

الإرهاب و الإنترنت

الأستاذ الدكتور : موسى مسعود أرحومة

جامعة "قاريونس" بنغازي - ليبيا

توطئة :

أضحى الإرهاب في العقد الأخير من هذا القرن مصدر قلق يقض مضجع المجتمعات كافة بدون استثناء ، وقد تنامي عدد المنظمات الإرهابية في السنوات القليلة الماضية بشكل كبير ، الأمر الذي ضاعف من وتيرة الجرائم الإرهابية وارتفاع عدد ضحاياها ، وهو ما أدى ويؤدي إلى ترويع الأمنيين في حياتهم وممتلكاتهم ، وإحداث اضطراب غير معهود في الأمن وشل خطط التنمية في كثير من الدول ⁽²⁾، وخير دليل على ذلك ما يجري في العراق والصومال وغيرها من الدول التي اكتوت ولا تزال تكتوي بنار الإرهاب صباح مساء ؛ إذ لا يكاد يمضي يوم إلا وتطالعنا وكالات الأنباء عن وقوع عمل إرهابي هنا وهناك .

ونتيجة للتطور التكنولوجي في مجال الإنترنت والاتصالات ، أخذ الإرهاب بعداً جديداً يختلف عن النمط التقليدي المتعارف عليه ، حيث أضحى الإرهابيون يوظفون هذه التقنية في ارتكاب جرائمهم الإرهابية بما يوفره لهم ذلك من إمكانيات واسعة ، بحيث صار الفضاء المعلوماتي أو بيئة الإنترنت ملاذاً آمناً للإرهابيين يمكنهم من خلالها التواصل فيما بينهم بسهولة ويسر ⁽³⁾، كما أن الشبكة العنكبوتية باتت تسخر بشكل كبير في التدريب على الإرهاب وكيفية تنفيذ العمليات الإرهابية والتخطيط لها عن بعد دونما حاجة للاتصال المباشر كما في الإرهاب التقليدي ، فضلاً عما تتيحه هذه البيئة من فرصة للتخفي بعيداً عن أعين الأجهزة الأمنية . وهكذا يكون الإرهاب قد دخل مرحلة متطورة للغاية ، تجسد فيما بات يعرف بإرهاب الإنترنت أو الإرهاب الإلكتروني ، الذي تعدى تسخير الشبكة العنكبوتية (الإنترنت) في ارتكاب جرائم الإرهاب التقليدية ، بحيث أضحت الشبكة ذاتها هدفاً لهجمات الإرهابيين .

وعلى هذا النحو أخذ الإرهاب منعطفاً متطوراً بات يقلق المجتمع الدولي بأسره ، ولم يعد أمره يعني دولة بعينها ، باعتبار أن هذا النمط من الإرهاب (الإرهاب عبر الإنترنت أو باستخدام الإنترنت) يشكل خطورة بالغة لاتساع رقعته ونطاقه من ناحية ولصعوبة اكتشافه وفداحة الأضرار الناجمة عنه من ناحية أخرى ، ومن هنا بات المجتمع الدولي يستشعر مخاطر هذا الأسلوب ، فعقد من أجله عدد من المؤتمرات سواء على الصعيد الدولي أم الإقليمي أم المحلي لبحث أفضل السبل لكيفية التصدي له ومواجهته بجهود جماعية بدلاً من الجهود الفردية التي لم تعد مجدية ، كما أن أغلب الدول عمدت إلى إصدار تشريعات بقصد مكافحة الإجرام المعلوماتي ومنها جرائم الإرهاب عن طريق الإنترنت (عبر الإنترنت) .

ولكن ما المقصود بالإرهاب عبر الإنترنت أو بواسطة الإنترنت ؟ وما الذي يميزه عن الإرهاب التقليدي ؟ وما دور الشبكة العنكبوتية (الإنترنت) في مجال الأعمال الإرهابية ؟ وما هي صور وأنماط الإرهاب المعلوماتي ؟ وأخيراً ، ما هي الاستراتيجيات المناسبة لمواجهة هذا النمط من الإرهاب ؟

إن الإجابة عن هذه التساؤلات ستكون المحاور الرئيسة لبحث هذا الموضوع ، ونحاول على ضوء ذلك تقسيمه إلى ثلاثة مطالب ، نخصص الأول لتحديد مفهوم الإرهاب ، أما المطلب الثاني فسنخصصه لبحث دور الإنترنت في الإرهاب (الإنترنت كمسرح للجرائم الإرهابية أو أداة لتنفيذها) ، في حين نفرّد المطلب الثالث والأخير لبحث استراتيجية مواجهة الإرهاب عبر الإنترنت .

المطلب الأول

تحديد مفهوم الإرهاب

يعد مفهوم الإرهاب من أكثر المفاهيم إثارة للجدل بالنظر إلى تباين وجهات النظر حوله ، وقبل تحديد مفهوم الإرهاب عبر الإنترنت أو بواسطة الإنترنت ، يقتضي الوقوف على مدلول الإرهاب بوجه عام .

والخوف لدى الناس الآمنين باستخدام وسائل من شأنها خلق حالة من الخطر العام (7)، وقيل بأنه عبارة عن استخدام العنف أو التهديد به من قبل فرد أو جماعة بحيث يتولد عنه الرعب أو الخوف من أجل بلوغ أو تحقيق هدف معين ، الذي يكون في الغالب هدفاً سياسياً (مثل احتجاز الرهائن — اختطاف الأشخاص والتنكيل بهم أو قتلهم — وضع المتفجرات أو العبوات الناسفة في أماكن تجمع الآمنين أو في وسائل النقل العام — أعمال التخريب — خطف الطائرات وتغيير مسارها أو التهديد بذلك — إرسال الجرائم الضارة "كالجمرة الخبيثة" — تسميم مياه الشرب — تعطيل شبكة الاتصالات أو الكهرباء وما إلى ذلك كثير) .

وأغلب التعريفات التي تتعلق بالإرهاب تحاول ربطه بتحقيق غرض سياسي ، وهذا من شأنه أن يضيق من مفهومه وإن كان الغالب هو كذلك ، ومع ذلك فإن ممارسة الأنشطة الإرهابية قد يكون مبعثه تحقيق غرض سياسي وقد يكون لغاية أخرى . وعليه ، يمكن تعريفه بأنه اللجوء إلى أية وسيلة تنطوي على العنف أو القوة (سواء كان هذا العنف واقعاً من فرد على آخر أو من جماعة على فرد أو جماعة أخرى) لبث الرعب والفرع لدى الطرف الذي هو ضحية هذا الإرهاب لتحقيق غاية معينة غير مشروعة (سياسية أو غيرها) وبما من شأنه أن يفضي إلى اختلال الأمن وتعريضه للخطر ، وبما ينذر بعواقب وخيمة في الأرواح أو الممتلكات أو هما معاً .

ثانياً — مفهوم الإرهاب عبر الإنترنت :

أ — تعريفه :

بفضل التطور التكنولوجي في مجال الاتصالات والتوسع في استخدام شبكة الإنترنت ، تطورت الجريمة وأساليب ارتكابها بما في ذلك الجرائم الإرهابية ، فقد تنوعت أشكالها وأنماطها ؛ إذ أصبح الإرهاب عبر الإنترنت يأخذ بعداً جديداً ليس فقط في آلياته وإنما في مفهومه أيضاً ، فالإرهابي الذي يستخدم الشبكة العنكبوتية في تنفيذ جرائمه يختلف حتماً عن ذلك الذي يلجأ إلى الإرهاب بالوسائل التقليدية المعروفة .

فتعريف هذا النمط من الإرهاب ينبغي أن يأخذ في الاعتبار الوسيلة التي يستخدمها الإرهابيون في تحقيق مآربهم — والتي تختلف عن الوسائل التقليدية — والمتمثلة في شبكة المعلومات الدولية (الإنترنت) ، وكذلك الأهداف التي تكون محلاً للاعتداء أو موضوعاً للأعمال الإرهابية ، وهو ما أفرز شكلاً مستحدثاً من الإرهاب وهو ما يُعرف "بالإرهاب الإلكتروني" .

وهذا النوع الأخير يعد في الوقت الراهن من أخطر أشكال الإرهاب في العصر الرقمي Digital age .

وبناءً على ما تقدم يمكن القول بأن الإرهاب في العصر الرقمي ، أو ما يعرف بالإرهاب عبر الإنترنت ، هو ذلك المتمثل في تسخير شبكة المعلومات الدولية (الإنترنت) في ممارسة الأنشطة الإرهابية (تخطيطاً وتدريباً وتنفيذاً) بالاستفادة من الإمكانيات التي تيسرها هذه الشبكة للإرهابيين ، وكذلك ما تتعرض له هذه الشبكة ذاتها من اعتداءات مباشرة بغية تدمير وإتلاف البيانات والمعلومات المخزنة بها أو شل عملها بحيث لم تعد قادرة على أداء دورها بكفاءة من أجل الانتقام أو الابتزاز أو تحقيق مأرب ما (سياسي أو غيره) ، كما في بث الفيروسات المختلفة لإتلاف وتدمير قواعد البيانات أو الملفات الخاصة بالجهة المستهدفة بالإرهاب أو عن طريق ما يعرف بالقنابل المنطقية Logic Bombs والقصف الإلكتروني .

و على هذا النحو ينبغي عدم الخلط بين الأعمال الإرهابية التي تتخذ من الإنترنت بيئة حاضنة لها أو موضوعاً لها ، وبين غيرها من الجرائم التي ترتكب بواسطة الإنترنت أو من خلال شبكة المعلومات الدولية ، مثل اختراق المواقع على الشبكة من قبل بعض الهواة (الهاكرز) أو لتحقيق أغراض إجرامية ، كتدمير البرامج والبيانات المخزنة على الشبكة ، أو الاحتيال المعلوماتي والتجسس المعلوماتي وما شابه ذلك . فهذه الطائفة من الجرائم وإن كانت هي الأخرى عواقبها وخيمة لما ينجم عنها في الغالب من أضرار مادية كبيرة قد تبلغ البلايين من الدولارات ، ومع ذلك لا تصنف من ضمن الأعمال الإرهابية بمفهومها الدقيق الذي سبق إيراده ، مع أنها تثير هي الأخرى القلق والفرع لدى المجتمع ، ومع أن القاسم المشترك بينها وبين الجرائم الإرهابية عبر الإنترنت كون النوعين من الجرائم يؤدي

الإنترنت دوراً في ارتكابها (إما أن الشبكة ذاتها هدف للاعتداء أو هي وسيلة للاعتداء على المصالح المراد حمايتها) .

ب — خصائص الإرهاب في العصر الرقمي :

يتميز الإرهاب في العصر الرقمي بجملة من السمات والخصائص عن الإرهاب التقليدي منها :

- 1 — صعوبة اكتشاف الإرهابيين والتعرف عليهم ، فهؤلاء يمكنهم ارتكاب أنشطتهم الإجرامية عن بعد وبللمسة زر على الحاسوب ، فيتحقق لهم ما يريدون ، ذلك أن هؤلاء الإرهابيين لديهم خبرة عالية بتقنية المعلومات وعلى قدر كبير من المهارة بحيث يمكنهم توظيف الشبكة العنكبوتية واستغلالها لفائدتهم دون أن يكون بمقدور الأجهزة الأمنية تعقبهم أو الوصول إليهم .
- 2 — قدرة الإرهابيين على تغيير أساليب عملهم وأماكنهم بحيث يمكنهم الإفلات من إمكانية مراقبتهم ، وذلك بإخفاء مواقعهم على الشبكة وظهورها في ثوب جديد⁽⁸⁾ .
- 3 — سهولة التواصل بين الإرهابيين عن بعد دونما حاجة إلى اجتماعهم من خلال الرسائل الإلكترونية أو غرف الدردشة أو ما شابه ذلك من الوسائل التي تتيحها لهم الشبكة العنكبوتية ، وهذا من شأنه أن يصعب تحديد أماكن تواجدهم⁽⁹⁾ .
- 4 — إن الأعمال الإرهابية عموماً ، التي تتم عبر الإنترنت أو عليه تتسم بكونها تنتمي إلى طائفة الجريمة المنظمة أو على الأقل تشترك معها في بعض الخصائص⁽¹⁰⁾ ، فالإرهابيون يخضعون لنظام صارم ، بحيث إن المجموعات وإن كانت تعمل لغرض واحد لكن لا تعرف بعضها البعض ، واستخدامها للشبكة المعلوماتية يجعلها حريصة أكثر على تنظيم نفسها تنظيمًا محكمًا ودقيقًا من أجل الاستفادة القصوى من الامتيازات التي تتيحها لهم هذه الشبكة .
- 5 — تتميز الأعمال الإرهابية عبر الإنترنت بسهولة تمويلها من خلال استغلال الشبكة المعلوماتية في تحويل الأموال بالسرعة الممكنة وبأسماء مستعارة عادةً .

- 6 — إن تنفيذ الأنشطة الإرهابية لا يتطلب التنقل من مكان إلى آخر ، أو التواجد في الأماكن التي تكون هدفاً للإرهابيين ، وإنما قد يتم ذلك عن بعد بالدخول إلى الموقع الخاص وتعطيل المنظومة الخاصة به .
- 7 — فوق هذا وذاك ، يُصنّف الإرهاب عبر الإنترنت ضمن طائفة الجريمة العابرة للحدود أو القارات أو ما يعرف بالجريمة عبر الوطنية Transnational Crime التي تتعدى الحدود الإقليمية للدول مما يضيف عليها بعداً دولياً ، وهذا من شأنه أن يخلق كثيراً من التحديات القانونية في مواجهتها والتصدي لها فيما يخص تحديداً إجراءات الاستدلال والتحقيق والمحاكمة ؛ نظراً لصعوبة تحديد مكان وقوع الجريمة ومن ثم القانون الواجب التطبيق . فالنشاط الإرهابي قد يقع في شرق الكرة الأرضية والنتيجة الضارة تقع في غربها ، الأمر الذي يثير التنازع في الاختصاص بشأنها ، ويتطلب صياغة قواعد قانونية ملائمة لهذا النمط من الإجرام⁽¹¹⁾ .
- 8 — إن الخسائر الناجمة عن الإرهاب في العصر الرقمي — وبالذات ما يعرف بالإرهاب الإلكتروني — فادحة تكاد تكون أضعاف الخسائر التي تُحدثها الأعمال الإرهابية التقليدية سواء من حيث الأرواح أو الممتلكات لاسيما في الدول التي تعتمد بشكل كبير على تقنية المعلومات .
- 9 — إن الإرهاب عبر الإنترنت لم يعد هدفه محصوراً في تحقيق مآرب سياسية ، كما هو الحال في الإرهاب التقليدي عادةً ، وإنما أضحت له أغراض أخرى متعددة وربما قد يكون في مقدمتها الأغراض الاقتصادية أو الانتقامية أو الدينية .

المطلب الثاني

دور الإنترنت في ارتكاب الأنشطة الإرهابية

كان إرهاب الإنترنت أو عبر الإنترنت إلى وقت قريب مجرد تصور يداعب خيال الروائيين من كتّاب قصص الخيال العلمي والسينمائيين ؛ تجلّى ذلك في ظهور عدد من الأفلام التي أُخرجت في السينما الغربية بالذات ، والتي تركت مزيداً من الهلع والرعب في أوساط الجماهير من مرتادي تلك الأفلام ومتتبعيها ، ومن ذلك إمكانية إقدام المنظمات

الإرهابية على تدمير أنظمة التحكم في المفاعلات النووية وما يمكن أن يفضي إليه من تخريب هذه المفاعلات وحدوث كوارث بيئية فظيعة . وهو الأمر الذي أثار اهتمام الكتاب لتسليط الضوء على هذه الظاهرة ولفت الأنظار إلى المخاطر التي من المتوقع حدوثها فيما لو تحقق وقوع مثل هذه الهجمات الإرهابية كي يتسنى اتخاذ الإجراءات الكفيلة بمواجهتها والحد منها .

ولكن جرائم الإرهاب بواسطة الإنترنت أو عبر الإنترنت أضحت حقيقة واقعة ، نلمس آثارها كل يوم . فالإرهابيون قد استفادوا مما تتيحه لهم شبكة الإنترنت لاقتراف جرائمهم ، بمعنى أن جرائم الإرهاب تطورت في أساليبها وكيفية التخطيط لها وتنفيذها بفضل تقنية المعلومات وشبكة الإنترنت⁽¹²⁾ ، ومن أمثلة الأعمال الإرهابية التي من المتصور أن تتم عبر هذه التقنية المتطورة أو باستخدامها ، التهديد إما بالقتل أو تدمير المعلومات أو البيانات أو بنشر الأفكار المتطرفة أو بالخطف أو احتجاز الرهائن نظير فدية معينة ، ومن أمثلة ذلك ما يُطلق عليه "القصف الإلكتروني" وتخريب شبكة المعلومات وإتلاف الأنظمة والبرامج بحيث لم تعد قادرة على العمل⁽¹³⁾ .

كما أن استخدام الشبكة العنكبوتية يساعد الإرهابيين على الاتصال ببعضهم وفي نشر الدعاية وتجنيد الإرهابيين ، وتدريبهم على كيفية تنفيذ العمليات الإرهابية⁽¹⁴⁾ .

وتمكن شبكة المعلومات الإرهابيين من تهديد حياة المرضى في المستشفيات من خلال اقتحام الصفحة الخاصة بهم وإحداث تلاعب أو تغيير في البرنامج العلاجي ، كما قد يتأتى تخريب الاقتصاد أو تهديده كما في حالة اختراق المواقع الخاصة بالبورصة ، ويتحقق الإرهاب الإلكتروني كذلك من اقتحام نظم الاتصالات أو الكهرباء⁽¹⁵⁾ ، أو التحكم في نظم المواصلات بما في ذلك الطائرات ، مما قد يؤدي إلى اضطراب مواعيد الرحلات الجوية أو حتى تفجير الطائرة من خلال العبث بالمنظومة الخاصة بحركة الطيران .

ويشير الخبراء إلى أن ثمة ازدياداً في عدد المواقع الإلكترونية للإرهابيين ، سواء التي تحرّض على الإرهاب أو تسهل التخطيط للعمليات الإرهابية وتنفيذها ؛ فمن 12 موقعاً سنة 1998م إلى حوالي 4800 موقع سنة 2005م ، وربما تضاعف هذا العدد في الوقت الحالي .

إذ من شأن الاعتماد على تقنية الإنترنت أن اتسع نطاق العمليات الإرهابية ، الأمر الذي صعب من إمكانية كشفها . فكل الجهود التي تبذل لمنع الإرهابيين من الاستعانة بالشبكة العنكبوتية لم تفلح ، فما إن يختفي موقع حتى يظهر بدلاً عنه موقع جديد (تبدل المواقع وتغيرها) وبمناوين إلكترونية جديدة بعد فترة جد قصيرة ، ويتعذر في الغالب تحديد مصدر الإرهاب أو الجهة التي شنته ، مما يجعله في كثير من الأحيان بمنأى عن الضبط أو الاصطياد .

فالإنترنت أضحي مسرحاً لتدريب الإرهابيين ، أو بالأحرى تحوّل يوماً بعد يوم إلى معسكرات للتدريب على الأعمال الإرهابية⁽¹⁶⁾ .

فبالرغم من النجاحات الجزئية التي تحققت هنا وهناك على الإرهاب التقليدي ، لكن فيما يخص الإرهاب الإلكتروني ظل بمنأى عن إمكانية السيطرة عليه أو كشفه . فالمواقع الإرهابية العديدة التي تتزايد باستمرار على شبكة الإنترنت تسهل استقطاب الإرهابيين الجدد من الشباب من خلال ما يقدم في هذه المواقع من إغراءات ، كما يتلقون دروساً عملية عن كيفية استخدام الأسلحة البيولوجية والمتفجرات ، حتى إنها باتت توصف بأنها بمثابة فصول دراسية للتدريب النظري والعملي في آن معاً .

وهذا مرده اتساع نطاق استخدام شبكة الإنترنت باعتبارها قد تغلغلت في كل بيت ، الأمر الذي جعلها وسيلة فعالة لتحريض الشباب على الإرهاب نظير ما يوعدون به من امتيازات ، حيث تستغل ظروف هؤلاء الشباب العاطلين عن العمل والذين سُدت في أوجههم سبل العيش الكريم ، مما يجعلهم عرضة للإيقاع بهم في براثن الشبكات الإرهابية التي عادة ما تعدهم بمستقبل أفضل في حال انضمامهم إليها والانصياع إلى تنفيذ أوامرها .

ولعله في مقدمة العوامل التي سهلت ارتكاب الأنشطة الإرهابية عبر الإنترنت أن هذه التقنية المتطورة مكنت الإرهابيين من الحصول على المزيد من التنسيق والتنظيم من خلال غرف الدردشة ، التي توفر فرصة أكبر للتواصل بين هذه الجماعات الإرهابية وتبادل الخبرات فيما بين أعضائها ، ويتأتى ذلك أيضاً عن طريق البريد الإلكتروني وغير ذلك من الآليات التي تمكن الإرهابيين من التواصل بسهولة ويسر عبر الشبكة العنكبوتية⁽¹⁷⁾ .

فباعثار أن الشبكة العنكبوتية لا تحدها حدود ، وبسبب صعوبة إخضاعها للرقابة على ما يُنشر فيها ، صارت ملاذاً آمناً للإرهابيين . ومن أمثلة الحالات التي استفاد فيها الإرهابيون من هذه الشبكة قيام فتاة ألمانية من موقعها في مدينة برلين بوضع معلومة عن كيفية تخريب أسلاك صناديق الإشارات الكهربائية في السكك الحديدية من أجل تعطيل حركة القطارات .

وتجلى ذلك أيضاً في اللجوء إلى التهديد بجميع أساليبه سواء بقتل بعض الشخصيات أو بتفجير بعض التجمعات أو المراكز ، أو ببث الفيروسات لتدمير بعض المواقع ، كما في حالة التهديد بقتل الرئيس الأمريكي الأسبق (كلينتون) من قبل شاب كندي سنة 1999م ، والتهديد بتفجير البيت الأبيض سنة 2000م من قبل أربعة طلاب إنجليز من خلال رسالة بريدية موجهة إلى الرئيس بيل كلينتون للتهنئة بمناسبة أعياد الميلاد، والتهديد بقتل رئيس كولومبيا من قبل طفل صيني سنة 1999م من خلال رسالة إلكترونية عبر الإنترنت ، والتهديد بإطلاق فيروس من قبل مجموعة من الأشخاص أصدقاء لأحد قراصنة المعلومات من أجل الضغط على السلطات المعتقل لديها بإطلاق سراحه ، وقيام مراهق أمريكي سنة 1999م بتهديد مدير شركة (ميكروسوفت) والمدير التنفيذي لشركة M.P.I من خلال رسالتين إلكترونيتين بتفجير الشركة في حالة عدم الالتزام بدفع مبلغ معين (5 ملايين دولار أمريكي) (18).

ومن مظاهر الإرهاب الإلكتروني ما يُعرف بـ "القصف الإلكتروني" ، حيث يتم توجيه آلاف الرسائل الإلكترونية إلى مواقع شبكة المعلومات من أجل تعطيلها وإصابتها بالشلل التام بحيث لم يعد بمقدورها استقبال الرسائل . وهذا النوع من الإرهاب كانت ضحيته بعض المؤسسات الكبرى مما ولد الذعر والخوف لدى المواطنين ، ويحاول المهاجمون إخفاء مصدر رسائلهم بتعمد استخدام عناوين وهمية بحيث لا يمكن كشفهم أو التعرف على هويتهم .

ولعل ما أصبح يثير الفزع لدى خبراء الإنترنت التخوف من لجوء الجماعات الإرهابية إلى استخدام هذه التقنية في تخريب البنية التحتية لأنظمة المعلومات .

فالإرهابيون يمكنهم انتقاء أهدافهم الحيوية بدقة متناهية في أي مكان في العالم والهجوم عليها في لحظة واحدة . وربما المثال الحي لمثل هذا القصف الإلكتروني ما تعرض له موقع (ياهو) سنة 2000م ، الذي أدى إلى توقفه عن العمل لمدة ثلاث ساعات، وحتى بعد عودته للعمل لم يعد يعمل بكامل طاقته وإنما بنسبة أقل (70% فقط) .

وقد طالت هذه الهجمات بعض المواقع لشركات أمريكية كبرى على الإنترنت ، مما أدى إلى تعطيلها لساعات ، وقد أسفر ذلك عن تكبدها خسائر كبيرة تقدر بعشرات الملايين ، فماذا لو استمر التوقف لأيام أو شهور ؟!

ويذكر في هذا الصدد أن هذا القصف الإلكتروني لم تنج منه مواقع أخرى منها شركة (أمازون) لبيع الكتب عبر الإنترنت وموقع شبكة (CNN) للأطباء على الإنترنت ، وهو ما كان سبباً في تدفق المعلومات ببطء على غير المعتاد واستمر ذلك زهاء ساعتين⁽¹⁹⁾ . وأمثلة أخرى كثيرة لا يتسع المقام للإشارة إليها ، كل ذلك جعل الأمريكيين يصابون بالذعر لاسيما أولئك الذين يعتمدون على استخدام هذه المواقع التي كانت هدفاً مباشراً لمثل هذه الهجمات الإرهابية .

ولنا أن نتصور مدى الهلع الذي تحدثه هذه الهجمات في نفوس الذين يتعاملون مع الشبكة العنكبوتية ، وهو أمر آخذ في الازدياد يوماً بعد يوم . وقد كانت الشركات اليابانية الكبرى هي الأخرى هدفاً لعدد من الأعمال الإرهابية من هذا القبيل ، تجلّى ذلك في أن بعض هذه الجماعات تمكنت من التلاعب بأنظمة الكمبيوتر والإنترنت في أكثر من خمسين شركة فضلاً عن عدد من الإدارات الحكومية ، مما أسفر عن حدوث خسائر فادحة ، فأصيب الاقتصاد بالشلل ، ومن ثم شعور الناس بالهلع والخوف .

وفي هذا المقام يشير الأستاذ (غابريل فايمان) أستاذ علوم الاتصال الإسرائيلي في دراسة قام بها عن المواقع الإرهابية بأن هذه الأخيرة تتطور بشكل سريع لا من حيث عددها وتزايدها المستمر ، وإنما من حيث تصميمها والتقنية المتبعة في إعدادها بما يجعلها تتفوق حتى على المواقع الحكومية الأمريكية في بعض الأحيان . بمعنى أن الإرهابيين يحاولون جاهدين الاستفادة ما أمكن من تقنية الإنترنت وتطوير تقنياتهم ليكونوا أكثر

تفوقاً ، بحيث يصعب كشفهم أو التعرف عليهم (20) .

وعلى العموم فإن الإرهاب عبر الإنترنت يمكن أن يؤدي إلى تدمير البنية التحتية ونظم المعلومات ، ومن ثم قد يفضي إلى تخريب الاقتصاد . كذلك فإن الإرهابيين يمكنهم التحكم في المرور الجوي ومولدات الكهرباء وشبكات الاتصالات وأنظمة القيادة العسكرية والتحويلات المالية بغية تحقيق أغراضهم . ويحاول الباحثون تهويل الأمر بمقولة أن الآثار الناجمة عن هذه الأنشطة الإرهابية عبر الإنترنت قد تتعدى تلك التي نجمت عن هجمات 11 سبتمبر سنة 2001م .

المطلب الثالث

استراتيجية مواجهة جرائم الإرهاب عبر الإنترنت

بالنظر إلى المخاطر الناجمة عن الأنشطة الإرهابية عبر الإنترنت ، التي وقفنا على بعض صورها وأشكالها وما قد يسفر عنها من آثار مدمرة ، أخذت دول العالم — بدون استثناء — تستشعر الخطر الداهم والتفكير جدياً في التصدي لهذا النوع من الإرهاب من خلال تطوير التقنيات التي تمكنها من حماية نفسها من الهجمات الإرهابية عبر الإنترنت ، إلى جانب إعادة النظر في تشريعاتها الوطنية لمواجهة هذا النمط من الإرهاب ، فضلاً عن تعزيز التعاون فيما بينها من خلال الاتفاقيات الجماعية والثنائية والرفع من كفاءة الأجهزة الأمنية والقضائية لكي تكون قادرة على تتبع الإرهابيين وكشف مخططاتهم الشريرة (21) .

ومن الجهود المبذولة في هذا المضمار أن كثيراً من الدول اتجهت إلى إصدار تشريعات لمكافحة الإجرام المعلوماتي بما في ذلك الأنشطة الإرهابية عبر شبكة الإنترنت بإصدارها تشريعات خاصة لهذا الغرض أو باستحداث تعديلات على قوانينها العقابية . وقد كانت الدول الأوروبية والولايات المتحدة الأمريكية وبعض الدول المتقدمة الأخرى سباقة إلى ذلك باعتبارها تعتمد بشكل كبير على هذه التقنية الحديثة ، الأمر الذي يجعلها أكثر عرضة للهجمات الإرهابية التي تهدد مصالحها ، كما أن دولاً أخرى ، ومنها بعض الدول العربية ، قد خطت خطوات إيجابية في هذا الشأن ، ومن هذا القبيل ما قرره المشرع الإماراتي بموجب القانون الاتحادي رقم (2) لسنة 2006م في شأن مكافحة

جرائم تقنية المعلومات ، الذي جرّم ضمن ما جرّم إنشاء المواقع أو نشر المعلومات على شبكة الإنترنت بقصد تمكين الجماعات الإرهابية من ترويج أفكارها أو الاتصال بقياداتها، أو كيفية صنع المواد المتفجرة وكل ما يمكن أن يستخدم في الأعمال الإرهابية ، ومثله فعل المشرع السعودي من خلال نظام الجرائم المعلوماتية الذي أضحى نافذاً في مستهل شهر إبريل سنة 2007م الذي يقرر عقوبة السجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحدهما على كل شخص ينشئ موقعاً لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصالات بقيادات تلك المنظمات أو ترويج أفكارها أو نشر كيفية تصنيع المتفجرات .

ويلاحظ هنا أن بعض التشريعات التي تصدرت لظاهرة الإرهاب عبر الإنترنت — ومنها القانون الإماراتي سالف الذكر — لم تكتفِ بالعقوبة الأصلية السالبة للحرية (السجن) وإنما أجازت للمحكمة توقيع عقوبة تكميلية متمثلة في غلق المواقع التي تستضيف المواقع الإرهابية متى كان المالك عالماً بذلك سواء بصفة مؤقتة أو دائمة وذلك من أجل إعاقة الإرهابيين من استخدام الشبكة المعلوماتية في أغراضهم الإجرامية⁽²²⁾ .

كما تم إبرام بعض الاتفاقيات لهذا الغرض ، وأبرزها وأهمها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية ، والمعروفة باتفاقية (بودابست) التي تم إبرامها في إطار دول مجلس أوروبا (أو المنضوية تحت مظلة المجلس الأوروبي) والموقع عليها في العاصمة الجارية (بودابست) في 23/11/2001م⁽²³⁾ ، من حوالي 30 دولة بما في ذلك أربع دول من خارج مجلس أوروبا ، وهي الولايات المتحدة الأمريكية واليابان وكندا وجنوب أفريقيا ، وهي تعد الاتفاقية الأولى لمواجهة الجرائم المعلوماتية بجميع صورها بما فيها جرائم الإرهاب.

وقد جاءت هذه الاتفاقية بمثابة رد فعل دولي جماعي بعد أحداث 11 سبتمبر التي تعرض لها مركز التجارة العالمي بنيويورك سنة 2001م ، حيث تقضي هذه الاتفاقية بإلزام أطرافها بتجريم الأفعال التي يساء فيها استخدام الإنترنت ، ومن ذلك توظيفه في ارتكاب الجرائم الإرهابية .

وما يهمنا في هذه الاتفاقية أنها رسمت آليات للتعاون الدولي في مكافحة الجرائم المعلوماتية

، ومن ضمنها جرائم الإرهاب الإلكتروني والإرهاب عبر الإنترنت سواء من حيث تبادل الخبرات والمعلومات بين الأجهزة المختصة في الدول الأطراف وكيفية تعقب الجناة وتبعهم وتسليم المجرمين وما إلى ذلك من صور التعاون وهي كثيرة⁽²⁴⁾.

كما تأخذ مكافحة هذه الجرائم صوراً أخرى ، ومنها إحكام الرقابة على مستخدمي شبكة الإنترنت في كثير من الدول ، ومنها الولايات المتحدة الأمريكية ، وهو ما حدا بالدول التي اكتوت بنار الإرهاب عبر الإنترنت إلى استحداث شرطة خاصة تعهد لها مهمة ملاحقة وتتبع مرتكبي جرائم إرهاب الإنترنت أو الإرهاب الإلكتروني⁽²⁵⁾.

وتنبغي الإشارة إلى أنه بعد أحداث سبتمبر تعالت الأصوات المنادية بضرورة تشديد الرقابة على مستخدمي الشبكة العنكبوتية (الإنترنت) من قبل الأجهزة الأمنية والقضائية .

وجراء الهجمات الإرهابية التي تعرضت لها أمريكا في أواخر الثمانينات وخلال حقبة التسعينات (ممثلة في تفجير طائرة آل (بان.إم) فوق بلدة لوكربي سنة 1988م وقضية هانوفر (هاكرز) سنة 1989م ، وقضية (سيتي بانك) سنة 1994م ، وتفجير (أو كلاهوما سيتي) سنة 1995م)⁽²⁶⁾، اضطرت الولايات المتحدة الأمريكية إلى اتخاذ مجموعة من الإجراءات التحريزية لحماية البنية التحتية الحساسة من الخطر الذي من المحتمل أن تتعرض له فيما لو وقعت هجمات إرهابية تهدد أمنها كالهجمات سالف الذكر ، تجلّى ذلك في قيام الرئيس الأسبق (بيل كلينتون) سنة 1996م بإنشاء لجنة رئاسية لحماية البنية التحتية الحساسة التي تعرف اختصاراً بـ (PCCIP) للاضطلاع بدراسة هذه البنية وما يحتمل أن تتعرض له من خطر واقتراح الاستراتيجية المناسبة لحمايتها . وبعد مضي سنتين من تأسيس هذه اللجنة أنشئ المركز القومي لحماية البنية التحتية (NIPC) . بموجب القرار الرئاسي رقم 63 (PDD-63) سنة 1998م ، الذي يقضي بتحويل مركز تحقيقات الكمبيوتر إلى نواة المركز القومي لحماية البنية التحتية⁽²⁷⁾ ، ويضم هذا المركز ممثلين عن عدة جهات ، وهي مكتب التحقيقات الفيدرالي ، ووزارات الدفاع والتجارة والطاقة والنقل ، وقطاع الاستخبارات ، وغيرها من الوكالات الفيدرالية إضافة إلى القطاع الخاص من أجل تبادل المعلومات .

وتتلخص مهمة هذا المركز في اكتشاف الهجمات الإرهابية وإصدار التحذيرات قبل تنفيذها ، وفي حالة حدوث هذا بالفعل يقع على عاتق المركز المذكور التحقيق في اقتحامات الكمبيوتر التي تهدد البنية التحتية الحساسة .

واضطلاعاً بدوره قام المركز القومي لحماية البنية التحتية بتدريب ما يربو على (4 آلاف) محقق فيدرالي أو تابع لحكومات الولايات المتحدة أو الحكومات المحلية أو الأجنبية، وذلك من خلال تقديم دورات تدريب أساسية تتعلق بالتحقيقات الأساسية عن أنظمة الكمبيوتر وشبكة الإنترنت ونظم التشغيل وأنظمة تحويل مسار المعلومات على الإنترنت ، وتعد هذه الدورات عادة في مكتب التحقيق الفيدرالي (FBI) .

ومن أجل توسيع مهام المركز سالف الذكر في تعقب الإرهاب وكشفه فإن ثمة موظفين تابعين له بدول أخرى خارج الولايات المتحدة .

وعلى إثر هجمات 11 سبتمبر 2001م أصدر الرئيس بوش الابن في 16 أكتوبر أمراً رئاسياً يحمل الرقم (13231) بشأن حماية البنية التحتية الحساسة في عصر المعلوماتية، وبموجب هذا الأمر تم تشكيل المجلس الرئاسي لحماية البنية التحتية الحساسة من أجل حماية أنظمة المعلومات المتعلقة بها ، حيث تم إنشاء مجلس يضم حوالي (30) رئيساً تنفيذياً لشركات مساهمة مهمته إسداء المشورة للرئيس فيما يخص أنظمة المعلوماتية التي تدعم القطاع الخاص وحكومات الولايات والحكومات المحلية .

وتسعى دول أخرى إلى محاكاة الولايات المتحدة في تبني استراتيجيات مماثلة بغية التضيق على الإرهابيين ومراقبة أنشطتهم عبر شبكة المعلومات الدولية (الإنترنت) ، ومنها بريطانيا التي هي بصدد إصدار قانون يجيز إنشاء قاعدة بيانات حكومية ضخمة لتخزين رسائل البريد الإلكتروني والمعلومات المتعلقة بالإنترنت والمكالمات الهاتفية والرسائل النصية لجميع المقيمين في بريطانيا لأجل مساعدة الأجهزة الأمنية في مكافحة الجريمة والإرهاب (28) .

وعملياً أضحت شركات الاتصالات تحتفظ بتسجيلات المكالمات الهاتفية والرسائل النصية لفترة تصل إلى 12 شهراً وذلك بناءً على التوجيهات الصادرة عن وكالات مكافحة

الإرهاب التابعة للاتحاد الأوروبي .

وللغرض ذاته اقترحت وزارة الداخلية البريطانية ما مؤداه التزام مقدمي خدمات الإنترنت وشركات الاتصالات بتسليم سجلات تضم مليارات الرسائل الإلكترونية وكذلك سجلات استخدام الإنترنت والمكالمات الهاتفية عبر شبكة الإنترنت ، وبموجب ذلك يتسنى لأجهزة الأمن والشرطة الوصول إلى المعلومات بعد الحصول على تصريح من المحاكم .

ويؤكد الاتحاد الأوروبي أن المواجهة الفعالة للأنشطة الإرهابية عبر الإنترنت ستم من خلال الشبكة العنكبوتية ذاتها . وهو ما عبرت عنه مسودة البيان الصادر عن سفراء دول الاتحاد والمعدة لاجتماع وزراء العدل والداخلية ، التي تضمنت تعاون الدول الأعضاء فيما بينها في مشاريع مشتركة لتبادل المعلومات بخصوص مواقع المتشددين على الإنترنت . وقد تضمنت هذه المسودة أن وكالات الشرطة الأوروبية (يوروبول) تعمل على إقامة بوابة معلومات تتيح تبادل المعلومات بخصوص مراقبة هذه المواقع . وتشمل هذه البوابة قائمة بروابط (وصلات) المواقع المشمولة بالمراقبة أو المزمع إخضاعها للمراقبة في المستقبل ، فضلاً عن بيانات عن المنظمات الإرهابية والخبراء الذين يعهد إليهم بمراجعة المواقع في نطاق دول الاتحاد .

ويذكر في هذا الصدد كما جاء على لسان وزير الداخلية الروسي بأن ثمة تعاوناً بين أجهزة حفظ النظام والقانون الروسية ونظيراتها في بعض الدول الأخرى مثل بريطانيا وإيطاليا وألمانيا في مجال تبادل المعلومات ومواجهة الهجمات الإلكترونية على مواقع البنوك، مؤكداً أنه من خلال الجهود المشتركة يمكن التصدي للإرهاب بصورة ناجعة وفعالة⁽²⁹⁾ . وتشير دراسة حديثة أن ثمة اتجاهات متزايدة في تقييد الدول حرية استخدام الشبكة المعلوماتية (الإنترنت) ، وقد أظهرت هذه الدراسة ما مفاده أن حوالي (25 دولة) من أصل (41 دولة) ممن شملها المسح من قبل المؤسسة التي اضطلعت بهذه الدراسة وهي مؤسسة (أوبن نت انيشياتف) أن هذه الدول تمارس الرقابة على الإنترنت⁽³⁰⁾ . وفي إطار مواجهة الاتحاد الأوروبي للأنشطة الإرهابية عبر الإنترنت خطا وزراء العدل في هذا الاتحاد خطوة متقدمة بإصدار قرار يقضي بتجريم التحريض على الإرهاب

بما في ذلك استخدام الشبكة العنكبوتية كوسيلة للدعاية واستقطاب الأفراد وتجنيدهم . ومن شأن هذا القرار أن يسمح للسلطات المختصة بتسهيل الاستفادة من تعاون المزودين بخدمات الإنترنت والتعرف على المجرمين . والغاية من وراء ذلك القرار هو توفير الآليات المناسبة لتمكين الأنظمة القضائية في دول الاتحاد من مقاضاة أولئك الذين يشجعون على الإرهاب ونشر الدعاية له وعرض المعلومات حول كيفية صنع المتفجرات .

وقد جاء على لسان منسق الاتحاد الأوروبي لمكافحة الإرهاب أمام البرلمان الأوروبي في 7 إبريل سنة 2008م بأن حوالي (5 آلاف) موقع على الإنترنت تسهم في تشدد الشباب في أوروبا ، وعلى هذا الأساس أوصى بدعم اقتراح سبق لألمانيا أن أبدته يقضي بتحويل شرطة (يوروبول) الأوروبية مهمة مراقبة الإنترنت (31) .

وفيما يتصل بمواجهة الإرهاب عبر الإنترنت يقضي قانون مكافحة الإرهاب الأمريكي في الجزء (216 منه) بالحد من إشراف القضاء على مراقبة الهواتف والإنترنت، إذ يخول الأجهزة الأمنية الحصول على جميع عناوين البريد الإلكتروني التي تتراسل مع الشخص المعني ، وهذه الصلاحية التي يمنحها القانون المذكور تفترض أن هذه الأجهزة الأمنية الممثلة في مكتب التحقيقات الفيدرالي (FBI) تكفي بالاطلاع على عنوان الرسالة دون مضمونها ، غير أنه من الناحية الواقعية ليس ثمة ما يحول دون كشف محتوى هذه الرسالة طالما لا توجد أية ضوابط تحول دون ذلك . والخطورة هنا تكمن في أنه بمجرد ادعاء الأجهزة الأمنية (FBI) بأن هذه المعلومات تتصل بتحقيق جنائي جارٍ فإن هذا القانون يوجب على القضاء منحها تصريحاً بالحصول على عناوين الرسائل دونما حاجة إلى تبرير اتصال التحقيق بالإرهاب .

ليس هذا فحسب ، بل إن هذا القانون يسمح للأجهزة الأمنية حق الوقوف على المواقع التي تتم زيارتها من الشخص المعني على الإنترنت (أي حق مراقبة البريد الإلكتروني للأشخاص الذين يتراسلون مع الشخص المعني) ، وهو ينسحب بالقدر ذاته على المكالمات الهاتفية دون حاجة إلى تصريح جديد (32) . ناهيك عن أنه يمكن لأي قاضٍ منح تصريحات المراقبة التي تصلح في جميع أنحاء الولايات المتحدة ، بمعنى عدم التقيد بالاختصاص المكاني في منح هذه التصريحات .

وفي إطار هذا القانون تم في الولايات المتحدة الأمريكية اعتقال شخص يعرف بـ(ملك التخريب) على الإنترنت لاثامه بإرسال ملايين الرسائل الإلكترونية بقصد التخريب بولاية واشنطن ، وقد عُدد هذا الشخص — على حد تعبير النائب العام — من أكبر المخربين على الإنترنت، حيث كان يلجأ إلى استخدام أجهزة حاسوبية مصابة بفيروسات ومن ثم يقوم بإرسال رسائل إلكترونية إلى عدة ملايين من عناوين الإلكترونية. وقد تعالت كثير من الأصوات في العالم بضرورة وضع معايير للرقابة والتجسس على المعلومات الشخصية لمستخدمي الإنترنت وشبكة الاتصالات الهاتفية والخليوية ، والعمل على أن يكون ثمة تنسيق دولي فعال في هذا المجال ، ولهذا الغرض يقترح رئيس مجلس إدارة الجمعية المصرية لمكافحة جرائم المعلومات والإنترنت أن ثمة حاجة ماسة للبدء في تبادل المعلومات والخبراء بين الأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت في دول العالم ، مع ضرورة العمل على نقل التقنية المتقدمة في هذا الخصوص من الدول التي تتوفر لديها إلى الدول الأخرى التي تفتقر إليها ، والتدريب على كيفية التعامل مع الإرهابيين عبر شبكة الإنترنت .

والأهم من هذا كله التأكيد على ضرورة تعزيز التعاون والتنسيق مع المؤسسات المعنية بمكافحة الجريمة (كالإنتربول) من أجل مواجهة كل صور الإرهاب عبر الإنترنت، وتطوير آليات التعاون على المستوى الجنائي بما يتلاءم مع اتساع شبكة المعلومات بدلاً من الإجراءات التقليدية المتسمة بالبطء والتعقيد . وهو يدعو كذلك إلى حث الدول على الانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب عبر الإنترنت ، وتشجيع قيام اتحادات عربية بغية التصدي لهذه الطائفة من الجرائم ، والعمل على تعزيز الأمم ن الوقائي من خلال تفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة جرائم الإرهاب عبر الإنترنت ، وأخيراً الدعوة إلى إنشاء شرطة عربية متخصصة لمكافحة الإرهاب عبر الإنترنت (33).

أما عن دور الأمم المتحدة في مكافحة جرائم الإرهاب عبر الإنترنت فقد أجمله بيان الأمين العام الذي جاء فيه ما مؤداه أن الشبكات الإرهابية "تتخذ من شبكة الإنترنت والاتصالات مجالاً لكسب التأييد وتجنيد الأفراد" ، ما يعني في نظره وجوب حرمانها من

هذه المكنة بالنظر لاعتماد الإرهابيين عليها بشكل كبير سواء في مجال الدعاية والإعلام أو التدريب أو استقطاب الإرهابيين مدلاً على ذلك أن عدد المواقع الإرهابية على الشبكة العنكبوتية سنة 1998م لم يتعدّ (20) موقعاً ليصبح سنة 2005م بضعة آلاف (34).

فالإرهابيون — على حد قوله — يمكنهم باستخدام هذه التقنية ممارسة أنشطتهم عبر الحدود ، الأمر الذي يتعين معه على الدول مكافحة هذا النوع من الإرهاب عبر الحدود أيضاً ، فالإنترنت أضحى ملاذاً آمناً لهؤلاء الإرهابيين ، وما إن توصل الأبواب أمامهم في دولة ما حتى يتحولوا إلى سواها .

وقد جاء قرار مجلس الأمن الدولي رقم 1624 لسنة 2005م ليكون بمثابة الأساس في استخدام الإنترنت لمواجهة أعمال التحريض على الإرهاب .

ويهيب الأمين العام في تقريره هذا بالدول الأعضاء في الأمم المتحدة ضرورة إبلاغ لجنة مكافحة الإرهاب بما اتخذ من طرفها من خطوات أو تدابير لوضع القرار المذكور موضع التنفيذ ، وفي الوقت ذاته للجنة المذكورة مد يد العون والمساعدة للدول كي يمكنها بناء قدراتها الفنية والقانونية في هذا المجال ، مبدئياً تعاون الأمم المتحدة مع الدول بسن التشريعات المناسبة لمكافحة الإرهاب عبر شبكة الإنترنت .

وقد أدركت دول كثيرة خطورة هذه المشكلة وضرورة التصدي لها بالوسائل الممكنة ، وهو ما تجلّى من خلال مؤتمر (تونس) العالمي المعني بمجتمع المعلومات لسنة 2005م الذي يؤكد على مواجهة هذه الظاهرة الخطيرة بجميع مظاهرها وأشكالها عبر شبكة الإنترنت وإن كان ذلك ليس على حساب حقوق الإنسان وما يفرضه القانون الدولي من التزامات .

الخاتمة

تخلص هذه الورقة إلى أن الإنترنت أضحى — بلا جدال — بيئة حاضنة للإرهاب ، بما تتيحه الشبكة العنكبوتية من مكنات واسعة للإرهابيين سهّلت تواصلهم ببعضهم

البعض ، الأمر الذي صعب من إمكانية كشف الأنشطة الإرهابية وتعقب مرتكبيها والمتورطين فيها .

وبالرغم من الجهود الكبيرة المبذولة للتصدي لهذه الظاهرة الخطيرة (الإرهاب عبر الإنترنت) على المستويين الدولي والوطني (تقنياً وقانونياً) ، فإن هذه الجهود لاتزال — لاسيما في بلادنا العربية — دون الطموح المنشود ، ولم تفلح في الحد من هذا النمط الجديد للإرهاب الذي تتسارع وتيرته يوماً بعد يوم . وعلى ضوء ما تقدّم نرى إبداء بعض المقترحات المتواضعة التي يمكن أن تُسهم في تعزيز آلية المواجهة لهذه الظاهرة، وهي :

1 — التأكيد على ضرورة عقد اتفاقية دولية عربية لمواجهة هذه الأنشطة على غرار الاتفاقية الأوروبية لمكافحة جرائم المعلومات .

2 — حث الدول العربية على سن تشريعات تحظر التحريض على الإرهاب أو تشجيعه عبر الشبكة العنكبوتية ، بحيث تضمن عقوبات مغلفة تناسب وخطورة هذه الجرائم بما في ذلك قفل المواقع المستضيفة لها .

3 — المبادرة بإقامة شرطة عربية تكون مهمتها تتبع جرائم الإرهاب عبر الإنترنت أسوة بما هو معمول به في إطار دول الاتحاد الأوروبي .

4 — السماح بمراقبة المواقع المشبوهة على شبكة الإنترنت على أن يكون ذلك بتصريح من القضاء درءاً لأي شطط أو تعسف ، وبما لا يشكل افتياتاً على الحريات الفردية ، وبشرط أن يكون ذلك بمناسبة التحقيق في قضية معينة .

5 — تدريب رجال القضاء والنيابة العامة على كيفية التعامل مع قضايا الإرهاب عبر الإنترنت بالنظر إلى طبيعتها الخاصة .

6 — التوسع في إجراء الدراسات الميدانية للوقوف على الأسباب الحقيقية الكامنة وراء الأنشطة الإرهابية بمختلف أنماطها وأشكالها ، ومحاولة مواجهة ذلك بأساليب علمية بدلاً من الاعتماد على أسلوب القمع .

7 — عقد المزيد من المؤتمرات والملتقيات العلمية حول جرائم الإرهاب الإلكتروني ، بحيث تتاح من خلالها الفرصة لتلاقي الأفكار والاتجاهات لكل من يعينهم أمر مكافحة الإجرام ، بما في ذلك رجال الأمن ورجال القضاء والقانون والإعلام وعلماء الاجتماع وخبراء تقنيات المعلومات .

8 — ينبغي إعادة النظر في مقررات كليات الحقوق في الوطن العربي وأكاديميات الشرطة بحيث تخصص مساحة للتعريف بهذا النوع من الإرهاب ومخاطره وآلية مكافحته من أجل تأهيل أطر قانونية وأمنية قادرة على التعامل مع هذه الظاهرة وما تفرضه من تحديات.

9 — وأخيراً العمل على إشاعة ثقافة التسامح لدى الجيل الناشئ من طلاب المدارس والجامعات في الوطن العربي من خلال وسائل الإعلام المختلفة (المسموعة والمرئية والمكتوبة) ، فضلاً عن تضمين ذلك المقررات الدراسية .

- حول هذا الموضوع انظر :
ياسمينه صالح ، إرهاب الإنترنت وحروب الاستنزاف الإلكترونية على الجزيرة نت :
<http://www.al-Jazirah.com/digimag/05122004/Wr ? htm>
وكذلك : اللواء الدكتور/حسين المحمودي بوادي ، إرهاب الإنترنت الخطر القادم ، الطبعة الأولى ، دار الفكر الجامعي — الإسكندرية ، 2006 م .
- زيادة الحاجة إلى استخدام الحاسب الآلي ضاعف من مخاطر التعرض للإرهاب الإلكتروني
cyber - terrorism . فالتقنية سلاح ذو حدين ، فكما توظف في الخير يمكن توظيفها في الشر .
- (انظر على الشبكة : خلدون غسان سعيد ، حرب إلكترونية عبر شبكات الكمبيوتر
(الإرهاب في الجرائم المعلوماتية) ، عن صحيفة الشرق الأوسط على شبكة الإنترنت بتاريخ
24 يوليو 2007 م) .
<http://www.aawsat.com/details .>
- (2) — فهو لم يعد عملاً فردياً وإنما بات يتسم بالتنظيم بحيث أضحت الجماعات الإرهابية توثق
صلاقتها ببعضها البعض سواء على المستوى المحلي أو الدولي ، وتخضع في عملها لنظام محكم
بحيث أصبح الإرهاب من بين صور الجريمة المنظمة إن لم يكن أبرز أشكالها . (انظر في هذا
المعنى : د.محمود صالح العادلي ، السياسة الجنائية لدرء جرائم العنف الإرهابي — دراسة
مقارنة ، ط2 ، 1997م ، دار النهضة العربية — القاهرة ، ص5 — 7) .
وانظر كذلك : أحمد خليفة ، "بين الإرهاب وحقوق الإنسان" ، المجلة الاجتماعية القومية ،
المجلد (31) ، العدد (3) ، سبتمبر 1994م ، ص147 — 167 .
- (3) — خالد حنفي علي : "الإنترنت وتصدير الإرهاب" ، مجلة السياسة الدولية ، س 41 ، العدد
(162) ، أكتوبر 2005م ، ص136 — 139 .
ومن الوسائل الشائعة في التواصل بين الإرهابيين عبر شبكة المعلومات الدولية (الإنترنت) :
البريد الإلكتروني الدوار ، والمواقع الإلكترونية ، ووسائل التفاعل المباشر مثل ساحات
ومنتديات الحوار ، وهو عبارة عن برنامج يتيح لمستخدمي الشبكة التواصل فيما بينهم عن
طريق الحوار المباشر بالصوت والصورة .
- (4) — المعجم الوسيط ، ج1 ، ط1 ، دار أمواج للطباعة والنشر والتوزيع ، بيروت — لبنان ،
1987م ، باب الرء ، ص376 .
- (5) — يُراجع : قاموس المورد ، إنجليزي — عربي ، منير البعلبكي ، ط 14 ، دار العلم للملايين —
بيروت ، 1980م ، ص960 .

- (6) — انظر تفصيلاً حول مفهوم الإرهاب وتباين الرأي حياله :
- أ. مصطفى مصباح دبارة ، الإرهاب — مفهومه وأهم جرائمه في القانون الدولي الجنائي ، رسالة ماجستير ، كلية القانون ، جامعة قاريونس ، القسم الجنائي ، الطبعة الأولى ، منشورات جامعة قاريونس — بنغازي ، 1990م ، ص 128 — 134 ؛ د. أحمد شوقي أبوخطوة ، تعويض الجاني عليهم عن الأضرار الناشئة عن جرائم الإرهاب ، الطبعة الثانية ، دار النهضة العربية — القاهرة ، 1997م ، ص 42 — 45 ؛ اللواء الدكتور/حسين الحمدي بواوي ، الإرهاب الدولي بين التجريم والمكافحة ، دار الفكر الجامعي — الإسكندرية ، 2005م ، ص 23 — 28 ؛ د. صلاح الدين جمال الدين ، إرهاب ركاب الطائرات ، دار الفكر — الإسكندرية ، 2006م ، ص 17 — 19 .
- (7) — انظر بشأن تعريف الإرهاب : حسين الحمدي بواوي ، ص 21 .
- (8) — خالد حنفي علي ، الإنترنت وتصدير الإرهاب ، ص 139 .
- (9) — المصدر ذاته .
- (10) — وإن كان البعض يحاول التمييز بينهما :
- انظر : د. كوركيس يوسف داود ، الجريمة المنظمة ، رسالة دكتوراه ، الطبعة الأولى ، 2001م ، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع ، عمان — الأردن ، ص 63 — 64 .
- وحول علاقة الإرهاب بالجريمة المنظمة انظر : سناء خليل ، "الجريمة المنظمة عبر الوطنية — الجهود الدولية ومشكلات الملاحقة القضائية" ، المجلة الجنائية القومية ، المجلد (39) ، العدد (2) ، يوليو 1996م ، ص 87 — 124 .
- (11) — يُراجع في هذا الخصوص بحثنا الموسوم بـ "السياسة الجنائية في مواجهة جرائم الإنترنت Cyber Crimes" ، مقدم إلى المؤتمر لدولي لجامعة الطفيلة التقنية حول "التنمية البشرية والأمن في عالم متغير" ، الأردن ، خلال الفترة 10 — 12/07/2007م ، ص 8 ؛ د. محمد سامي الشوا ، ثورة المعلومات وانعكاساتها في قانون العقوبات ، ط2 ، دار النهضة العربية — القاهرة ، 1998م ، ص 87 .
- R. Gassin, Le droit pénal de L' informatique, D. 1988, chr. 35.
- (12) — انظر على شبكة الإنترنت : صلاح الصيفي ، الإرهاب الإلكتروني ... وحش جديد يصعب اصطياده ، آفاق ، تاريخ النشر 2008/2/4 .
- http://www.aafaq.org/malafat.aspx?id_mlF=43

(13) — انظر بشأن ذلك :

اللواء/محمود الرشيدى : "الجرائم الإلكترونية والتأمين الإلكتروني" ، قضايا [المركز الدولي للدراسات المستقبلية والاستراتيجية] ، العدد (11)، السنة الأولى ، نوفمبر 2005م ، ص30 — 32.

وكذلك : محمد أمين الرومي ، جرائم الكمبيوتر والإنترنت ، دار المطبوعات الجامعية — الإسكندرية ، 2004م ، ص56 — 60 ؛ د. عمر محمد بن يونس ، التحكم في جرائم الحاسوب وردعها (المراقبة الدولية للسياسة الجنائية) ملخص الترجمة العربية لمرشد الأمم المتحدة لعام 1999م (ترجمة وعرض) ، ص43 — 46.

(14) — على شبكة الإنترنت : الإرهاب الإلكتروني أحدث صرعة في معارك الصراعات الدولية الباردة .

[http:// www.annabaa.org/nbanews/63/351. htm](http://www.annabaa.org/nbanews/63/351.htm)

(15) — فالإرهابيون يمكنهم شن هجماتهم الإرهابية عن بعد ، ويكون حجم الدمار كبيراً .

(انظر على شبكة الإنترنت : مكافحة الإرهاب عبر الإنترنت ، من صحيفة الوطن ، الإثنين 26/5/2005م ، س13 ، العدد 4649) .

<http://www.alwatan-news.com/data 20080523/innercontent. asp? val= america 1-1>

(16) — انظر على الإنترنت نص الحوار الذي دار ضمن برنامج بانوراما بتاريخ الأربعاء 8/11/2007م على قناة العربية : "بانوراما : الإنترنت تحول إلى معسكرات تدريب للإرهاب"

<http://www.alarabiya.net/programs/2007/11/10/41472.htm>

(17) — انظر : اللواء محمود الرشيدى ، مجلة قضايا ، بحثه السابق ، ص 39 ، 40 ؛ وكذلك انظر على شبكة الإنترنت "الإنترنت تحول إلى معسكرات تدريب للإرهاب" ، على الموقع السابق ذكره ، تاريخ الزيارة 2/4/2008م .

(18) — انظر بشأن الوقوف على المزيد حول الحالات الواقعية عن التهديد الإرهابي عبر شبكة الإنترنت : اللواء الدكتور/حسين المحمدي بوادي ، ص90 — 96 .

(19) — المرجع نفسه ، ص97 وما بعدها .

(20) — انظر على الشبكة المعلوماتية (الإنترنت) : "تزايد خطير في مواقع الإرهاب على الإنترنت".

<http://arabic.rnw.nl/currentaffaires/ cur>

(21) — ويتم عادة تعقب المواقع المحرصة للإرهاب بقفلها أو اقتحامها ، ويستعان أحياناً ببعض

قراصنة الإنترنت أنفسهم (الهاكرز) لهذا الغرض . ويمكن من الناحية الفنية تتبع الإرهابيين عن طريق البروتوكول الخاص بالحواسيب أو ما يعرف بـ (ip-address) ، وإن كان هؤلاء الإرهابيون يلجأون في كثير من الأحيان إلى إقامة مواقع بديلة عوضاً عن تلك التي يتم قفلها أو كشفها ، كما يعملون على استخدام شبكة الإنترنت من خلال مقاهي الإنترنت بدلاً من الحواسيب الخاصة بهم تفادياً لكشفهم من قبل الأجهزة الأمنية . (انظر: خالد حنفي علي ، الإنترنت وتصدير الإرهاب ، ص139) .

(22) — يُراجع بحثنا السابق ، ص9 — 17 .

(23) — Convention on cyber crime Budapest, 23. XI. 2001.

لمعرفة المزيد عنها انظر على شبكة الإنترنت :

<http://www.conventions.coe.int/Treaty/EN/Treaties/htm/185.htm>

<http://www.conventions.coe.int/Treaty/EN/Cadreliste/Treaties/htm>

وبخصوص التعليق على أحكامها ومراحل إبرامها انظر :

د.عمر محمد بن يونس ، الجرائم الناشئة عن استخدام الإنترنت ، رسالة دكتوراه ، الطبعة الأولى ، دار النهضة العربية — القاهرة ، 2004م ، ص198 — 216 ؛ منير الجنيهي وممدوح الجنيهي ، بروتوكولات وقوانين الإنترنت ، دار الفكر الجامعي — الإسكندرية ، 2005م ، ص180 — 185 .

(24) — انظر بحثنا السابق ، ص20 — 25 .

(25) — المرجع نفسه ، ص17 — 19 .

والجدير بالذكر في هذا المقام أنه في إطار تطوير الأجهزة المعنية بمكافحة الجرائم المعلوماتية قامت الجماهيرية الليبية باستحداث إدارة خاصة لمكافحة هذه الطائفة من الجرائم تكون تبعيتها للإدارة العامة للأدلة والبحث الجنائي ، وذلك بموجب قرار أمين (وزير) اللجنة الشعبية العامة للأمن العام رقم (63) لسنة 2005م بشأن تقرير حكم في القرار رقم (131) لسنة 2004م بشأن التنظيم الداخلي للجهاز الإداري للجنة الشعبية العامة للأمن العام . وقد خُولت هذه الإدارة بموجب قرار إنشائها جملة من الاختصاصات من بينها وأهمها مكافحة جرائم الحاسوب والإنترنت وجرائم تقنية المعلومات الأخرى ، وتقديم الدعم الفني للمؤسسات العامة في مجال الأمن المعلوماتي ، والقيام بأعمال البحث والتحري وجمع الاستدلالات في الجرائم المذكورة ، كما عُهد إليها وضع وتنفيذ برامج التوعية في مجال الأمن المعلوماتي وجرائم الحاسوب والإنترنت والجرائم عالية التقنية بالتنسيق مع الجهات ذات

العلاقة، فضلاً عن وضع الأسس والضوابط لإدارة واستضافة مواقع المؤسسات العامة على الإنترنت والإجراءات الأمنية الواجب توافرها ، واختصاصات أخرى لا يتسع المقام لذكرها . والملاحظ أن هذه الاختصاصات واسعة جداً ، وأن الباب مفتوح لإضافة اختصاصات أخرى إليها ، ونظراً لما تشكله من قيود على حرية استخدام شبكة الإنترنت ، فكان ينبغي أن ينظمها قانون لا قرار وزاري .

(26) — انظر على شبكة الإنترنت : بول روجرز : "حماية أمريكا ضد الإرهاب عبر الإنترنت" .
<http://Usinfo.State.gov/journals/1101/ijpa/Focus4.htm>

(27) — المرجع ذاته .

(28) — انظر حول هذا الموضوع : "عبارة مكافحة الإرهاب شناعة الحكومات لانتهاك خصوصية الإنترنت" ، عن شبكة الأخبار العربية محيط .

الجمعة 23/مايو/2008م <http://www.moheet.co/show-news.aspx ? nid moheet.com>
<http://www.ara.reuters.com/article/internetnews>

(29) — انظر على الشبكة العالمية (الإنترنت) :
<http://www.annabaa.org/nbanews/63/351.htm>

(30) — انظر على الإنترنت :

<http://www.moheet.com/show-news.aspx ? nid>

(31) — انظر على الإنترنت : "الاتحاد الأوروبي يجرم الدعاية للإرهاب عبر الإنترنت" .
<http://www.halwasat.com/content/view/2706/109/>

(32) — انظر على شبكة المعلومات : د. إبراهيم علوش : "قوانين مكافحة الإرهاب الأمريكية : إجراءات مؤقتة أم انقلاب على الدستور ؟" .

<http://www.Freearabvioce.org/arabi/new newAmerican laws.htm>

(33) — انظر على الشبكة الدولية : "المعلوماتية تفتح أبواب مكافحة الإرهاب ونقص التعاون الدولي يغلقها" .

<http://www.al-Jazirah.com.Sa/digimag/16072006/gadeia 14.htm>

(34) — انظر نص التقرير المذكور على شبكة الإنترنت "الاتحاد في مواجهة الإرهاب" .
<http://www.un.org/arabic/unitingagainst terrorism/chapter3./htm>