التحريض أو الانطلاق منها لشن الهجمات الإرهابية الإلكترونية ضد الدول الأخرى.

7. السعي إلى إنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب عبر الشبكات المعلوماتية والأنظمة الإلكترونية وتشجيع قيام اتحادات عربية تسعي للتصدي لجرائم الإرهاب الإلكتروني.

8. التأكيد على أهمية نشر القيم الإنسانية الفاضلة، وإشاعة روح التسامح والتعايش، وحث وسائل الإعلام على الامتناع عن نشر المواد الإعلامية الداعية للتطرف والعنف.

9. التأكيد على أن "المعرفة قوة" ففي ظل غياب عربي شبه كامل عن صناعة المعلومات 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 مخاطر 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 الهشاشة الأصيلة في البنية التحتية للشبكة العالمية للمعلومات، مما يُمهد لهجمات إرهابية ربما تؤدي إلى نتائج كارثية على المجتمعات الدولية والاقتصاد العالمي