الإرهاب الإلكتروني : المفهوم والجهود الدولية والإقليمية لمكافحته

تاريخ إرسال المقال : 2017/03/05 تاريخ قبول المقال للنشر: 2017/04/20

نجيب بن عمر عوينات
المعهد العالي للإعلامية بالكاف بجامعة جندوبة تونس

الملخص :

شهد الفضاء الإلكتروني استخدامات أخرى غير سلمية بإستغلاله ساحة جديدة للصراع الدولى وأخذت تلك الصراعات الإلكترونية تستخدم السبل كافة فى شكل ظاهرة الإرهاب الإلكترونى الذي يمكن تعريفه بكونه "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادرة عن الدول أو الجماعات أو الأفراد عبر الفضاء الإلكتروني ، أو أن يكون هدفاً لذلك العدوان ، بما يؤثر على الاستخدام السلمي له..«

وأمام المخاطر و التهديدات التي يشكلها الإرهاب الإلكتروني سعى المجتمع الدولى إلى دعم الاستخدام السلمي للفضاء الإلكترونى من خلال توضيح الحقوق والواجبات التي تجعل الدول تشعر بإلزامية للتعاون مع غيرها ، وهو ما يتجلى من خلال العديد من الإتفاقيات الدولية والتشريعات الوطنية.

الكلمات المفتاحية : الإرهاب الإلكتروني ، التشريعات الوطنية ، الاتفاقيات الدولية .

Abstract:

Cyberspace witnessed many non-peaceful uses. It's been used as a new arena for international conflicts. All means were used to promote the phenomenon of cyber terrorism. "Aggression, intimidation, moral or physical threat via electronic means emanating from states, groups or individual through cyberspace."

In order to face the threats that cyber terrorism presents the international community attempts to goad the peaceful uses of cyberspace. This happens through clarifying the duties and rights that make Countries feel compulsory to cooperate with each other. This is reflected through several international conventions and national legislation.

مقدمة:

لم يتمكن المجتمع الدولي إلى حد الآن من الاتفاق على تعريف واضح ودقيق لمفهوم الإرهاب نظرا لاختلاف المعايير بين الدول وتباين الرؤى حوله، نظرا لكونه ظاهرة معقدة ومتداخلة[1]، إذ أن غياب تعريف واحد وموحد للإرهاب تتفق عليه معظم البلدان يعد من أبرز العقبات التي تواجه الحدّ من ظاهرة الإرهاب، الذي تتعدد تعاريفه مما أدى إلى عجز منظمة الأمم المتحدة رغم عقود من المناقشة والجدل من تحديد مفهوم جامع ومانع وعالمي يرضي المجموعة الدولية، لأنّ الاختلاف يكمن من جهة في التفريق بين المنظمات الإرهابية وحركات التحرير، ومن ناحية أخرى في الجدل المتعلق بإرهاب الدولة[2].

وسنحاول تعريف الإرهاب لغويا، فكلمة إرهاب في اللغة اللاتينية[3] تعرف تحت تسمية «Terror"، التي يقصد بها الرعب أو الذي يلهم الرهبة، وهي مستمدة من العبارة "terrere"، بمعنى التخويف، وإذا رجعنا إلى اللغة العربية نجد أن عبارة إرهاب مصدرها يعود إلى الفعل رهب، واشتقت منه مفردات أخرى منها رهبة، ورهبانا التي تفي نفس المعنى والذي يدل على الخوف والفزع لقوله تعالى: «يَا بَنِي إِسْرَائِيلَ اذْكُرُوا نِعْمَتِيَ الَّتِي أَنْعَمْتُ عَلَيْكُمْ وَأَوْفُوا بِعَهْدِي أُوفِ بِعَهْدِكُمْ وَإِيَّايَ فَارْهَبُونِ»[4].

وأما اصطلاحا تحدد الموسوعة العالمية أن: «الإرهاب هو الاستعمال المنهجي للعنف لأغراض سياسية، بغية الترهيب والتخويف لإحداث صدمة ليس فقط في الضحايا إنما كذلك عند الرأي العام»[5].

وفي هذا السياق عرّفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937 الإرهاب بأنّه: «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».

وقد وضع وزراء الداخلية والعدل العرب في الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998 تعريفا للإرهاب بأنّه: كل فعل من أفعال العنف أو التهديد أيًا كانت بواعثه وأغراضه يقع تنفيذًا لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو اختلاسها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[6].

وفي الواقع إنّ الإرهاب ظاهرة قديمة، لكنّها صارت في السنوات الأخيرة من أبرز القضايا حضورا في المنابر الدولية. ولعل هناك سمة أساسية تميز العمل الإرهابي وهي التي تدفع إلى تجريمه ومعاقبة مرتكبيه وهي التخويف والترهيب والترويع عن طريق استخدام الوسائل المؤدية إلى ذلك أو عن طريق التهديد باستخدامها أيا كان الغرض من وراء ذلك مادام غرضا غير مشروع من الناحية القانونية[7].

وعلى الرغم من أنّ جوهر الإرهاب يظل واحدا من حيث استخدام العنف أو التهديد باستخدامه من أجل إثارة الخوف والهلع في المجتمع، فإنّ أشكال الإرهاب وأدواته وأساليبه تختلف وتتطور مع مرور الزمن، فقد أدى اتساع نطاق ثورة الاتصالات والتطور التكنولوجي المذهل الذي ألغى الحدود والفواصل الجغرافية بين الدول وبسبب طبيعة شبكة معلومات الإنترنت وانفتاحها غير المحكوم أخلاقياً وسياسياً وثقافياً وقانونياً وتجارياً وصعوبة الرقابة والمساءلة على ما ينشر فيها، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة الإرهاب الالكتروني والتي أخذت أشكال حديثة تتماشى مع التطور التقني[8].

وقد أصبح الإرهاب عبر شبكة الإنترنت بيئة مناسبة للممارسات الإرهابية ونشر الأفكار المتطرفة التي تسيطر على وجدان الأفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض ومصلحة المجتمع أو القيام بأعمال تخريبية بشكل يخفي هويتهم المباشرة وبشكل بسيط، ففي حين يحتاج الإرهاب الفعلي إلى أسلحة ومدرعات وقنابل وتحركات سرية جداً قد تصيب أو تخفق ناهيك عن التكاليف المادية لإنجاح هذه العمليات، لا يحتاج الإرهاب الإلكتروني سوى إلى بعض المعلومات ليستطيع اقتحام الحواجز الإلكترونية، كما أن تكاليف القيام بهذه الهجمات لا تتجاوز جهاز حاسوب والدخول إلى الشبكة العنكبوتية.

إن خطر الإرهاب الإلكتروني يكمن في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله، أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق.

إن الشبكة العالمية فتحت مجالا حيويا للأنشطة التي تقودها الجماعات الإرهابية، إذ بات مؤكدا اليوم العلاقة الوطيدة بين الإرهاب واستخدام الوسائل التكنولوجية بهدف زعزعة استقرار وأمن المجتمعات والدول، فالجريمة الإرهابية بعدما كانت محلية محضة تحولت لتصبح عابرة للحدود[9]، وإذ لم يكن هناك قلق في السابق مع بدايات شبكة الإنترنت من جرائم يمكن أن ترتكب عليها أو بواسطتها ليست لكونها آمنة في تصميمها وبناءها، بل نظرا لمحدودية مستخدميها، علاوة على كونها كانت مقصورة على فئة معينة من المستخدمين – الباحثين ومنتسبي الجامعات-إلا أنه ومع توسع استخدامها ودخول جميع فئات المجتمع إلى قائمة مستخدميها بدأت تظهر على الوجود ما يسمى بالجرائم المعلوماتية على الشبكة[10] أو بواسطتها، جرائم تتميز بحداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها. ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود، وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود أي أنها ذات طبيعة عالمية.

نحاول من خلال هذه الورقة البحثية التطرق لمفهوم الإرهاب الإلكتروني من ناحية أنواعها وأشكاله والمجالات التي يستهدفها إضافة إلى الجهود الدولية لمكافحته وفي ختامها المقال

سنورد بعض التوصيات التي من تساعد في التصدي للإرهاب الإلكتروني والحد من انتشاره وتفشيه.

المبحث الأول : تعريف الإرهاب الإلكتروني وبيان خطورته

ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب، ولا يختلف الإرهاب الإلكتروني عن الإرهاب العام إلا في نوعية الأداة المستخدمة لتحقيق الغرض الإرهابي، فالإرهاب الإلكتروني يعتمد على استغلال الإمكانيات العلمية والتقنية، واستخدام وسائل الاتصال والإنترنت، من أجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم.

المطلب الأول : تعريف الإرهاب الإلكتروني

يتألف مصطلح «الإرهاب الإلكتروني» أو (Cyber terrorism) من كلمتين، كلمة مألوفة (Cyber)ومتداولة وتعني الإنترنت، والكلمة الأخرى (Terrorism) وتعني الإرهاب والتي، حتى الآن لم تعرّف تعريفاً محدداً.

ونسوق بعض التعاريف التي أعطيت للإرهاب الإلكتروني، والتي تتميز في معظمها بتشابه العناصر التأسيسية المكونة له، وبوحدة الأهداف التي يسعى لتحقيقها، وكذا الخلفيات التي تحركه، فالإرهاب الإلكتروني:

1- هو كل فعل يقع تنفيذا لغرض إرهابي، يهدف إلى تخريب أو إتلاف النظم المعلوماتية داخل الدولة، بغرض زعزعة استقرارها أو الضغط على حكومتها السياسية لتحقيق مطالب معينة.

2- هو استخدام الموارد المعلوماتية المتمثلة في شبكات المعلومات وأجهزة الكمبيوتر والإنترنت من أجل التخويف أو التهديد أو الإرغام لأغراض سياسية.

ويعرّفه كذلك باري كولينز (Barry Collins) بأنه " سوء الاستخدام القصدي لنظام المعلومات الرقمي والشبكات، أو مكوناتها لتحقيق هدف يدعم أو يشمل حملة إرهابية أو فعل إرهابي"[11].

ويمكن تعريف الإرهاب الإلكتروني بأنّه النشاط غير القانوني الذي يقوم به طرف ما بوساطة التقنية الإلكترونية الرقمية عبر شبكاتها لتحقيق غرض محدد[12].

ويمكن تعريف الإرهاب الإلكتروني كذلك بأنه «نشاط أو هجوم متعمّد بدوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام العالمي، ويستخدم الفضاء الإلكتروني بوصفه عاملاً مساعداً ووسيطاً في عملية التنفيذ للعمل الإرهابي، كما يسعى لإحداث تأثير معنوي ونفسي عبر التحريض على بث الكراهية ويأتي هذا العمل في صورة رقميّة عبر استخدام آليات الأسلحة الإلكترونية الجديدة في معارك تدور رحاها في الفضاء الإلكتروني، وقد يقتصر

تأثيرها على بعدها الرقمي، أو تتعداه لتصل إلى الإضرار بأهداف مادية تتعلق بالبنية التحتية الحيويّة.

ويمكن شرح مفهوم "الإرهاب الإلكتروني" بأنّه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، باستخدام الموارد المعلوماتية والوسائل الإلكترونية.

ويمكن من خلال كل هذه التعريفات السابقة تعريف «الإرهاب الإلكتروني» بأنّه «هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. ولكي يعتبر المرء إرهابياً على الإنترنت، وليس فقط مخترقاً، فإن الهجمات التي يشنها يجب أن تؤدي إلى عنف ضد الأشخاص أو الممتلكات، أو على الأقل تحدث أذى كافياً من أجل نشر الخوف والرعب.

والملاحظ بخصوص هذه التعريفات السابقة هو الارتباط الوثيق للإرهاب المعلوماتي بالمستوى المتقدم الذي باتت تكنولوجيا المعلومات تلعبه في كافة مناحي الحياة، فضلا عن حجم المخاطر التي يمكن أن يسببها والتي قد تلحق الشلل التام بأنظمة القيادة وتؤدي إلى قطع شبكات الاتصال بين الوحدات والقيادات المركزية، وتعطيل أنظمة الدفاع الجوي أو اختراق النظام المصرفي أو إرباك حركة الطيران المدني أو غيرها[13].

لقد ظهر الارتباط بين الإنترنت والإرهاب بشكل واضح بعد أحداث الحادي عشر من سبتمبر 2001، وانتقلت المواجهة ضد الإرهاب والإرهابيين من المواجهة المادية المباشرة إلى المواجهة الإلكترونية وتحولت الحروب الواقعية إلى حروب رقمية، وأصبح الإنترنت من أشد الأسلحة فتكاً وهدماً إذا ما أستُخدم لأغراض سيئة وتحقيق نوايا إرهابية، ويمكن تصنيف الإرهاب الإلكتروني كنوع من أنواع الجرائم الإلكترونية إذا ما اقتُرفت تحقيقاً لأغراض إرهابية، مثلما ما حصل في العام 2000، حينما أدى انتشار فيروس الحاسوب

«I love you" إلى إتلاف معلومات قدرت قيمتها بنحو 10 مليارات دولار أمريكي، وفي العام 2003، أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسوب. وقدّر "مجلس أوروبا في الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت" كلفة إصلاح الأضرار التي تسببها فيروسات المعلوماتية بنحو 12 مليار دولار أمريكي سنوياً.

ومع ذلك، فليس هناك حتى الآن مفهوم دولي مُوحَّد للإرهاب بصفةٍ عامة، والإرهابِ الإلكتروني بصفةٍ خاصة، وليس هناك جهود واضحة حتى الآن لوضع تشريعات داخلية صارمة لِمُكَافحة الجرائم التي تتعلَّق بالإرهاب الإلكتروني، فمنظمة الأمم المتحدة لم تعالج حتى الآن أية حالة يمكن الاستناد إليها في تعريف الإرهاب الإلكتروني وإمكانية التعامل معه من الناحية القانونية، فالقانون الدولي لم يعطِ تعريفاً واضحاً، ومنهجاً معيناً للتعامل مع هذا النوع

الجديد من الإرهاب الذي يمكن اعتباره أداة إرهابية مؤذية جداً، فمع غزو الإنترنت دول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظرا لكونها عابرة للحدود لا دين ولا وطن لها، وتتم بسرعة فائقة دودن رقابة من أي دولة مما جعل من الإرهاب الإلكتروني بإرهاب المستقبل الذي أصبح هاجسا حقيقيا يهدّد سلامة وأمن المجتمع الدولي، عن طريق التهديد بتدمير أساليب وإستراتيجية الدفاعات الأمنية والاقتصادية للدول وعوائدها المالية باستخدام الخطط التخريبية والفيروسات لتدمير مختلف البرامج المعلوماتية وإتلاف مختلف البيانات الخاصة بتقنية الرقمية في حفظ وتخزين البرامج المعلوماتية لأية دولة ومهما كانت درجة سريتها.

المطلب الثاني : الإرهاب الإلكتروني الخطر القادم

لقد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، والذي يمثل تهديدا على المصالح الاستراتيجية والحيوية، إذ يمكن أن تتسبب هجمات إلكترونية إرهابية في خسائر فادحة حيث يمكنها إعاقة حركة الملاحة البحرية والجوية وتعطيل الاتصالات الدولية والإضرار بالمؤسسات المصرفية.

وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضرارًا جسيمة على الأفراد والمنظمات والدول، إذ إن المواقع الإلكترونية المشبوهة أو «الإرهابية الهدف» في ازدياد مضطرد منذ العام 2001، والتي فاقت أعدادها 17 ألف موقع إلكتروني، فقد هيمن الذعر على المختصين بمكافحة «الإرهاب الإلكتروني» حين تمكن أحد القراصنة من السيطرة على نظام الكمبيوتر في مطار أمريكي صغير، وأطفأ مصابيح إضاءة ممرات الهبوط، ما هدد بحصول كارثة. وتعززت المخاوف حين زادت التهديدات بالهجمات ذات الدوافع السياسية، وخصوصاً بعد ظهور مصطلح «الجهاد الإلكتروني»، الذي تبنته جماعات عدة بغرض ضرب مصالح إلكترونية لدول مثل الولايات المتحدة، وإسرائيل، وبريطانيا، وغيرها.

ولم يقتصر الأمر على هذه الدول فقط؛ إذ بدا أن حجم التهديدات الإرهابية الإلكترونية يتزايد تلقائياً مع كل توسع وانتشار في استخدام تكنولوجيا المعلومات في مناطق العالم المختلفة، كما يبدو أن ممارسة أنشطة «الإرهاب الإلكتروني» لا تقتصر على إقليم محدد كما لا تستهدف دولاً معينة.

إن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسب الآلية والشبكات المعلوماتية، مما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة

والاتصالات، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية[14].

وتتركز المخاوف من هجمات "الإرهاب الإلكتروني" في عدد من السيناريوهات منها: تطوير فيروس يمّكن من السيطرة على أجهزة الهواتف في مجتمع ما، وجعلها تتصل كلها في وقت واحد برقم الطوارئ لشل عمل خدمة الطوارئ. وتزيد فداحة الخسائر في حال ترافق مع هذا الشلل تفجير قنبلة في سوق أو مبنى. كما يمكن توليد برنامج يمّكن من قطع التيار الكهربائي لفترة طويلة، أو السيطرة على نظام المراقبة الجوية وتوجيه الطائرات في أحد المطارات، بحيث تتصادم وتتحطم دون الحاجة إلى إرهابيين على متنها.

ويعترف الخبراء الأمنيون المتخصصون بمكافحة الجرائم الإلكترونية بأن "الهجمات التي شنت حتى الآن غير معقدة إلى حد ما، غير أن ما تظهره عمليات المحاكاة من احتمالات شن هجمات أكثر اتساعاً وتنظيماً أمر يدعو للخوف ".

ويعتقد المتخصصون في مجالات مكافحة الإرهاب أن الخسائر الناجمة عن العمليات العديدة التي يشهدها العالم يومياً في إطار ما يعرف بـ "الإرهاب الإلكتروني"، تعد "هامشية وضئيلة جداً"، إذا ما قورنت بما يمكن أن يحدثه هجوم إرهابي إلكتروني على نطاق واسع ومخطط جيداً...

وتأسيساً على ما سبق يمكننا القول بأن الإرهاب الإلكتروني يرتبط بالتطورات التي تحدث في مجتمع المعلومات، فهو يزداد خطورةً وفتكاً كلما زاد التقدم في المجال المعلوماتي، فالاكتشاف والتطور والبناء حتماً يقابله التجسس والتخلف والهدم، فالدمار الذي قد يلحقه الهجوم الإرهابي بأنظمة المعلومات التي تتحكم في كل مرافق الحياة في هذه المجتمعات التي تعتمد على الكمبيوتر والإنترنت اعتماداً مطلقاً قد يعطل حياة مجتمع بأكملها، والخسائر التي قد تنجم عن مثل هذا الهجوم هي أكبر بكثير مما قد يتصوره العقل إذا لم يدرس ويخطط لوقوعه.

ومما لا شك فيه أن الإرهاب الإلكتروني هو إرهاب الغد، نظراً لتوسع وتنوع أهدافه وتنوع المجالات المستهدفة من قبلهم والتي يمكن الاعتداء عليها مع توفير قدر كبير من السلامة للمعتدي وصرف جهد قليل وعدم التعرض لخطر اكتشاف هويته إلا بعد عناء ووقت طويل في البحث والتقصي.

المبحث الثاني : التعاون الدولي لمكافحة الإرهاب الإلكتروني

في عالم مزدحم بشبكات اتصال دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية متباعدة بإستخدام تقنيات لا تكفل للمعلومات أمنًا كاملًا، يتاح في ظلها التلاعب عبر الحدود بالبيانات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أضرارًا فادحة، يغدو التعاون

الدولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات أمرًا ضروريا، وإزاء ذلك كان لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات . وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها ولمعاقبة مرتكبيه، ولهذا سوف نتناول بالدراسة التعاون الدولي في مجال مكافحة الإرهاب الإلكتروني من خلال الجهود الدولية في هذا المجال، (المطلب الأول) مع دراسة التجارب العربية في مجال مكافحة الإرهاب الإلكتروني «(المطلب الثاني).

المطلب الأول : الجهود الدولية في مجال مكافحة الإرهاب الإلكتروني

في بداية التسعينات من القرن العشرين عقد مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين المنعقد في هافانا بكوبا، الذي أكد في قراره رقم 45_121 الصادر في 14 ديسمبر 1990 المتعلق بالجرائم ذات الصلة بالحاسب الآلي أن الدول الأعضاء مطالبة بتكثيف جهودها كي تكافح بمزيد من الفعالية عمليات إساءة استعمال الحاسب الآلي التي تستدعي تطبيق جزاءات جنائية على الصعيد الوطني، بما في ذلك النظر إذا دعت الضرورة في:

أ. تحديث الأنظمة والإجراءات الجنائية بما في ذلك اتخاذ تدابير من أجل ضمان أن تكون الجزاءات بشأن سلطات التحقيق وقبول الأدلة على نحو ملائم.

ب. النص على جرائم وجزاءات وإجراءات تتعلق بالتحقيق والأدلة، للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي[15].

كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالإرهاب الإلكتروني، بما في ذلك دخولها حسب الاقتضاء أطرافًا في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة الخاصة المرتبطة بالجرائم ذات الصلة بالحاسب الآلي، وفتح آفاق جديدة للتعاون الدولي في هذا المضمار ولاسيما فيما يتعلق بوضع أو تطوير ما يلي:

أ. معايير دولية لأمن المعالجة الآلية للبيانات.

ب. تدابير ملائمة لحل مشكلات الإختصاص القضائي التي تثيرها الجرائم المعلوماتية العابرة للحدود، أو ذات الطبيعة الدولية.

ت. اتفاقيات دولية تنطوي على نصوص تنظيم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية في الوقت نفسه لحقوق الأفراد والدول[16].

أما منظمة الإنتربول فقد واصلت جهودها في مجال مكافحة جرائم الحاسب والانترنت

وأنشأت لذلك وحدة متخصصة في جرائم الانترنت تحديدا وشكلت فرق عمل بدأت في أوروبا عام 1990 وفي مختلف الدول لبحث ورصد جرائم التقنية ومن ضمنها الإرهاب الإلكتروني.

وفي منتصف التسعينات من القرن العشرين، حيث قام الرئيس الأمريكي بيل كلينتون في عام 1996 بتشكيل لجنة حماية منشآت البنية التحتية الحساسة.وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات، إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة الأمريكية.

وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة الأمريكية بإنشاء هيئاتها ومراكزها الخاصة للتعامل مع احتمالات الإرهاب الإلكتروني، فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفاً من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني[17].

وقد قررت الدول الثماني الكبار إقامة نقطة مراقبة دائمة للإنترنت تعمل على مدار 24 ساعة تقوم بإعطاء إنذار بمجرد تسرب أحد القراصنة إلى الشبكة وبمجرد إطلاق صفارة الإنذاريتحرك على الفور نخبة من خيرة الأخصائيين في عالم الإنترنت لتحديد مكان المشتبه فيه بإتباع أثره الإلكتروني وفقاً لمجال نشاطه الإجرامي.

وفي شهر أكتوبر 1999 اجتمع في موسكو وزراء العدل والداخلية للدول الثماني الكبار وطلبوا من ممثليهم وضع خيارات وحلول عملية تسمح بكشف ومتابعة الإتصالات الإلكترونية الدولية في إطار التحقيقات الجنائية. وقد صدر عنهم التصريح التالي:« بغية التأكيد من أننا جميعا نستطيع أن نحدد مكان وهوية المجرمين الذين يستخدمون الإتصالات الالكترونية لأهداف غير مشروعة، يجب علينا أن نزيد قدراتنا على إقتفاء أثر وكشف هذه الاتصالات الإلكترونية لأهداف غير مشروعة، يجب علينا أن نزيد قدراتنا على اقتفاء أثر وكشف هذه الاتصالات أثناء وبعد إجرائها حتى وإن كانت تلك الاتصالات تمر عبر عدة دول، ولما كانت الإجراءات الحالية تتسم بالبطء وتتم في إطار تعاون ثنائي فقط بدلا من أن تهدف إلى مواجهة الجرائم بصفة مطلقة، لذلك يجب أن يتعاون الجميع مباشرة من أجل مكافحتها وإيجاد حلول سريعة وحديثة ».[18]

وفي 12 أفريل 2000 تم نوقيع إتفاقية منظمة مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية بإشراف منظمة الأمم المتحدة التي أكدت في مادتها الأولى على أنّه:« ينبغي للدول أن تكفل عدم توفير قوانينها وممارساتها ملاذا آمنا للذين يسيئون إستعمال تكنولوجيا المعلومات لأغراض إجرامية».

كما توجت الجهود التي بذلها الإتحاد الأوروبي والمجلس الأوروبي بصدور إتفاقية

بودابست لمكافحة الجرائم المعلوماتية (الجرائم الإلكترونية) وتعرف بالاتفاقية الأوربية لمكافحة الجريمة المعلوماتية[19].

ووضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في 11/23/ 2001 ودخلت حيز التنفيذ في 2004 [20]، وتعتبر الاتفاقية متاحة أمام أية دولة من دول العالم للانضمام إليها.

واشتملت الاتفاقية على 48 مادة موزعة على أربعة فصول. تناول الفصل الأول تعريف المصطلحات المستخدمة وتناول الفصل الثاني الإجراءات الواجب اتخاذها على المستوى المحلي في مجال قانون العقوبات والإجراءات الجنائية وقواعد الاختصاص القضائي، ويهدف الفصل الثالث إلى تنظيم التعاون الدولي، ويضم الفصل الرابع والأخير الشروط الختامية.

وفي إطار هذا التعاون نصت الاتفاقية على أن: «تتفق الأطراف على أوسع نطاق للتعاون بهدف إجراء التحقيقات أو الإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية وجمع الأدلة في الشكل الالكتروني لهذه الجرائم » . كما أنه يمكن لكل طرف في الحالات الطارئة أن يوجه طلبا للمعاونة أو للاتصالات المتعلقة بها عن طريق وسائل الاتصال السريع مثل الفاكس أو البريد الالكتروني على أن تستوفي تأكيد رسمي لاحق إذا اقتضت الدولة المطلوب منها المساعدة في ذلك.

وعقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية بالبرازيل ما بين 12-19 أفريل 2010 حيث ناقشت فيه الدول الأعضاء بتعمق مختلف التطورات في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، حيث أحتل هذا النوع من الجرائم موقعا بارزا على جدول أعمال المؤتمر وذلك تأكيدا على خطورتها والتحديات التي تطرحها[21].

وفي إعلان قمة شيكاغو في اجتماع مجلس شمال الأطلسي في 20 ماي 2012 تم التأكيد على ضرورة دمج إجراءات الدفاع الإلكتروني في هياكل وإجراءات الحلف، مع الالتزام بتحديد وتوفير قدرات الدفاع الإلكتروني الوطنية التي تعزز التعاون والعمليات المشتركة بين دول الحلف، بالإضافية إلى تطوير قدرات الدول الأعضاء بصورة أكبر لمنع الهجمات الإلكترونية وإكتشافها والتصدي لها ومعالجة التهديدات الأمنية الإلكترونية بالإشتراك مع الدول الشريكة المعنية في إطار كل حالة بمفردها، وكذلك مع المنظمات الدولية، ومن بينها الاتحاد الأوروبي -على النحو المتفق عليه-ومجلس أوروبا والأمم المتحدة ومنظمة الأمن والتعاون في أوروبا من أجل زيادة التعاون الملموس.

وعلى مستوى دول العالم ومع مواكبة التطور الهائل لتقنية المعلومات سنت أنظمة لضبط التعاملات الإلكترونية، وتضمنت تلك الأنظمة عقوبات للمخالفين في التعاملات الإلكترونية ففي ماليزيا صدر نظام في عام 1997م للمخالفات الإلكترونية، وقد صنف

المخالفات إلى: الوصول غير المشروع إلى الحاسب الآلي والدخول بنية التخريب أو التعديل غير المسموح به وتتراوح العقوبات المحددة بين غرامات مالية تصل إلى 150.000دولار ماليزي مع السجن مدة تصل إلى عشر سنوات[22].

وفي فرنسا يعد قانون جون فران God rain الذي صدربتاريخ 5 يناير1988 من القوانين التي تدخلت مبكراً في هذا المجال وهو نموذج للتجديد التشريعي الذي يمكن تطبيقه بسهولة ويسر لمكافحة الجرائم التقليدية والحديثة الخاصة بالمعلومات مثل الفيروسات والقنابل bombe logique كما يعاقب على الجرائم المسماة حصان طروادة، وبرامج التجسس التي من شأنها ملاحظة موقع ما أو شبكة معلومات.

كما وضعت الحكومة البريطانية خططا للتصدي للإرهاب الإلكتروني قدرت تكلفتها بحوالي 500 مليون جنيه إسترليني، ولا يعتبر هذا المبلغ كبيرا قياسا على ما سيوفره من خسائر قد تنتج من ولوج الأشخاص إلى مواقع تهدف إلى نشر ثقافة إرهابية.

كما تبحث الحكومة الألمانية حاليا سبل تشديد القوانين الأمنية في البلاد وذلك في إطار مشروع قانون جديد تقدمت به وزيرة العدل الألمانية بريجيته تسيبريز بالتنسيق مع الوزارات الألمانية المعنية في خطوة جديدة تهدف إلى التصدي لخطر الإرهاب بكل أنواعه وخاصة في الشبكة العنكبوتية.

وعن محتوى مشروع القانون الجديد أفادت تسيبريز أن هذا القانون يهدف إلى تشديد العقوبات الجنائية على كل من يقوم بعمليات إعداد وتجهيز متعلقة بجرائم عنف إرهابية خطيرة. وينص القانون الجديد على معاقبة مرتكبي جرائم العنف، حتى الذين لا ينتمون إلى تنظيمات إرهابية، كما سيفرض القانون عقوبات جنائية قد تصل إلى السجن لمدة ثلاث سنوات على من يقوم بنشر إرشادات لتعليم صناعة القنابل على الإنترنت أو يقوم بتحميل مثل تلك الإرشادات على الكمبيوتر الخاص به. وعلاوة على ذلك سيفرض القانون الجديد أيضا عقوبات جنائية قد تصل إلى السجن لمدة ثلاث سنوات على من يتصل بتنظيمات "إرهابية" بهدف تلقى تدريبات داخل أحد معسكراتها على سبيل المثال.

وتهدف كل هذه الجهود إلى التعاون بين جميع الدول لمواجهة هذا التحدي وزيادة القدرة لجميع الحكومات للقضاء على الحركات الإرهابية والأنشطة الإجرامية التي تستخدم تقنية عالية على المستوى الدولي.

المطلب الثاني : التجارب العربية في مجال مكافحة الإرهاب الإلكتروني

في العالم العربي توجد بعض التشريعات التي تغطي جرائم المعلوماتية والحاسب بشكل أو بآخر خاصة في تونس والمغرب والمملكة العربية السعودية والأردن والإمارات العربية المتحدة وعمان وقطر.

ولقد حققت دول مجلس التعاون لدول الخليج العربية تقدماً ملحوظاً في مجال

استخدامات تكنولوجيا المعلومات، وحظيت دولة الإمارات العربية المتحدة خصوصاً بموقع ريادي في هذا المجال. وقد استدعى هذا التقدم اتساعاً في الثغرات التي تمّكن "الإرهابيين الإلكترونيين " من شن هجماتهم، وهو الأمر الذي حدا بخبراء دوليين إلى اعتبار أن "حكومات دول الخليج العربي عرضة لمخاطر كبيرة من الإرهاب الإلكتروني عبر الإنترنت"، مشيرين إلى أن "هذه المخاطر تتفاقم مع مرور الأيام لأن التقنية وحدها غير قادرة على حماية بيانات الحكومات بشكل كلي من الهجمات المتوقعة".

وتعتبر دولة الإمارات العربية أول دولة عربية تسن قانونًا مستقلًّا لمكافحة الجرائم المعلوماتية، وفي هذا السياق تنص المادة 21 من القانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات على أنّه: « كل من أنشأ موقعاً أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أية أدوات تستخدم في الأعمال الإرهابية، يعاقب بالحبس مدة لا تزيد على خمس سنوات »[23].

وتجدر الإشارة إلى أن المشرع الإماراتي قد نص صلب المادة 7 من قانون قم (1) لسنة 2004 بشأن مكافحة الجرائم الإرهابية على معاقبة كل من يقوم بتدريب شخصا أو أكثر على استعمال الأسلحة التقليدية أو غير التقليدية أو وسائل الاتصال السلكية أو اللاسلكية أو الالكترونية أو أية وسيلة اتصال أخرى أو علمه فنونا حربية أو أساليب قتالية أيا كانت، بقصد الاستعانة به لتنفيذ عمل إرهابي بالسجن المؤبد أو المؤقت.

ولقد صدرت في المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء رقم (163) في 24 -10 -1417هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها[24].

كما نص القرار على تكوين لجنة دائمة برئاسة وزارة الداخلية وعضوية وزارات : الدفاع، والمالية ، والثقافة والإعلام ، والاتصالات وتقنية المعلومات ، والتجارة ، والشؤون الإسلامية، والتخطيط ، والتعليم العالي ، والتربية والتعليم ، ورئاسة الاستخبارات ، ومدينة الملك عبد العزيز للعلوم والتقنية، وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام (الإنترنت) والتنسيق فيما يخص الجهات التي يراد حجبها، ولها على الأخص ما يأتي :

أ. الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للإنترنت والتي تتنافى مع الدين الحنيف والأنظمة.

ب. التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.

وهذا القراريبين مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطها.

كما تم إصدار أنظمة تحد من جرائم الإرهاب الإلكتروني وفي هذا السياق تم إقرار نظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم م/ 17 وتاريخ: 3/8/ 1428 هـ بناءً على قرار مجلس الوزراء رقم: (79) وتاريخ: 3/7/ 1428هـ[25] الذي فرض عقوبات بالسجن أو الغرامة أو كليهما معا على كل شخص ينشئ موقعا لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أو نشر كيفية صنع المتفجرات[26]، وفي هذا السياق تنص المادة السابعة من هذا القانون على أنّه» يعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين كل شخص يقوم بإنشاء موقع منظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات الأجهزة الحارقة أو المتفجرات أو أداة تستخدم في الأعمال الإرهابية » .

وفي المغرب فقد تفطن المشرع المغربي لخطورة انتشار الإجرام المعلوماتي وأثر ذلك على أمن واستقرار المجتمع المغربي، وقد ظهر ذلك مع عرض مشروع القانون المتعلق بالإرهاب على مجلس الوزراء بتاريخ 16 جانفي 2003[27]، حيث وردت لأول مرة الإشارة إلى إمكانية ارتكاب أفعال إجرامية إرهابية عن طريق المعالجة الآلية للمعطيات[28].

وما يلفت النظر هو أن القانون المغربي رقم 03 -03 المتعلق بالإرهاب يعد أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المساس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف، فالفصل 1-218 حدد بعض الأفعال المجرمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات الفقرة 7[29]، وذلك بعد محاولة تحديد مفهوم الإرهاب في مستهل هذا الفصل.

ومما تجدر الإشارة إليه عند الحديث عن القانون المغربي رقم 03-03 المتعلق بمكافحة الإرهاب أن الفصل 2-218 منه عاقب على استعمال وسائل الإعلام ومنها الإلكترونية في الإشادة بالأعمال الإرهابية، وقد حدد الفصل المذكور العقوبة في الحبس من سنتين الى ست سنوات وبغرامة بين 10 ألاف و200 ألف درهم[30]، ومعلوم أن وسائل الإعلام الإلكترونية متعددة من أبرزها الشبكة الدولية للمعلومات-الانترنت-.

وفي السودان صدر قانون جرائم المعلوماتية لسنة 2007 الذي نص في الفصل الخامس منه على أنّه :« كل من ينشئ أو ينشر أو يستخدم موقعاً على شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها لجماعة إرهابيه تحت أي مسمي لتسهيل الاتصال بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع المواد الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن مدة لا تتجاوز سبع سنوات أو بالغرامة

أو بالعقوبتين معاً » .

أما المشرع الأردني فقد نص صلب المادة 10 من قانون جرائم أنظمة المعلومات لسنة 2010 على أنّ: « كل من استخدم نظام المعلومات أو الشبكة المعلوماتية أو أنشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها، أو تمويلها يعاقب بالأشغال الشاقة المؤقتة ».

أما في قطر فقد صدر القانون رقم 14 لسنة 2014 المتعلق بمكافحة الجرائم الإلكترونية الذي نص صلب المادة 5 منه على أن: "يعاقب القانون بالحبس مدة لا تتجاوز ثلاث سنوات والغرامة 500 ألف ريال لإدارة موقع يتبع "تنظيماً إرهابياً"، أو نشر أخبار تعرض الدولة للخطر أو "ترويج الأخبار الكاذبة ضد سلامة الدولة"، أو تسهيل الاتصال بقادة وأعضاء الجماعات الإرهابية أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أي أداة تستخدم في الأعمال الإرهابية".

الخاتمة:

يمكن القول مما سبق:

- 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.
- أنّ الإرهاب الإلكتروني هو إرهاب المستقبل نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها بعيدا عن الإزعاج والفوضى، مع توفير قدر كبير من السلامة والأمان للإرهابيين.
- إن أسباب الإرهاب الإلكتروني ودوافعه متعددة ومتنوعة، وهي عينها أسباب ظاهرة الإرهاب عموماً، وذلك لأن الإرهاب الإلكتروني يعتبر نوعاً من أنواع الإرهاب وشكلاً من أشكاله، كما أن هناك عوامل عديدة تجعل من ظاهرة الإرهاب الإلكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الإرهابية.
- قد أصبح الإرهاب الإلكتروني هاجسا يخيف العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضرارًا جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير الضرورية لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا نزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.
- على الرغم من إدراك أهمية وجود وتطبيق أحكام وأنظمة لضبط التعاملات الإلكترونية

والتي تعتبروسيلة من وسائل مكافحة الإرهاب الإلكتروني، فإن الجهود المبذولة لدراسة وتنظيم ومتابعة الالتزام بتلك الأحكام لا يزال في مراحله الأولية، وما تم في هذا الشأن لا يتجاوز مجموعة من القرارات والاتفاقيات التي لا تستوعب القضايا المستجدة في أعمال تقنية المعلومات كما لا توجد بصورة منظمة ومعلنة أقسام أمنية، ومحاكم مختصة، ومنتجات إعلامية لشرائح المجتمع المختلفة.

- أن عدم وجود اتفاق دوليّ واضح في التعامل مع ظاهرة الفضاء الإلكتروني وتنظيم استخدامها وتحديد الحقوق والواجبات، قد يجعل الدول لا تشعر بأي إلزام في التعاون مع غيرها مما يشكّل جزءاً مهمّاً من تعقّد المشكلة، نظرا لمساهمته في تعثر معرفة الهجمات الإلكترونيّة ومصدرها ومواجهتها.

التوصيات و المقترحات :

1- تفعيل دور المكافحة الوقائية التي تسبق وقوع الإرهاب الإلكتروني، وذلك من خلال تفعيل دَور المؤسسات التوعويَّة (المسجد، الأسرة، دُور التعليم، أجهزة الإعلام) بالتوعية بخطورته، والسعي في تقوية الوازع الديني[31]، بالإضافة إلى التأكيد على أهمية دور وسائل الإعلام والمؤسسات المدنية ونظم التعليم في بلورة إستراتيجيات 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.

2- التنسيق وتوحيد الجهود بين الجهات المختلفة: التشريعيّة، والقضائيّة، والضبطية، والفنية، وذلك من أجل سد منافذ الإرهاب الإلكتروني قدر المستطاع،و تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الإلكترونية، وتوفير التقنيات اللازمة لمواجهتها، عبر تطوير أمن شبكات الحاسب بإستخدام أنظمة التشفير المتقدمة و"الجدران النارية" في الشبكات، وأنظمة اكتشاف المخترقين عالية الدقة، والبرامج المضادة للفيروسات، والدعوة 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. وفي تقرير لمجلس الدولة الفرنسي عن الإنترنت والشبكات الرقمية في سبتمبر 1997 قالت إيزابيل فالك23 «نحن لا نوجد في فراغ تشريعي بالنسبة للإنترنت ولا أوافق من ينادي أو يطالب بقانون خاص بشبكات المعلومات لأننا لدينا العديد من التشريعات التي يمكن تطبيقها على كل حالة على حدة، خصوصاً وأننا أمام مجال يتبخر كل شيء فيه ويتطاير، ويصعب تطبيق العقوبة. وبالتالي يجب تصور وضع آلية تضم المؤسسات العامة والأفراد وأن يتعاون الجميع لتطبيق قواعد القانون في تلك البيئة الجديدة مع تأكيد الإحترام اللازم لإستخدام الشبكات.فنحن نمتلك ترسانات من العقوبات لكنها لا تؤدي إلى شيء وذلك لصعوبة تطبيقها ما لم تتضافر القوى العامة والخاصة. كما أن المدى العالمي الذي

تتميز به شبكة الإنترنت يستلزم تضافر كل الدول، بينما لا توجد رؤية موحدة بين دول العالم.

3- كما أشار التقرير إلى أهمية تفعيل وتقوية دور الشرطة والقضاء في مجال الإنترنت حيث جاء فيه: «أن الاقتناع بالقانون لا يتأتى إلا إذا تم احترامه، ولذلك يجب العمل على تطبيقه. ولكي يطبق القانون بصفة فاعله يجب تقوية وسائل الشرطة والعدالة».

4- إنشاء قانون دولي مُوَحَّد، ومحاكم خاصَّة دوليَّة محايدة تتولَّى التحقيق في الإرهاب الإلكتروني، ويكون لها سلطة الأمر بضبط وإحضار المجرم الإلكتروني للتحقيق معه أيًّا كان موقع هذا المجرم وبلده، وهذا الاقتراح أو التوصية تتناسب مع مقام الإرهاب الإلكتروني الذي تمثَّل الكرة الأرضيَّة أمامه قرية صغيرة واحدةً قريبة المدى متقاربة الأطراف.

5- عقد الإتفاقيات بين الدول بخصوص الإرهاب الإلكتروني وقايةً وعلاجاً وتبادلاً للمعلومات والأدلة،وحث الدول إلى الإسراع والانضمام إلي الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.. لا شك أن مطوري تكنولوجيا المعلومات وخبراء الإنترنت مطالبون بملاحقة أنشطتهم التوسعية بأنشطة حماية وسد ثغرات لحماية هذا الفضاء الحيوي من أن يصبح ساحة إرهاب دامية33. ويجب أن يهتم المجتمع الدولي بإبرام اتفاقيات تقنن التشريعات اللازمة لمكافحة تلك الجرائم، وتنظم الجهود الدولية لمحاربتها، بما في ذلك بحث إنشاء «نظام للإنذار المبكر من الهجمات الإلكترونية»، وتطوير برامج آمنة، وزيادة وعي المسؤولين التنفيذيين والعملاء بالحاجة إلى إجراءات أمنية أفضل.

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

7- وفي الختام يمكن القول أنه يمكننا مواجهة الإرهاب الإلكتروني على المستوى الدولي عبر عدة مستويات، لعل من أبرزها:

أ. على المستوى الرقمي من خلال انتهاج سياسة تقنيّة في أمن المعلومات والعمل على تأمين شتى المنشآت الحيوية، مع مكافحة المواقع التي تحث على الإرهاب والكراهية وازدراء الأديان أو التي توفر معلومات مساعدة للعمل الإرهابي.

ب. على المستوى الفكري باعتباره الأهم، لأنّ الفكرة هي التي تحرك القوّة. ولهذا يجب التركيز على المواجهة «الذكّية» مع الإرهاب عبر دحض أفكاره وعزله عن المجتمع، مع بثّ أفكار مضادة لما يروّج الإرهابيون له، وكذلك ضرورة تتبلوّر ثقافة عالمية تنبذ العنف، وتجتث جذور الصراع والكراهية والفقر والظلم والجهل التي تشكل بيئة دولية لتوالد العنف والإرهاب والحروب.

الهوامش :

1 برغم اهتمام المجتمع الدولي بالعمل على منع ومكافحة العمليات الإرهابية في مختلف صورها وأشكالها، فإنّ مفهوم الإرهاب قد أثار الكثير من الجدل والخلاف بسبب ما أحاط تحديد هذا المفهوم من اعتبارات سياسية مما يدل على صعوبة وضع تعريف محدد للإرهاب. ولمزيد التعمق في هذا الشأن راجع:

- أحمد حسين سويدان: الإرهاب الدولي في ظل المتغيرات الدولية، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2005.

GUILLAUME (G.):"Le terrorisme et le droit international". R.C.A.D.I، 1989-III، Volume 215، pp.287-416.

2علاء الدين راشد: المشكلة في تعريف الإرهاب، دار النهضة العربية، القاهرة، 2006، ص.أ.

3 تثبت الدراسات الفرنسية أن عبارة إرهاب وإرهابي ظهرت في القرن 18 في أعقاب الثورة الفرنسية، إذ كانت الدولة تقوم بإرهاب السكان مستعملة القوة لاسترجاع الأمن ومنه استخدم مفهوم «terreur institutionnalisée». ثم تحولت كلمة«terreur» في القرن 19 إلى عبارة «terrorisme» لتفيد " العنف الموجه ضد الدولة أو أعضاء الحكومة بغية ضرب استقرار هياكل الدولة وإضعاف البلاد. أنظر http://www.dictionnaires-francais.fr

4 آية 40 من سورة البقرة.

5 Le terrorisme est l›emploi systématique de la violence attentats، assassinats، enlèvements، ...) à des fins politiques، de telle sorte que leur retentissement psychologique – terreur et peur – dépasse largement le cercle des victimes directes pour frapper l›opinion publique concernée :http://fr.wikipedia.org/wiki/Terrorisme

6 راجع الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام 1998.

7 محمد مسعود قيراط: الإرهاب: دراسة في البرامج الوطنية واستراتيجيات مكافحته: مقاربة إعلامية، جامعة نايف العربية للعلوم الأمنية، الطبعة الأولى، الرياض، 2011، ص.19.

8 العريان : العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة، الدورة التدريبية لمكافحة الجرائم الإرهابية المعلوماتية، بالمغرب، 2006، ص. 32-33.

9 رامي متولي القاضي :مكافحة الجرائم المعلوماتية دار النهضة العربية، القاهرة، الطبعة الأولى، 2012، ص.5.

10 جرائم الحاسب الآلي – ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية " الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من 4-2004/4/5م

11ذياب موسى البدانة: دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي، 9-14 أفريل 2006 بالمغرب

12 مصطفى محمد موسى: الإرهاب الإلكتروني (دراسة قانونية_أمنية_نفسية_إجتماعية)، دار الكتب والوثائق القومية المصرية، الطبعة الأولى، القاهرة، 2009، ص.5.

13 عبد المجيد الحلاوي: أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي، الدورة التدريبية مكافحة الجرائم الإرهابية المعلوماتية، 9-14 أفريل 2006 بالمغرب

14 عبد الله بن عبد العزيز بن فهد العجلان: الإرهاب الالكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2 -4 جوان 2008.

15 غازي عبد الرحمان هيان الرشيد: الحماية القانونية من جرائم المعلوماتية (الحاسب والإنترنت)، أطروحة أعدت لنيل شهادة الدكتوراه في القانون، كلية الحقوق بالجامعة الإسلامية في لبنان،2004، ص.186.

16 هشام محمد فريد رستم: الجرائم المعلوماتية، أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة، 2000، ص.48-49.

17 يوسف حسن يوسف: الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، 2011، ص.135.

18 وليد الكشباطي: جرائم اختراق الأنظمة المعلوماتيّة، محاضرة ختم تمرين تربص محاماة بتونس، 12 جوان 2009.

19 Site du Conseil de l'Europe: http://conventions coe.hnt.

20 كريستينا سولكمان: المعايير الدولية المتعلقة بجرائم الأنترنت (مجلس أوروبا)، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19-20 جوان 2007 بالمغرب، ص.120 119-.

21 صغير يوسف: الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013، ص.94.

22 محمد القاسم، رشيد الزهراني عبد الرحمن السند، عاطف العمري: دراسة تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات 10-11-1423هـ

23 ناصر بن محمد البقمي: مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجي أبو ظبي، الطبعة الأولى، 2008، ص.5

24 عبد الرحمن السند: وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب، الجزء الأول، (الرياض: جامعة الإمام محمد بن سعود الإسلامية، 1425هـ-2004، ص.41.

25 أحمد بن عبد الرحمان البعادي: دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع والمأمول، المؤتمر الثالث لرؤساء المحاكم العليا، (23-25 سبتمبر 2012) بالخرطوم، ص. 13.

26 وجاء في المادة الثانية من هذا النظام: (يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1 -المساعدة على تحقيق الأمن المعلوماتي.

2 -حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3 -حماية المصلحة العامة، والأخلاق، والآداب العامة.

4 -حماية الاقتصاد الوطني).

27 محمد جوهر: خصوصيات زجر الإجرام المعلوماتي، المجلة المغربية للقانون والاقتصاد والتدبير، العدد 52، 2006، ص84

28 بينت الأحداث الأليمة لـ16 ماي 2003 أن المغرب مستهدف أيضا في أمنه الاجتماعي من طرف الجماعات الإرهابية مما سرع بالتصويت على مشروع القانون المجرم للإرهاب لملأ الفراغ القانوني

29 ينص الفصل 1-218 (تعتبر الجرائم التالية أفعالا إرهابية، .....7-الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات.....)

30 ينص الفصل 2-218(يعاقب بالحبس من سنتين إلى ست سنوات وبغرامة تتراوح بين 10000 و200000درهم كل من أشاد بأفعال تكون جريمة إرهابية بواسطة الخطب أو الصياح أو التهديدات المفوه بها في الأماكن أو الاجتماعات العمومية أو بواسطة المكتوبات والمطبوعات المبيعة او الموزعة أو المعروضة للبيع أو المعروضة في الأماكن أو الاجتماعات العمومية أو بواسطة الملصقات المعروضة على أنظار العموم بواسطة مختلف وسائل الإعلام السمعية البصرية والالكترونية)

31 فايز بن عبد الله الشهري: التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة الظاهرة الإجرامية على شبكة الإنترنت، مصدر سابق، المجلة العربية للدراسات الأمنية والتدريب، المجلد 20، العدد 39، فيفري 2005، ص148 – وما بعدها).

32 Rapport du conseil d'Etat «Internet et les réseaux numériques Isabelle Falque Pierrot، rapporteur général. Petites Affiches.

33 جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة 1998، ص.75.