رابطة العالم الإسلامي

الأمانة العامة

الإدارة العامة للمؤتمرات والمنظمات

أثر ظاهرة الإرهاب الإلكتروني في نشر الفكر المتطرف

« دراسة تحليلية »

إعداد

الدكتور أحمد محمد فرحان

الأستاذ المساعد بكلية إدارة الأعمال بجامعة الملك فيصل - الأحساء

مقدم إلى

مؤتمر مكة المكرمة السادس عشر

الشباب المسلم والإعلام الجديد

الذي تنظمه

رابطة العالم الإسلامي

تحت رعاية خادم الحرمين الشريفين

الملك سلمان بن عبد العزيز آل سعود

مكة المكرمة

٣ - ٤ / ذو الحجة / ١٤٣٦ هـ ، الموافق ١٦ - ١٧ / سبتمبر / ٢٠١٥ م

رابطة العالم الإسلامي

مكة المكرمة – المملكة العربية السعودية

صندوق البريد (٥٣٧) أو (٥٣٨) مكة المكرمة (٢١٩٥٥)

هاتف: ٠٠٩٦٦١٢٥٦٠٠٩١٩ – الفاكس: ٥٦٠١٣١٩ – ٥٦٠١٢٦٧

برقياً: رابطة – مكة، تلكس: ٥٤٠٠٠٩ و٥٤٠٣٩٠

www.themwl.org

البريد الإلكتروني للإدارة العامة للمؤتمرات والمنظمات

conferences@themwl.org

واتس أب : (٠٠٩٦٦٥٠٣٣٩٦٣٢٠) : whatsApp

بسم الله الرحمن الرحيم

المحدد الأول: الإطار العام للدراسة

مقدمة ومشكلة الدراسة:

الحمد لله رب العالمين، والعاقبة للمتقين، والصلاة والسلام على أشرف الأنبياء والمرسلين، سيدنا ونبينا محمد وعلى آله وصحبه أجمعين، أما بعد:

يسعى الإرهاب الآثم جاهداً إلى زعزعة دعائم الأمن للأفراد والمجتمعات، وذلك من خلال ما يتم استخدامه من أسلحة غير مشروعة مجتمعياً ودينياً، ولعل من أهم هذه الأسلحة: الإرهاب الإلكتروني؛ الذي يؤثر على كافة مرافق المجتمع الرقمية، فعلى الرغم من الفوائد الجمة للوسائل الإلكترونية والتكنولوجية الحديثة؛ إلا أن سهولة استخدامها قدمت إلى هذه الجماعات المتطرفة أداةً تمكِّنهم من محاربة المجتمعات، والتي أصبحت مصابة بهاجس الرعب من الهجمات التخريبية الضارة الناتجة عن الإرهاب الإلكتروني.

وعلى الرغم من اتخاذ الدول كافة التدابير الممكنة لحماية أجهزتها من الآثار الضارة لهذه الهجمات؛ إلا أن هذه المحاولات لم تمنعها، فلقد ارتبطت تقنيات عصر المعلومات ببروز أذرُع الإرهاب الإلكتروني، والذي قدَّم للجماعات المتطرفة أدواتِ الاتصال التي تمكِّنهم وبأسلوب ميسَّر من تكوين شبكات دولية، وكذلك استقطاب الشباب وضِعاف النفوس من مختلف أنحاء العالم الذي أصبح قرية صغيرة.

فنظراً لتعدد أشكال وأساليب هذا النوع من الإرهاب، واتساع مجال الأهداف التي يمكن تدميرها من خلال الاعتماد على تقنية المعلومات؛ يمكن

القول إنه إرهاب المستقبل، والذي يوفر للإرهابيين أداةً تؤدي إلى إلحاق حجمٍ هائل من الخسائر مع تمتعهم بقدْر كبير من السلامة والأمان.

فالإرهاب الإلكتروني يستهدف أولاً البِنيةَ التحتيةَ للمجتمع، والتي أصبحت الآن تُدار عن طريق الحاسبات الآلية، فيتسبب في خسائر مادية هائلة تصيب حركةَ الملاحة الجوية أو البحرية أو شبكات الكهرباء والنظام المالي للدول، من خلال إلحاق الضرر بالبنوك والمؤسسات المصرفية.

وعليه فإن مشكلة البحث تَبرز في «تَنامي ظاهرة الإرهاب الإلكتروني وخاصةً في المجتمعات الرقمية»، وترتبط ظاهرةُ التطرف بهذه الظاهرة ارتباطاً طردياً، فتستخدم الوسائل التكنولوجية كسلاح تدميري من جهة، وكأداة لبث أفكارها وتجنيد المزيد من الأتباع من جهة أخرى، وتزداد وطأة هذه الأسلحة مع الانتشار السريع للوسائل والأجهزة التكنولوجية، وانخفاض تكلفتها وعدم القدرة على إثبات جرائمها.

أهداف الدراسة:

تهدف إلى الوقوف على ماهية الإرهاب الإلكتروني وعلاقة هذه الظاهرة بالتطرف، مع توضيح الدور الذي تلعبه شبكات المعلومات في نشر أفكار ومبادىء التنظيمات الإرهابية، وتوضيح الجهود الدولية والمحلية التي بُذلت للحد من هذه الظاهرة، وذلك بهدف وضع برنامج شامل ومتكامل لإدارة مخاطر ظاهرة الإرهاب الإلكتروني؛ اعتماداً على الآليات التقنية والأمنية والعسكرية والسياسية التي تُستخدم في تخفيض تبِعات الإرهاب الإلكتروني، والتي تمثل أحدَ أهمِّ أذرُع ظاهرة التطرف.

أهمية الدراسة:

تَبرز أهمية دراسة الإرهاب الإلكتروني في تقديم مجموعة آلياتٍ تهدف إلى حماية المجتمعات من تبِعات هذه الظاهرة السلبية، من خلال إلقاء الضوء على الدور الذي يجب أن تتبناه الدول والجماعات والأفراد للتصدي لها والوقاية منها، ذلك بالإضافة إلى تقديم بعض التوجيهات التي تزيد من مقدار الوعي لدى الأفراد من كافة المجتمعات، بالوسائل والطرق التي تلجأ إليها التنظيمات الإرهابية لاستقطاب وتجنيد هؤلاء الأفراد.

منهجية الدراسة:

سوف تجمع منهجية الدراسة بين عدة مناهج بحثية لخدمة الجانبين العلمي والعملي؛ لإحداث تكامل فيما بينهما لتحقيق هدف الدراسة، حيث سيتم اتباع المناهج البحثية التالية كل بقدر الحاجة:

١- المنهج الاستقرائي: حيث يتم استقراء ومراجعة البحوث والدراسات المتعلقة بالمشكلة قيد البحث، سواء تعلقَت بظاهرة الإرهاب الإلكتروني أو ظاهرة التطرف.

٢- منهج تحليل المحتوي: حيث سيتم تحليل الأفكار والعلاقات والمداخل والجوانب العملية والعلمية التي ستشتمل عليها البحوث والدراسات التي سيتم استقراؤها بما يَخدم أهدافَ البحث.

٣- المنهج التطبيقي: حيث سيتم دراسةُ الوسائل والآليات التي تكون قابلةً للتطبيق كحلولٍ مقترحة لعلاج ظاهرة الإرهاب الإلكتروني.

المحدد الثاني

تحليل الاتجاهات التي تناولت موضوع الدراسة

انطلاقـاً مـن أهميـة اسـتقراء الاتجاهـات التـي تناولـت موضـوع الإرهـاب الإلكتروني وأثره في نشر الفكر المتطرف؛ فإن الباحث يستعرض في هـذا الجـزء؛ الأبحاث والدراسات التي حفلت بها المعرفة من حيث الأهمية والمفهوم، ومن أبرز الدراسات السابقة في هذا المجال:

١ - دراسة أيسر محمد عطية:

عنوانهـا: «دور الآليـات الحديثـة للحـد مـن الجـرائم المسـتحدثة»، تنـاول الباحث فيها ماهية الإرهاب الإلكتروني وبيان أشكاله ووسائله، وتوضيح مـدى تَنامي الدور الذي يلعبه الإنترنت في نشر الأفكار والمبادئ المتطرفة، وخلُصـت الدراسة إلى أن الإرهاب الإلكتروني يشكل تهديداً قويـاً للـدول والمجتمعـات، وأن أكثر الوسـائل المسـتخدمه في الإرهـاب الإلكـتروني: هـو البريـد الإلكـتروني (أيسر، ٢٠١٤).

٢ - دراسة رانيا نظمي:

عنوانها: «الفراغ الفكري وتأثيراته على الاستخدام السيئ لتقنية الاتصـالات الحديثة»، قُدمت ضمن بحوث مؤتمر الإرهاب ٢٠٠٩؛ تهدف إلى التعرف على مخاطر هذه الظاهرة وآثارها بين أفراد المجتمع، والوقـوف علـى الـدور الـديني والتربوي والاجتماعي في التصدي لهذه الظاهرة، والتعـرف علـى قنـوات التـأثير في نشـر الفكـر المنحـرف، وقـد توصـلت الدراسـة إلـى أهميـة دور التكنولوجيـا بشِـقيها المـادي والمعنـوي، وبنوعيهـا المدنيـة والعسـكرية؛ في دعـم النشـاط الإرهابي (رانيا، ٢٠٠٩).

٣- دراسة عبد الله بن عبد العزيز بن فهد العجلان:

عنوانها: «الإرهاب الإلكتروني في عصر المعلومات»، طُرحت ضمن بحوث المؤتمر الدولي الأول لحماية أمن المعلومات، وهدفتْ إلى محاولة استكشاف وتحديد معالم الظاهرة الإرهابية المستحدثة التي تعتمد على استخدام الإمكانيات العلمية والتقنية واستغلال وسائل الاتصالات وشبكات المعلومات، وذلك من خلال تحديد مفهوم هذه الجريمة وبيان أسبابها ودوافعها وخصائصها وأهدافها، ومن ثم إبراز أهم مظاهرها وأشكالها، وقد توصلت الدراسة إلى أن الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم (عبد الله، ٢٠٠٨).

٤- دراسة عبد الحميد ابراهيم محمد العريان:

عنوانها: «العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة»، وقد تناولت العوامل الفاعلة في انتشار جرائم الإرهاب وكيفية التصدي للجرائم المعلوماتية ودور المجتمع المدني في مكافحة هذه الظاهرة، وأوصى الباحث بضرورة التدخل التشريعي لمواجهة القصور في التشريعات والقوانين الحالية (عبد الحميد، ٢٠٠٦).

٥- دراسة عبد الرحمن بن عبد الله السند:

عنوانها: «وسائل الإرهاب الإلكتروني، حكمها في الإسلام وطرق مكافحتها»، تمثل هذه الدراسةُ أحدَ أهم المصادر العلمية في هذا التخصص، وقد تناولَت المقصودَ بالإرهاب الإلكتروني ووسائله وطرق مكافحته، وتوصلت إلى أن التعاملات المرتبطة بالتقنية لابد وأن تخضع لأحكام الكتاب والسنة، كما أكدت على أن البريد الإلكتروني يمثل أهمَّ وسائل هذه الظاهرة، كما أن المواقع الإلكترونية هي القناة التي يقوم من خلالها الإرهابيون ببث أفكارهم ومعتقداتهم (عبد الرحمن، ٢٠١٠).

٦- دراسة عبد الصبور عبد القوي علي:

عنوانها: «الجريمة الإلكترونية والجهود الدولية للحد منها»؛ وتناولت تحديدَ طبيعة الجريمة الإلكترونية والأسبابَ الدافعة لها، وأهم صور الاعتداء الجنائي على المعلومات في الإنترنت، وأكدت الدراسة على ضرورة التعاون الدولي للحد من الجرائم الإلكترونية بما يضمن استحداثَ إطارٍ لتبادل الخبرات وإيجاد تشريعٍ دولي وتبني منظومة معلوماتية موحَّدة تعتمد إنشاء مكتب عالمي أو إقليمي للتوثيق الإلكتروني (عبد الصبور، ٢٠٠٨).

٧- دراسة كريمة شافي جبر محمود:

عنوانها: «الإرهاب المعلوماتي»؛ وهدفت إلى التعرف على الإرهاب المعلوماتي وكيفية معالجته من خلال زيادة كفاءة أجهزة الحماية الأمنية لأنظمة المواقع الإلكترونية للحفاظ على سرية المعلومات، ولقد توصلت الدراسة إلى أن من أهم العوامل التي يمكن الاعتمادُ عليها حتى يتم احتواء هذه الظاهرة: محاولة حماية البِنية التحتية من خلال صياغة سياسات أمنية وطنية وتدريب الكوادر المعلوماتية، ثم الارتقاء بأمن النظم المعلوماتية وعزل الموارد المعلوماتية بالغة الأهمية (كريمة، ٢٠١٠).

٨- دراسة مصطفى محمد موسى:

عنوانها: «التنظيمات الإرهابية وشبكة الإنترنت» وتناولت تحديدَ ماهية التنظيمات الإرهابية، وأنواعَ شبكات المعلومات، والخدماتِ التي تستخدمها التنظيمات الإرهابية في شبكة المعلومات، والأساليبَ الجديدة التي تتبعها في التجنيد واختراق شبكات المعلومات، وتوصلت إلى أن معظم الدول العربية لم تُصْدر تشريعات تُجرِّم استخداماتِ التنظيمات الإرهابية، وأوصت بضرورة دعوة

شركات أمن المعلومات الإلكترونية للمشاركة العلمية في الندوات والمؤتمرات المحلية ذات الصلة بموضوع الإرهاب الإلكتروني (مصطفى، ٢٠٠٧).

٩- دراسة يوسف بن أحمد الرميح:

عنوانها: «الإرهاب والجريمة الإلكترونية بالمجتمع»، وقد تناولت مفهومَ ظاهرة الإرهاب الإلكتروني وأبعاد وسمات هذه الجريمة وأساليب الجرائم الإرهابية التقنية، ودور المجتمع تجاه تلك الجرائم، وأوصت بضرورة أن تقوم الجهات الأمنية والتشريعية القضائية بتطوير أساليبها ووسائلها حتى يمكنها التعامل مع جرائم ثورة المعلومات الحديثة، ومواجهة تلك الجرائم الإلكترونية بأسلوب علمي متطور وغير تقليدي (يوسف، ٢٠١٤).

رؤية الباحث حول ما تضمنته الدراسات السابقة:

دراسة ظاهرة الإرهاب الإلكتروني تمثل تحدياً كبيراً أمام الباحثين؛ ذلك لأنها تتضمن أكثر من منظور، فبالإضافة إلى الجانب التقني؛ هناك المنظور الديني والسياسي والاقتصادي والعسكري، لذا فهناك حاجة للمزيد من الكتابات في هذا، فالمتأمل للدراسات السابقة يجدها ركزت على جانب واحد فقط: إما التقني أو الديني أو السياسي، وتناولت هذه الظاهرة من رؤية خارجيةلم تتعمق في دراستها ولم تضع آليات واضحة يمكن تطبيقُها، الأمر الذي دعاني لوضع برنامج متكامل يتضمن مجموعة من الممارسات التي تهدف إلى الحد من تبِعات هذه الظاهرة السلبية التي تعاني منها كل المجتمعات، وذلك من خلال تحليل لنتائج الدراسات السابقة، ثم تكوين رؤية شاملة متعمقة لمفهوم ودوافع تلك الظاهرة، الأمر الذي يضمن الوصولَ إلى نتائجَ فعالةٍ تمكِّننا من مواجهة ظاهرة الإرهاب الإلكتروني، والتي تمثل أحدَ أهم أدواتِ التنظيمات المتطرفة.

المحدد الثالث

تأصيل علمي لمفهوم وأبعاد ظاهرة الإرهاب الإلكتروني

ابتُليت المجتمعاتُ الحديثةُ والدولُ المتقدمةُ بالتطور الإلكتروني والتكنولوجي؛ والذي نتج عنه الإرهابُ الإلكتروني، فرغم الفوائد الهائلة للوسائل التكنولوجية الحديثة في أي مؤسسة أو نظام؛ إلا أن سهولة استخدامِها والتحكمِ بها عن بُعد؛ قدم سلاحًا للجماعات المتطرفة يمكِّنها من اختراق الأجهزة الأمنية للدول وتهديدها والتجسس عليها وإلحاق الضرر بها، مع توفير أكبر قدر من السلامة والأمان لمرتكبي هذه الجرائم، وصارت شبكات المعلومات أداةً لاستقطاب الشباب وتجنيدهم، والمؤسف أن ٨٠٪ من المنتمين لتنظيم داعش الإرهابي؛ تم تجنيدُهم عن طريق مواقع التواصل الاجتماعي، أي أن المواجهة مع الإرهاب لم تُصبح بعدُ مواجهةً ماديةً فِعليةً على أرض الواقع، بل انتقلت لتصبح مواجَهةً من خلال الفضاء الإلكتروني.

أولاً: مفهوم الإرهاب الإلكتروني:

- عرَّفه باحثٌ بأنه: «الاستخدام المحرض سياسيًا للحاسوب بوصفه سلاحًا أو هدفًا بواسطة مجاميع أو عملاء؛ تهدف إلى إثارة الرعب ونشره؛ للتأثير في أفراد المجتمع أو إكراه الحكومة على تغيير سياستها الوطنية لصالح أهداف هذه المجاميع» (Clay, 2003)، وأرى أن هذا التعريف تناول الظاهرة من الجانب السياسي والفني على أنها تمثل إدارة للجماعات وحدها دون غيرها ولم يتناول تأثير الأفراد.
- وعرَّفه مركز حماية البنية التحتية الوطنية الأمريكي (NIPC) بأنه: «فِعل إجرامي يمارَس بواسطة الحاسوب أو أدواته،فيُفضي إلى نشر العنف

والموت أو التدمير وإثارة الهلع والإرهاب؛ لإكراه حكومة أو نظام سياسي على تغيير سياسته» (كريمة، ٢٠١٠).

- وعرَّفه عبد الرحمن السند بأنه: «العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية؛ الصادر بغير حقٍ من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عِرضه أو عقله أو ماله، بشتى صنوف وصور الفساد في الأرض» (عبد الرحمن،٢٠٠٧).

ونلاحظ ازدياد الخطورة الإجرامية للجماعات المتطرفة، والتي قامت بتوظيف إمكانتها لإتمام عمليتها الإجرامية، ويعتمد هذا النوع من الإرهاب على استخدام شبكات المعلومات من أجل إلحاق الضرر بالآخرين وتهديدهم وابتزازهم ونشر الفوضى (عبد الله، ٢٠٠٨).

وقد سماه بعض الباحثين: «الإرهاب الأخضر»، وجعله الدكتور محمد بن على البشي: أخطر أنواع الإرهاب التي تواجه المجتمعات بصفة عامة والمملكة بصفة خاصة؛ وعُرف بالأخضر لأنه يعتمد على الإرهاب المبنِي على النظم التكنولوجية وشبكات المعلومات الدولية، فمن خلالها يستطيع الإرهابيون اختراق النظم الأمنية واستعراض الخطط الأمنية وتحديد مكانها وزمانها دون تكلفة، مع عدم الحاجه إلى مواجهة مباشرة تُحدث دماراً هائلاً لنظم الأمن المجتمعية (كريمة، ٢٠١٠).

ويمكن تقسيم جرائم الإرهاب الإلكتروني إلى: جرائم تستهدف المعلومات لتدميرها، وجرائم تستخدم وسائل التكنولوجيا كأدواتٍ لارتكاب جرائمها عن بُعد، وجرائم ترتبط بمحتوى مواقع المعلومات والتي تمكِّنها من بث أفكارها المتطرفة (يوسف، ٢٠١٤).

ثانياً: العوامل التي أسهمَت في نمو ظاهرة الإرهاب الإلكتروني:

قد يتبادر إلى الأذهان تساؤلٌ على قدرٍ كبير من الأهمية: «ما هي المحفزات التي أدت إلى النمو العنكبوتي لمثل هذه الظاهرة»؟ والإجابة: أن دوافع الإرهاب الإلكتروني هي نفسها أسباب الإرهاب، فهي مكون من مكوناته، وهناك عدة أسباب متداخلة ومتشابكة أسهمت في نمو هذه الظاهرة؛ بعضٌ منها شخصية، والأخرى فكرية وسياسية واقتصادية واجتماعية، وذلك ما جعلها جديرة بالبحث والدراسة.

ظاهرة الإرهاب الإلكتروني ظاهرة مركَّبة ومعقَّدة، ومن خلال نظرة مدققة لدوافعها؛ نجدها متولدة من الدوافع الخاصة بظاهرة الإرهاب والتطرف، والتي نتجت عن التفريط في أوامر الله سبحانه وتعالى، والوقوع فيما نهى عنه، مروراً بالدوافع الشخصية كالنقمة على المجتمع، والإخفاق الدراسي، وانعدام أهمية الشخص في أسرته ومجتمعة، والإخفاق في تحقيق الرغبات والأهداف، والرغبة في الظهور والسيطرة.

كما أن للدوافع الفكرية درجة عالية من الأهمية؛ لما تمثله من تحول الشخصية بالاتجاه إلى التطرف والتشدد والجهل والفهم الخاطئ لأحكام الشريعة، بينما تمثل الدوافع السياسية الإطار التنفيذي التحولي للشخصية المتطرفة كضعف موقف المجتمع والإحباط السياسي وغياب العدالة الإجتماعية داخل الدولة.

ولا يجب أن نُغفل الدورَ المهم للدوافع الاقتصادية في نمو ظاهرة الإرهاب، والتي تنطوي على عناصر؛ أهمها سهولة تحويل الأموال اللازمة لدعم الإرهاب كنتيجة للتقدم العلمي والتقني، وانتشار البطالة في المجتمع، كما

أن هناك دوراً كبير تلعبه الدوافع الاجتماعية والتي يرى البعض أنها تمثل أحد الأركان الأساس للتطرف، والتي تُعزَى للتفكك الأسري والإجتماعي وغياب مقومات التربية السليمة والفراغ وفقد الهوية المجتمعية.

الخصائص المميزة لظاهرة الإرهاب الإلكتروني:

ويمثل الإرهاب الإلكتروني أحد القنوات الرئيسة والفاعلة للتطرف؛ وعليه فإن كلاً من دوافع الإرهاب؛ هي أيضاً دوافع للإرهاب الإلكتروني، والذي بات سلاحاً سهلاً للجماعات والمنظمات الإرهابية، ومن العوامل التي تميز الإرهاب الإلكتروني على وجه الخصوص:

١- غياب المركزية في السيطرة والرقابة على شبكات المعلومات، والتي هي أحد أهم نتائج ظاهرة الفراغ التنظيمي والقانوني لدى بعض المجتمعات.

٢- طمْس معالم الجريمة الإلكترونية؛ الأمر الذي يجعلها جريمة صعبة الإثبات.

٣- إنخفاض تكلفة سلاح الجريمة المتمثل في بعض الأجهزة الإلكترونية واستخدام شبكات المعلومات.

٤- كون شبكة المعلومات مفتوحة للجميع، وضعف بِنْية الشبكات المعلوماتية، وقابليتها للاختراق.

٥- انخفاض مستوى المَخاطر بالنسبة لمرتكبي الجريمة وعدم الحاجة لإثبات الهوية الشخصية (عبد الله، ٢٠٠٨).

ثالثاً: أبعاد ومحددات جريمة الإرهاب الإلكتروني:

الإرهاب الإلكتروني أحد الجرائم التي تواجه المجتمع، ومن أهم طرق مواجهته: الإلمام بالأبعاد المختلفة لهذه الجريمة، فمن وراء الشعارات الدينية البراقة؛ تنطلق أبواق التنظيمات الإرهابية التي تزعم أنها خلف مظلة دينية توهم المجتمع أنها للمصلحة العامة، معتمدة في ذلك على ارتباك وتخبُّط بعض الحكومات؛ الأمر الذي يولد إحباطاً لدى العامة ويدفعهم للتعلق بآراء هذه الفئات ظناً منهم أنها المنقذ، فالظروف السياسية والاجتماعية والثقافية؛ عملت لتوليد هذه الأنظمة المخربة، وكان لوسائل الإعلام والاتصالات المفتوحة؛ العامل الأكبر لتنميتها؛ فهذه التنظيمات تتميز بطابعها غير الحدودي مما يجعلها عابرة للأقطار، سواء في مجال حرصها الدائم على التواصل مع الجماهير وبث أفكارهم الهدامه، أو في مجال الجريمة الإلكترونية (يوسف، ٢٠١٤).

واعتماد الجريمة على تقنية المعلومات؛ يجعلها عملية مستحدَثة ومتطورة تقنياً، بخلاف خروجها عن الحدود الإقليمية في جميع مراحلها؛ سواء الإعداد أو التنفيذ أو الآثار المترتبة عليها عاجلة وآجلة، ويزيد جرائم الإرهاب الإلكتروني تعقيداً: ازدياد أعداد مرتكبيها وتعدد جنسياتهم؛ خاصة عندما تصيب هذه الجرائم البنية التحتية المجتمعية؛ ونلاحظ أن عنصر السرية يمثل الغطاء الآمن للتنظيمات الإرهابية، وهناك علاقة طردية بين درجة السرية وتعاظم حجم الخسائر والأضرار المتولدة عن الجريمة، ومرتكبو هذه الجرائم على درجة عالية من الخبرة والتعامل مع التكنولوجيا والتقنية، مما يجعلهم يحرصون على عدم ترْك دليل مادي بعد ارتكابهم الجريمة، فضلاً عن أن غياب الهوية والدليل الرقمي وسهولة إتلافه وتدميره؛ يُصعِّب إثباتَ هذا النوع من الجرائم،وما يزيد الأمر صعوبةً وتعقيداً؛ وجودُ نقص في خبرة بعض الأجهزة

الأمنية، وعدم مواكبتهم للتطورات التقنية، بالإضافة إلى أن هذه الجريمة غير خاضعة لنطاق إقليمي محدد؛ حيث إنها دولية، والمتفحص لمعالم الجريمة الإلكترونية؛ يجد أنها لا تحتاج إلى العنف والقوة؛ بل تتطلب وجود أدوات تكنولوجية حديثة (عبد الله، ٢٠٠٨).

وتتطلب طبيعة الإرهاب الإلكتروني؛ اللامحدودية في التصنيف، لأنها تعتمد أساليب وآليات متطورة، فأشكال الإرهاب الإلكتروني لا تخرج عن التهديد والقصف الإلكتروني عبر الإنترنت من خلال رسائل البريد الإلكتروني، ومحاولة تدمير أنظمة المعلومات من خلال اختراق شبكة الإنترنت بهدف التخريب، بالإضافة إلى سرقة المعلومات عن طريق التجسس على المعلومات الاقتصادية والسياسية والعسكرية والشخصية.

وتؤكد الأبحاث الحديثة على أن شبكة التواصل الاجتماعي؛ تمثل أحد قنوات الانتشار للتنظيمات الإرهابية والجماعات المسلحة التي لم تَعد تعتمد على القوة العسكرية فقط في تحقيق أهدافها؛ بل تعتمد أيضاً على وسائل الاتصال والإعلام كأداةٍ لنشر أفكارها، وللحصول على الدعم المادي والمعنوي (هايل، ٢٠٠٨)

رابعاً: الأهداف المختلفة للإرهاب الإلكتروني:

تناوَل الكثير من المحللين الاستراتيجين؛ الأهداف المتوقعة للهجمات الإرهابية المحتملة كنتيجةٍ للإرهاب الإلكتروني، حيث يعتمد منفذو جرائم الإرهاب الإلكتروني؛ على تحقيق أهداف غير مشروعة،والخطر هنا في سهولة استخدام هذا السلاح الرقمي مع شدة أثره وضرره وازدياد مخاطره في الدول المتقدمة التي تدار بِنيتُها التحتية بالتقنية التكنولوجية المتقدمة، ومن هذه

الجرائم: الاستيلاء على الأموال، إثارة الرأي العام، تهديد السلطات العامة والمنظمات الدولية، الانتقام من الحكومات بإلحاق أضرار بالبِنية التحتية ووسائل الاتصال وتقنية المعلومات بالمنشآت العامة والخاصة، فالإرهاب الإلكتروني أصبح خطراً يهدد العالم بأَسْره، مما يعرِّض سلامةَ المجتمع وأمْنه للخطر، ويصيب النظامَ العام والأمنَ المعلوماتي بالخلل، كالتأثير السلبي المتعمَّد على نُظم المواصلات، من خلال الاختراق العمد لنُظم التحكم المروري: الجوي والبري والبحري، بإحداث أخطاء زمنية تؤدي إلى كوارث مرورية؛ كتغير توقيت فتح المدرج للطائرات أثناء الهبوط؛ مما قد يؤدي إلى كارثة اصطدام طائرتين، وقد تمتد هذه الأيدي الغادرة إلى استهداف نُظم الاتصالات، مما يؤدي إلى منع الاتصال بين أجهزة ومؤسسات الدولة ويصيبها بالشلل، وفي كثير من الأحيان؛ يعتمد منظمو هذه الهجمات على تدمير شبكات توليد الطاقة وتوزيعها؛ مما يؤدي إلى تعطُّل مرافق الدولة (حسن، ٢٠٠٧).

ومن أقدم الجرائم المعلوماتية: جرائم الاستيلاء على الحسابات والأرصدة المصرفية، واستخدام التقنيات الحديثة في تحويل الأموال وإحداث خلل في الأسواق المالية، ومن أخطر السيناريوهات التي تضعها الجماعات المتطرفة: استهداف القوات المسلحة ونُظم المعلومات المرتبطة بوزارة الدفاع، من خلال اختراق نُظم الدفاع الجوي والتحكم في أنظمة الدفاع والصواريخ الموجهة عن بُعد (كريمة،٢٠١٠) (عبد الله، ٢٠٠٨).

ورغم تعدد مجالات استخدام سلاح شبكة المعلومات في الجرائم الإرهابية؛ إلا أن هناك مجموعة من الأهداف المحددة التي تسعى لها هذه التنظيمات التي لا تخرج عن محاولة الحصول على تمويل استخدامه كأداة للتنسيق لشن هجمات إرهابية وإعطاء التعليمات.

المحدد الرابع: ديناميكية تنفيذ المخططات الإرهابية وبث الفكر المتطرف من خلال المنظومة الإلكترونية

تعتمد المنظمات الإرهابية المتطرفة على عدة وسائل تمكِّنها من تحقيق جرائمها غير المشروعة بحيث يتولد ضرر عام وبث الرعب والسيطرة والتأثير على متخذي القرار، فشبكة الإنترنت تمثل شبكة معلوماتية ينطبق عليها جميع محددات نموذج المعلومات ذو الأبعاد الثلاثة والتي تتناول حفظ المعلومات باستخدام أدوات الحفظ لأجهزة الحاسب الآلي، بالإضافة إلى سلامة المعلومات عن طريق عدم تغيير المعلومات المخزنة على الأجهزة، وضمان حفظ المعلومات المخزنة بطريقة آمنة وسرية (عبد الحميد، ٢٠٠٦).

أذْرُع الإرهاب الإلكتروني:

١- البريد الإلكتروني: أكثر القنوات المستخدمة في التواصل بين أفراد الجماعات الإرهابية على مستوى العالم، وكقناةٍ لنشر الأفكار المتطرفة والترويج لها بين الفئات المتعاطفة معهم عبر المراسلات الإلكترونية.

٢- شبكات المعلومات كبديلٍ لمعسكرات التدريب التي ربما ينكشف أمرُها وتكون عُرضةً للمهاجمة، ويتم ذلك من خلال تقديم برنامج تدريب متكامل يتضمن التدريبات البدنية وكيفية التخطيط للهجمات الإرهابية (صغير،٢٠١٣).

٣- شبكة المعلومات لنشر ثقافة الإرهاب والتطرف والترويج لها من الجماعات المتطرفة؛ والتي تسعى إلى جذْب أكبر عدد من الراغبين في تبنِّي أفكارهم؛ وذلك بتقديم قاعدة فكرية متكاملة تتضمن عباراتٍ حماسيةً بأسلوب عاطفي تساعدهم على تجنيد المزيد من الشباب.

٤- شبكات المعلومات كوسيلة للتخطيط والتنسيق لشن هجمات إرهابية بعيداً عن أعين الجهات الأمنية؛ فالعمليات الإرهابية معقدة، واستخدام الإنترنت يوفر مخزوناً من المعلومات التي تحتاجها المنظمات الإرهابية في تنفيذ هجماتهم، فهي موسوعة إلكترونية متعددة الثقافات والمعلومات التي تتصل بمواقع المنشآت الحيوية ومواعيد الرحلات الجوية (خالد، ١٤٢٣)، فانخفاض تكلفة وسائل الاتصال من خلال شبكة المعلومات؛ يتيح للجماعات الإرهابية قناةَ اتصالٍ تسمح لهم بالتنسيق وتبادل المعلومات دون الكشف عن هوياتهم، وتدمير شبكة معلوماتية؛ خسائره اليومية أضعاف خسائر انهيار مبنى أو قصف منشأة أو تفجير جسر أو اختطاف طائرة (عبد الله، ٢٠٠٨).

٥- «الاعتصام والحصار الافتراضي» الذي يهدف إلى توقف عملية الدخول للحسابات وإحداث خلل مؤقت أو دائم في نُظم التشغيل الإلكترونية من خلال الاعتماد على الفيروسات.

٦- «قنبلة البريد الإلكتروني» بإرسال آلاف الرسائل الإلكترونية مما يؤدي إلى كفه عن العمل.

وقد قام أحد الباحثين بتقسيم طرق وأساليب الجرائم الإلكترونية طبقاً للهدف من حدوث الجريمة، فهناك جرائم الاستيلاء على الأموال من خلال التسول عبر الإنترنت، والاستيلاء على المعلومات السرية لحسابات الائتمان، وسرقة المعلومات المالية، واختراق الحسابات المصرفية، وتحويل مبالغ مالية من حسابات العملاء إلى حسابات المخترقين، وجريمة الائتلاف المعلوماتي وتزوير البيانات والمعلومات أو المخرجات الكومبيوترية الخاصة بالحكومة الإلكترونية، وأساليب الجرائم الرقمية في الاعتداء على النفس والعِرض

بالمواقع الإباحية، وتعتمد الجماعات الإرهابية هذه الوسائل للابتزاز والحصول على المال والمعلومات.

وتعتمد التنظيمات الإرهابية على القنوات التكنولوجية في بث أفكارها؛ من خلال إنشاء مواقع على شبكة الإنترنت تدعو إلى معتقداتهم ومبادئهم، وقد يمتد إلى تعليم الطرق والوسائل التي يتم الاعتماد عليها عند تنفيذ العمليات الإرهابية؛ كصناعة المتفجرات، وكيفية اختراق الحسابات السرية والبنكية، والدخول على المواقع المحجوبة، واختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية.

صار الإعلام أداةً مساندةً للإرهاب؛ فيستغل الإرهابيون البلبلةَ الإعلاميةَ الناتجة عن تباين وتناقص الأخبار المتعلقة بأي حدث إرهابي بحيث تزداد صعوبة تحديد هوية الفاعل ومطاردته على الفور (رانيا، ٢٠٠٩).

كما تُمثل شبكة الإنترنت مكاناً آمناً لالتقاء أفراد التنظيمات المتطرفة والمجرمين؛ وذلك لنقل خبراتهم فيما يتعلق بطرق تنفيذ الجرائم الإرهابية، مدعمين تنظيماتهم باستقطاب الشباب ذوي النفوس الضعيفة، وتسمح الشبكة أيضاً لقيادات الجماعات المتطرفة بإصدار بيانات إلكترونية ونشرها عبر وسائل الإعلام، ثم تصل إلى مختلف شرائح المجتمع، وهذه البيانات تأخذ أشكالاً مختلفة تتضمن رسم أهدافاً وخططاً عامة للتنظيم أو التهديد والوعيد بشن هجمات إرهابية، أو تبنِّي تنفيذ عمليات انتحارية (عبد الحميد، ٢٠٠٦).

تَستخدم التنظيماتُ الإرهابية الشبكاتِ الإلكترونيةَ لشن هجماتها بهدف تدمير المواقع والبيانات الإلكترونية، ولا توجد وسيلة تقنية يمكن تطبيقُها لمنْع

وقوع هذه الهجمات، فالتغير الدائم في النظم التكنولوجية وإلمام المخترق بها كونه يمثل عملاً رئيساً بالنسبة له؛ جعلت الاختراق والتدمير الإلكترونيَ أحد الأهداف السهلة للجماعات الإرهابية؛ بِغضِّ النظر عن البُعد الجغرافي، فقد تمتد أيدي هذه الجماعات إلى تدمير أحد المواقع الحيوية وإلحاق الضرر بأنظمة القيادة والسيطرة والاتصالات ومحطات توليد الطاقة والمياة.

يعتمد الإرهاب الإلكتروني على استخدام الفيروسات كسلاحٍ لإلحاق الضرر بنُظم المعلومات والبيانات، فقدرتُه على التضاعف والتكاثر والانتقال من جهازٍ إلى آخر وتغيُّر شكله وتحوُّره كي يتلائم مع كافة النظم التكنولوجية؛ يجعل منه أحدَ أخطر الأسلحة في هذا العصر، والهدف الأكبر لكل منظمة إرهابية: استهداف النظم العسكرية، عن طريق اختراق نُظم المعلومات الخاصة بالأسلحة الاستراتيجية، ونُظم الدفاع الجوي، فإذا حالف المخترقَ الحظُّ؛ تمكَّن من فك شِفرة إطلاق الصواريخ وإحداث دمار كارثي، أو يستخدم هذه المعلومات للتجسس والضغط على الحكومات لتنفيذ مطالبهم، كما قد يستهدف المخترقُ محطاتِ توليد الطاقة والتوزيع؛ لأهميتها في المجتمعات واعتماد الإنسَان المعاصر عليها بشكل أساس، ويتم ذلك من خلال شن عدة هجمات معلوماتية تؤدي إلى تعطل العديد من مرافق الحياة في البلاد وسيادة الفوضى.

تمثل البِنية التحتية أحد أهم الأهداف التي يضعها المخترق نُصب عينيه؛ فإحداث خلل في نُظم الشبكات التي تتحكم في حسابات البنوك وأسواق المال؛ يؤدي إلى إضعاف الثقة في النُّظم الاقتصادية، مما يؤدي إلى نشر الفوضى في الصفقات التجارية الدولية، وإحداث تَوقُّف جزئي أو كلي في منظومات التجارة والأعمال، واستهداف نُظم المواصلات عن طريق اختراق نُظم التحكم بخطوط الملاحة الجوية والبرية والبحرية.

وأخيراً قد يلجأ الإرهابيون إلى استخدام النظم التكنولوجية في عمليات التجسس؛ سواءٌ على الأشخاص لابتزازهم؛ أو على الدول والمنظمات الدولية، وما يُسهل هذه المهمة: وجود وسائل التقنية الحديثة وأقمار التجسس والبث الفضائي وإفشاؤها لدول أخرى معادية، بالإضافة إلى برامج حاسوبية من مصادر غير موثوق بها، فهي «كحِصان طروادة» إشارة إلى سرعة اختراقه وتكاثره في أي نظام معلوماتي؛ حيث يعتمد على وحدات الماكرو الموجودة في برامج معالجة النصوص، أو إخفاء معلومات داخل معلومات من خلال لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة؛ في معلومات أخرى عادية داخل الحاسب الآلي؛ ثم يجد وسيلةً لتهريب تلك المعلومة العادية في مظهرها، وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبُها حتى ولو تم ضبط الشخص متلبساً (عبد الرحمن، ٢٠٠٧).

المحدد الخامس

آليات الحد من ممارسات الإرهاب الإلكتروني

القضاء على الإرهاب الإلكتروني ضرْبٌ من الخيال، ولكن يمكن إدارة أخطاره وتخفيض الآثار الناجمة عنه إلى أقل حد ممكن، ونتناول هنا مجموعةً من الممارسات التي تحُدِّ من هذه الظاهرة، وكنتيجةٍ للتطورات التقنية المتسارعة والآثار الاقتصادية والاجتماعية الناتجة؛ فلا يمكن لأي مجتمع أن يعيش في معزل عنها، ولكن من الضروري وضع الآليات التي ترشح هذا الاستخدام عن طريق تدعيم الممارسات الإيجابية والحد من الممارسات السلبية من خلال تكاتف مؤسسات المجتمع وأفراده.

الإرهاب والتطرف والعنف؛ لم يأتِ اعتباطًا، ولم ينشأ جزافًا، بل له أسبابه ودواعيه، ومعرفة السبب غاية في الأهمية؛ إذ تحدد نوعَ العلاج وصِفة الدواء، فلا علاج إلا بتشخيص، ولا تشخيص إلا ببيان السبب.

وأسباب نشأة هذا الفكر متعددة متنوعة، فقد تكون فكرية أو نفسية أو سياسية أو اجتماعية أو اقتصادية أو تربوية، وهي أسباب متشابكة ومتداخلة، ولهذا لا ينبغي أن نقف عند سبب واحد، فالظاهرة التي أمامنا ظاهرة مُركَّبة معقدة، وأسبابها كثيرة متشابكة.

يكابد الإسلام اليومَ حربًا ضَروسًا تعددت مصادرُها وتنوعت أشكالهُا وتبدلت وسائلُها؛ لتتناسب مع تغيرات الأحوال وتبدلات الزمان واختلاف المكان؛ وإن اتفقت كلُّها على وحدة الهدف والمحاولات المستميتة للقضاء على الإسلام في حربه بيد أبنائه (علي، ٢٠٠٨).

طرق إدارة أخطار ظاهرة الإرهاب الإلكتروني:

أولى أدوات برنامج إدارة الأخطار: حماية البِنية التحتية؛ بصياغة سياساتٍ أمنيةٍ تعمل على تقليل الاختراق، وتعتمد على مجموعة من المختصين في هذا المجال، مع إجراء تقييمٍ مستمر وتحديد الثغرات الموجودة ومحاولة علاجها، وذلك من خلال إعادة تصميم نُظم الشبكات الإلكترونية واستخدام أسلوب المحاكاه لتحديد مواقع الثغرات على الشبكات ومعالجتها، مع الارتقاء بالأمن المعلوماتي للنظم المعلوماتية من خلال تبنِّي سياسة عزل الموارد المعلوماتية بالغة الأهمية عن نظم الشبكات المحلية وشبكة الإنترنت؛ لضمان حمايتها من عمليات الاختراق، وتوظيف تقنيات متقدمة لحماية النظم المعلوماتية؛ كالجدران النارية وبرمجيات مكافحة الفيروسات، واستخدام تقنيات متقدمة لتشفير المعلومات ومعالجتها بحيث لا يمكن الوصول إليها، وصياغة سياسات أمنية محكمة لضمان أمن نُظم المعلومات، كما يعتمد وضْع برنامج ناجح لإدارة مخاطر الإرهاب الإلكتروني؛ على مجموعة من الإجراءات التي يمكن تقسيمُها إلي إجراءات ترتبط بالنظم التكنولوجية، وأخرى مرتبطة بالعوامل المؤثرة على الأفراد المنتمين للجماعات المتطرفة.

أما فيما يتعلق ببرامج إدارة الأخطار المرتبطة بالنظم التكنولوجية؛ فهي تتضمن التأكدَ من فاعلية نظم الحماية الفيزيائية التي تتألف منها نظم المعلومات، ويشمل: إدارة حسابات مستخدمي شبكات المعلومات، وكلمات المرور، وتوفير برامج حماية النظام من الفيروسات، وإعداد وحفظ النسخ الاحتياطية، وتوفير برامج لإدارة الأزمات التي تستهدف نظم المعلومات (كريمة، ٢٠١٠)، ويتم ذلك من خلال نوعين من الإجراءات؛ أولهما: المقاومة الفنية المشتملة على وضع نظم أمنية قوية تعمل على ترشيح وتشفير البيانات

المهمة وتطوير برمجيات الحماية من الفيروسات، ثم الدور الفعال للمقاومة النظامية والتي تتضمن الإجراءات المتبعة دورياً للمحافظة على نظم المعلومات السرية وأهمها التغير الدائم لكلمات المرور وعمل النسخ الاحتياطية (عبد الرحمن، ٢٠٠٧).

إن مطوري تكنولوجيا المعلومات وخبراء الإنترنت؛ مطالبون بملاحقة أنشطتهم التوسعية بأنشطة حماية وسدِّ ثغرات لحماية هذا الفضاء الحيوي من أن يصبح ساحة إرهاب دامية، ويجب أن يهتم المجتمع الدولي بإبرام اتفاقيات تقنن تشريعات مكافحة تلك الجرائم، وتنظيم الجهود الدولية لمحاربتها، بما في ذلك بحث إنشاء «نظام للإنذار المبكر من الهجمات الإلكترونية»، وتطوير برامج آمِنة، وزيادة الوعي لدى المسؤولين التنفيذيين.

كما يجب تطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الإلكترونية، وتوفير التقنيات اللازمة لمواجهتها، عبر تطوير أمن شبكات الحاسب باستخدام أنظمة التشفير المتقدمة و«الجدران النارية» في الشبكات، وأنظمة اكتشاف المخترَقين عالية الدقة، والبرامج المضادة للفيروسات، كما أن إنشاء إدارات لمكافحة «الإرهاب الإلكتروني» في أنظمة الأمن، خصوصاً في الدول التي تشهد تقدماً مطَّرداً في اعتمادها على تكنولوجيا المعلومات؛ أمر حيوي، خاصة وأن التطور الحاصل فيها يتسارع، وتزداد فجوة الثغرات التكنولوجية؛ مما يستلزم مواجهة خاصة للحد من احتمالات نجاح التهديدات الإرهابية في هذا المجال.

ولابد من تقديم إجراءات لبرنامج إدارة المخاطر للعوامل المتعلقة بالبيئة الداخلية والخارجية للأفراد المنتمين للتنظيمات المتطرفة، يتضمن تقديمَ مجموعة من برامج الوقاية والعلاج؛ تشتمل على جميع جوانب حياة الفرد

ومعاملاته في المجتمع، فالتطرف لا يتخذ شكلاً ثابتـًا؛ وإنما هو متحور طِبقـًا لتداعيات الظروف، وهناك دور مهم لكلٍّ من أطراف المجتمع المختلفة، فيجب تحديد برامج هادفه تستوعب طاقات وتحديات الشباب وتعمل على تشجيع مشاريعهم، وذلك من خلال الدور الهام الذي تلعبة الأجهزة المحلية ومنظمات المجتمع المدني عن طريق إيجاد قنوات قادرة على استيعاب الطاقات لدى الشباب واستثمارها واستغلالها الاستغلالَ الأمثل.

ولا يجب أن نُغفل الدورَ المهم للتنشئة السوية للمؤسسات التعليمية؛ وذلك من خلال تطوير المناهج الدراسية بما يتلائم وحاجات الطلاب النفسية والاجتماعية والمهنية، والتركيز على تنمية المهارات عن طريق تدعيم الأنشطة الحرة حتى يتمكن من توظيفها مستقبلاً؛ تحقيقـًا للتراكم الفكري والعلمي، وبث الوعي الديني الصحيح والبعد عن الغلو والتطرف، ولن يتأتى ذلك إلا من خلال الاشتراك مع الدور العظيم الذي تلعبه الأسرة، والتي تعمل على تشكيل وصقل شخصية الفرد منذ طفولته؛ من خلال غرس القيم الدينية والأخلاقية المعتدلة، وتصحيح مسار الطفل أو الشاب كلما تطلب الأمر ذلك، مع عدم الإفراط في الشدة والقسوة، وغرس روح الشورى والمناقشة والحوار، يدعمها الدورُ التوعوي للمؤسسات الدينية الشرعية؛ والتي تهدف إلى توضيح الأمور الغامضة في الشريعة الإسلامية، وتنشئة جيل على علم ودراية بتعاليم الدين الصحيحة، ويعتمد ذلك على الدور الذي يلعبه العلماء المستنيرون، والحرص على فتح جميع قنوات الاتصال بالجماهير أمام دعاة التيار المعتدل، مما يعمل على نمو الفكر الإسلامي الصحيح المعتدل، ويضيق فرص نشأة التيار المتطرف الذي يدعو إلى العنف، ولن يتأتى ذلك إلا عندما ينزل الدعاةُ إلى الشباب ويكونوا قادةً ومرجعـًا لهم، ويتم تزويدُهم بمعلومات شرعية لما

يستجد من أحداث؛ حتى يتسنى لهم إزالةُ أية شائبة تَعلق بأذهان الشباب، مع تشديد الرقابة على أجهزة الإعلام لما لها من تأثير واسع وانتشار جماهيري بين الأطياف المختلفة للمجتمع، والحرص على أن تَبعد عن المتضمنة مشاهدَ العنف، والتركيز على النماذج المشَرِّفة التي تمثل قدوةً ودافعاً للأطفال والشباب، مع التأكد من أن هذه الأجهزة تؤمن بأن الحرية الحقيقية في الإسلام ولكن بضوابط (ممدوح، ٢٠٠٠).

كل ذلك في إطار منظومة متكاملة من الرقابة والحزم لأجهزة وزارة الداخلية؛ والتي يجب عليها الاهتمام بتطوير الوسائل التكنولوجية ونظم المعلومات والاتصالات، لكي تتواكب مع التقنيات المتقدمة التي تتعامل بها التنظيمات المتطرفة بما يمكِّنهم من ملاحقتهم، ولن يتأتى ذلك إلا من خلال رفع مستوى الكفاءات البشرية التي تنتمي لهذا الجهاز الفعال؛ عن طريق الدورات التدريبية الداخلية والخارجية، والتعاون الميداني المشترَك مع الدول المتقدمة في مجال تقنيات شبكات المعلومات، مع سَنِّ التشريعات التي تُجَرِّم الأعمالَ الإرهابيةَ والتحريضَ عليها بما في ذلك وسائل الإرهاب الإلكتروني، فكثير من الدراسات توصلت إلى أن انخفاض معدل الجرائم يرتبط طردياً مع فرض قوانين صارمة، لذا قامت مدينة الملك عبد العزيز للعلوم والتقنية بحجب بعض المواقع الضارة، كما قامت شركة الاتصالات التركية بحجبها أيضاً (مصطفى، ٢٠٠٧).

ويجب الاقتناع التام والكامل لهذه الأجهزة بأن هناك فارقاً كبيراً بين الإسلام بسماحته ورحمته، وبين التطرف المتشدد، ويتم ذلك من خلال الدورات التدريبية، كما يجب التأكد من تصحيح النظرة إلى المتطرفين بأنهم ليسوا متطرفين؛ وإنما هم مرضَى في حاجة إلى العلاج، حيث إن اختلاف النظرة إليهم يُبنَى عليها اختلافُ طريقة التعامل معهم.

ويجب التنويه على أن العالم دولاً وشعوبًا؛ أمام تحد كبير، يتطلب تنسيقًا إلكترونيًا عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلاً عن تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة هذه المشكلة وبخاصة الإنتربول؛ لمواجهة كافة أشكال جرائم الإرهاب على الإنترنت، وينبغي تجريمُ استخدام شبكة الإنترنت في عملياتٍ إرهابيةٍ؛ حيث إن قانون الجزاء جاء خاليًا منها، وكذلك قانون الإرهاب.

المحدد السادس: الجهود الدولية والمحلية المبذولة لمكافحة ظاهرة الإرهاب الإلكتروني

لقد بات الإرهاب بكافة أنواعه وأشكاله؛ خطراً يهدد أمن وسلامة المجتمع، فهو عمل إجرامي وعنف فكري ضد المدنيين بقصد إشاعة الفتنة وإحداث الخوف والذعر؛ وسيسعى الباحث جاهداً من خلال هذا المبحث؛ إلى تسليط الضوء على الجهود الدولية والمحلية المبذولة لمكافحة هذه الظاهرة.

أولاً: الجهود الدولية للتصدي لخطر الإرهاب الإلكتروني:

عجزت الجهود الدولية عن إيجاد مفهوم موحد للإرهاب الإلكتروني؛ وذلك في إطار وضع آليات للحد من هذه الممارسات الضارة، ولكنَّ مجلس الأمن قدَّم تعريفاً للإرهاب بصفة عامة، يمكن أن ينطبق على بعض أشكاله الخاصة كالإرهاب الإلكتروني؛ يقول التعريف: «العمل الإرهابي: عمل إجرامي ضد المدنيين بقصد الإضرار أو إحداث الرعب أو إكراه حكومةٍ أو منظمةٍ ما» (أيسر،٢٠١٤).

ومن هذا المنطلق فلابد من تفعيل آليات التعاون الدولي وإصدار التشريعات التي تتضمن اتفاقيات تجريم ممارسات الإرهاب الإلكتروني، كما يجب تفعيل دور المنظمات الدولية والإقليمية من أجل توفير الحماية القانونية لهذه الجرائم، وإيجاد تشريع دولي خاص لمواجهة هذا الخطر، ولابد من وجود منظومة معلوماتية موحدة تعتمد في إنشائها على مكتب عالمي أو إقليمي للتوثيق الإلكتروني، مع تسجيل كافة البرامج المعلوماتية وحفظها واعتماد الدلائل أو القرائن الرقمية؛ كدلائل إثبات الجريمة وإدانة مقترفيها، والحرص على إدراج مثل هذه الجرائم ضمن اختصاصات المحكمة الجنائية الدولية نظرا لطابعها العالمي (عبد الصبور، ٢٠٠٨).

ومن خلال استعراض أهم الجهود المبذوله دولياً؛ نجد أن الاتحاد الأوروبي قد وضع خُطة جديدة يقوم بموجبها بتفتيش أجهزة الكمبيوتر عن بُعد وذلك لمكافحة جرائم الإنترنت، وستشجع الخُطةَ تبادلَ المعلومات بين قوات الشرطة الإلكترونية لملاحقة ومقاضاة المجرمين، وستنسق هذه القواتُ المعروفة باسم «يوروبول»؛ عملَها الاستقصائيَّ، وستوجه تحذيرات حول موجات الجريمة الإلكترونية (موقع البوابة القانونية www.tashreaat.com).

وقدم الاتحاد الدولي للاتصالات دليلاً إلكترونياً لتتبع المعايير الأمنية الخاصة بتكنولوجيا المعلومات والاتصالات لمكافحة الجريمة على شبكة المعلومات.

ثانياً: جهود المملكة العربية السعودية في الحد من الإرهاب الإلكتروني:

مَنَّ الله على المملكة العربية السعودية باعتمادها على القرآن الكريم والسنة النبوية المطهرة في كافة تشريعات وشؤون المملكة، مما يؤكد على البعد عن التطرف والغلو في كافة المعاملات، ولما كانت النظم التكنولوجية جزءاً من كيان المملكة؛ باتت تعتمده بشكل فاعل في إدارة أغلب مرافق الدولة، فانطبق عليه ما ينطبق على باقي كيانات المملكة التي تخضع لأحكام الشريعة الإسلامية المستمدة من القرآن والسنة؛ والتي توجب سَنّ القوانين ووضْع اللوائح الملزِمة لاتباعها، وتُعد تجربة المملكة في التصدي للإرهاب؛ تجربة رائدة تحظى بتقدير محلي ودولي، نظراً لمعالجتها الناجحة عبر جهود كبيرة مبنية على أسس علمية عميقة.

١ - التشريعات القانونية:

أصدرت الأجهزة التشريعية في المملكة العديد من القوانين التي تُجرم معاملات الإرهاب الإلكتروني، حيث فرضت عقوباتٍ مشددةً لمخالفيها، فقد جاء قرار مجلس الوزراء برقم ١٦٣ لعام ١٤١٧ هـ والذي تضمن العديد من النصوص التي تناولت تجريمَ محاولات اختراق أنظمة الحاسبات الآلية المتصلة بشبكات المعلومات الدولية، وكذلك المواقع التي تتمتع بحقوق الملكية الفكرية دون الحصول على موافقةٍ مسبقة، ويتم متابعة كافة التطورات التي تتناول مجالَ الجرائم الإلكترونية؛ من خلال لجنةٍ تم تشكيلُها بعضوية كلٍّ من: وزارة الإعلام والدفاع، وزارة والتعليم العالي، أجهزة الاستخبارات، ومشاركة مدينة الملك عبد العزيز للعلوم التقنية، والتي لها حق الضبط الأمني للمعلومات التي تُتناقل عبر شبكة المعلومات، كما عملت وزارة الداخلية جاهدةً على تفعيل قانون مكافحة جرائم المعلومات؛ والذي تضمَّن ١٦ مادة بعقوبات صارمة ضد مرتكبي هذه الجرائم، تشتمل على تعريفات لمصطلحات الجرائم الإلكترونية وعقوبة مرتكبيها.

٢ - المبادرات:

سعت المملكة العربية السعودية لعقد دورات تدريبية تتناول ظاهرةَ الإرهاب الإلكتروني وكيفيةَ الوقاية منها، كما تحاول الحدَّ من انتشار هذه الظاهرة من خلال إنجاز مشروع قانون نظم التجارة الإلكترونية، وتسعى إلى تنمية مهارات المشاركين في مجال مكافحة الإرهاب الإلكتروني؛ وذلك عن طريق إكسابهم المعارف التي تعينهم على تحديد أنواع الجرائم وكيفية ارتكابها ومعرفة مرتكبيها.

وقد قدم معالي الدكتور عبد الرجمن السند؛ مجموعة من المبادرات التي تعمل على درء خطر الإرهاب الإلكتروني عن المجتمع، تضمنت حثَّ الجهات المعنية على إصدار اللوائح والقوانين التي تُلزم أطرافَ المجتمع بالبعد عن هذه الممارسات الضارة، كما حذر أيضاً من استخدام البريد الإلكتروني كأداةٍ للإرهابيين للتواصل وتبادل المعلومات، وأكَّد على أن اختراق البريد الإلكتروني بمثابة تجسس وخرْق لخصوصية الآخرين، والشريعة الإسلامية كفلت الحقوقَ الشخصيةَ للإنسان وحرَّمت الاعتداءَ عليها، وأكد على ضرورة حجب المواقع التي تدعو وترسخ للفكر المتطرف، ودعا لتطوير كفاءة أجهزة الأمن وقدرتها على التعامل مع الجرائم الإلكترونية؛ بحيث تتمكن من تقديم الأدلة المقبولة للجهات القضائية.

كما قامت المملكة بالعديد من المبادرات والجهود للقضاء على الفكر المنحرف والأعمال الإرهابية؛ أهمها: مبادرة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز في ٥ من جمادى الأولى ١٤٢٥هـ؛ الموافق ٢٣ من يونيو ٢٠٠٤م، وتضمنت عفواً عن كل من يسلِّم نفسَه ممن ينتمون إلى تلك الفئة الضالة.

كما شكلت وزارة الداخلية لجنةَ المناصحة، وهي لجنة شرعية من العلماء والدعاة والمفكرين؛ تهدف لتصحيح المفاهيم الخاطئة والمغلوطة لدى الموقوفين، ونصحهم وتوجيههم إلى تعاليم الدين الإسلامي الصحيحة؛ وفق ما شرعه الله سبحانه وتعال، وبيَّنه رسولُ الهُدى ﷺ في سنته الصحيحة.

وبذلت وزارة الثقافة والإعلام العديدَ من الجهود كمحاولةٍ لتصحيح الفكر التكفيري المتطرف؛ عن طريق الاستدلال بالقرآن الكريم والسنة النبوية المطهرة، والاجتهادات التي تَوصل إليها السلفُ الصالحُ وأئمةُ المسلمين.

أما وزارة الشوون الإسلامية فقد أبرزت خطأ الفكر التكفيري المنحرف وخطره على الشباب؛ من خلال المحاضرات والندوات العلمية والتعليمية من أجل زيادة الوعي وتحريم هذا الفكر المتطرف، وبذلت وزارة التربية والتعليم جهوداً لتوعية الطلاب والطالبات بخطورة الأعمال الإرهابية وحُرمتها في الإسلام، والآثار الواقعة على مرتكبيها، وحث المعلمين على توعيتهم بذلك وتوجيههم إلى المسار الصحيح.

٣- دور مؤسسات البحث العلمي:

لقد كان وما زال لمؤسسات البحث العلمي في المملكة دور كبير في التصدي لهذه الظاهرة، فلا ننسى الدور الرائد الذي قامت به أكاديمية الأمير نايف للعلوم الأمنية؛ والتي أولت الإرهابَ الاهتمامَ البالغ من حيث تضمين المناهج الدراسية الموضوعاتِ العلميةَ في مجال مكافحة الإرهاب بوجه عام، والإرهاب الإلكتروني بوجه خاص، بالإضافة إلى الرسائل العلمية والمحاضرات عن الإرهاب وطرق مكافحته ومواجهته.

٤- الاتفاقيات الدولية:

استمراراً لجهود المملكة للحد من انتشار الإرهاب؛ فقد صادقت على العديد من الاتفاقيات والمعاهدات الخاصة لمكافحة هذه الظاهرة، ومنها: معاهدة المؤتمر الإسلامي لمكافحة الإرهاب الدولى عام ١٩٩٩، والاتفاقيات العربية لمكافحة الإرهاب تحت رعاية مجلس وزراء الداخلية والعدل العرب، والتي تم انعقادها في عام ١٩٩٨، وهي الاتفاقية الأبرز والأهم التي تم إنجازها على الصعيدين الأمني والعربي، حيث سجل العرب من خلالها سبقًا بين دول العالم في مجال مكافحة الإرهاب، كما قامت المملكة بتوقيع اتفاقيات أمنية ثنائية مع بعض الدول العربية والإسلامية لمكافحة الإرهاب والتصدي له ومحاربتة بكافة الطرق.

الخاتمة

مما سبق يمكننا القول إن الإرهاب الإلكتروني هو إرهاب المستقبل؛ لما له من أشكال عديدة وأساليب متنوعة، فمن خلال المدخل العملي والعلمي؛ نجد أن أسباب هذه الظاهرة لا تختلف كثيراً عن أسباب ظاهرة الإرهاب بصفة عامة، فهناك العديد من العوامل التي تجعل منها سلاحًا حاداً للجماعات والمنظمات الإرهابية المتطرفة، حيث إن اعتماد الدول على وسائل الاتصالات وشبكات المعلومات المعرفية؛ سيكون العامل الأكبر في فتح المجال أمام مرتكبي هذه الجرائم لتحقيق أهدافهم وتدمير البنية التحتية المعلوماتية.

كما أن من أبرز وأهم أشكال الإرهاب: تبادل المعلومات الإرهابية الزائفة ونشرها في الشبكة الإنترنت؛ وإنشاء المواقع الإرهابية الإلكترونية، والتجسس، والتهديد، والترويع الإلكتروني، وتدمير المواقع والبيانات الإلكترونية ونظم المعلومات المعرفية، لذا فلابد من السعي لعقد مؤتمر دولي بإشراف هيئة الأمم المتحدة لإبراز وإيجاد تعريف موحد ومحدد للإرهاب، والاصطفاف صفًا واحداً من خلال خطة عملية دولية لمواجهته ومكافحته بجميع صوره وأشكاله، ويتم ذلك تحت الشعار التالي «الإرهاب لا دين له»، وعدم الربط بين الإرهاب وبين أي دين أو جنسية.

كما يجب التأكيد على الدور البارز والمهم لوسائل الإعلام المختلفة، لوضع القواعد الإرشادية التوعوية للمواطنين، ومما لا شك فيه أنه يجب التطوير الفعلي للقوانين والإجراءات الجنائية لمنع الإرهابيين من استغلال قوانين اللجوء والهجرة في شن هجمات إرهابية إلكترونية ضد الدول المستضيفة.

ولا يجب أن نُغفل الدورَ المهم للمجتمعات والمنظمات الدولية لمحاولة وضع تعريف واضح ومنهج محدد للتعامل مع هذه الظاهرة في إطار القانون الدولي، فقد اختلفت نظرة الدول إلى هذه الجريمة؛ فهناك من يعتبر الإرهاب الإلكتروني سلوكًا جنائيًا، والبعض يعتبرة مقاومة مشروعة، وهناك اتجاه لاعتباره جريمة سياسية أو إلكترونية كحرب وقرصنة المعلومات.

النتائج والتوصيات

يمكن بلورة أهم النتائج التي توصلت إليها الدراسة والتوصيات كما يلي:

أولا: أهم نتائج الدراسة

١- يمكن تعريف الإرهاب الإلكتروني على أنه: «التهديد المادي والمعنوي للدول أو الجمعيات أو الأفراد، والعدوان عليهم باستخدام التقنيات التكنولوجية الحديثة».

٢- من أهم الوسائط المستخدمة في الإرهاب الإلكتروني: استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، وكذلك تصميم مواقع على شبكة الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، وتعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية.

٣- أن الجهود المبذولة لدراسة وتنظيم ومتابعة الجرائم الإلكترونية لا تزال في مراحلها الأولى.

٤- تسعى المملكة العربية السعودية بجهود مضنية في مكافحة الإرهاب الإلكتروني، وأصدرت مجموعة من الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، إضافة إلى عقد دورات تدريبية حول موضوع مكافحة جرائم الحاسب الآلي بمشاركة مختصين دوليين.

٥- تكنولوجيا الإرهاب بأبسط صورها: هي الأنشطة العقلية الموجهة والمهارات التي يستخدمها الإرهابي للتعامل مع بيئته المحيطة؛ لتحقيق هدفه في التأثير والسيطرة على متخذي القرار؛ باستخدام المواد

والأدوات والتجهيزات والآلات، وتطوير المهارات والأساليب وطرق التنظيم المختلفة.

٦- أبرز وأهم مظاهر الإرهاب الإلكتروني وأشكاله: تتمثل في تبادل المعلومات الإرهابية ونشرها على شبكة الإنترنت، وإنشاء المواقع الإرهابية الإلكترونية، وتدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، والتهديد والترويع والتجسس الإلكتروني.

٧- التعاملات الخاصة بتقنية المعلومات يجب أن تخضع للأحكام المستمَدة من القرآن والسنة الصحيحة.

٨- أسباب الإرهاب الإلكتروني ودوافعه؛ متعددة ومتنوعة، وهي عينها أسباب الإرهاب عموماً.

٩- هناك عوامل تجعل الإرهابَ الإلكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الإرهابية.

ثانياً: التوصيات

يوصِي الباحث بناءً علي نتائج الدراسة التحليلية؛ بما يلي:

١- إيجاد منظومة معلوماتية موحدة تعتمد في إنشائها على مكتب عالمي أو إقليمي للتوثيق الإلكتروني.

٢- السعي لتطبيق البرنامج المقترح لإدارة أخطار الإرهاب الإلكتروني؛ وإنشاء هيئة وطنية تكون مسؤولة عن متابعة إجراءات التطبيق وتصحيح الانحرافات، وتعاون كافة هيئات والجهات الحكومية معها.

٣- تكثيف البحث في تكنولوجيا الإرهاب -وخصوصاً في الشق المعنوي منها- للوصول إلى منهجية عملية للتعامل مع آلية النشاط الإرهابي؛ مما يسهل التفكير بأسلوب الإرهابي والتعامل معه.

٤- الغلو والتشدد في الدين أمر خطير على مجتمعنا؛ لذا وجب على العلماء والمفكرين أن يسهموا في المزيد من الآليات والوسائل وسبل الوقاية من هذه الآفة.

٥- على الأسرة أن توضح لأبنائها أهمية حب الوطن؛ وأنها من طاعة الله ﷻ.

٦- السعي إلى الإسراع بإنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب الإلكتروني، والانضمام للاتفاقيات الدولية في هذا، وزيادة التعاون على المستوى الوطني والإقليمي لتبادل الخبرات والتجارب.

٧- الاهتمام بالدور التوعوي الذي تلعبة المؤسسات الدينية الشرعية؛ والتي تهدف إلى توضيح كافة الأمور الغامضة في الشريعة الإسلامية، مما يؤدي إلى تنشئة جيل على علم ودراية بتعاليم الدين الصحيحة.

٨- تشديد الرقابة على أجهزة الإعلام لما لها من تأثير واسع وانتشار جماهيري بين الأطياف المختلفة للمجتمع.

٩- يجب علي أجهزة وزارة الداخلية؛ الاهتمام بتطوير الوسائل التكنولوجية ونظم المعلومات والاتصالات لكي تتواكب مع التقنيات المتقدمة التي تتعامل بها التنظيمات المتطرفة بما يمكِّنهم من ملاحقتهم.

١٠- العالم دولاً وشعوباً؛ أصبح أمام تحد كبير يتطلب تنسيقاً إلكترونياً عالي المستوى بين الأجهزة الأمنية في كافة الدول، فضلاً عن تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية.

مراجع الدراسة

أولاً: المراجع العربية:

١- أيسر محمد عطية: «دور الآليات الحديثة للحد من الجرائم المستحدثة»، الملتقى العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية)، كلية العلوم الاستراتيجية (٢٠١٤).

٢- حسن مظفَّر الرزو: «الفضاء المعلوماتي» بيروت، مركز دراسات الوحدة العربية (٢٠٠٧).

٣- خالد بن محمد الطويل: «التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية»، مركز المعلومات الوطني، وزارة الداخلية، ورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات، ١٩/ ١٠/ ١٤٢٣هـ، الرياض.

٤- رانيا نظمي: «الفراغ الفكري وتأثيراته على الاستخدام السيئ لتقنية الاتصالات الحديثة»؛ مؤتمر الإرهاب (بين تطرف الفكر وفكر التطرف)، الجامعة الإسلامية بالمدينة المنورة (٢٠٠٩).

٥- صغير يوسف: «الجريمة المرتكَبة عبر الإنترنت»؛ رسالة ماجستير منشورة، كلية الحقوق والعلوم السياسية، جامعة مولود معمري (٢٠١٣).

٦- عبد الله بن عبد العزيز بن فهد العجلان: «الإرهاب الإلكتروني في عصر المعلومات»؛ بحث مقدم إلى المؤتمر الدولي الأول: «حماية أمن المعلومات والخصوصية في قانون الإنترنت»، عُقد بالقاهرة (٢٠٠٨).

٧- عبد الحميد إبراهيم محمد العريان: «العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة: ما هو رد فعل القطاع الخاص؟» كلية التدريب، قسم البرامج التدريبية،: مكافحة الجرائم المعلوماتية (٢٠٠٦).

٨- عبد الرحمن بن عبد الله السند: «وسائل الإرهاب الإلكتروني؛ حكمها في الإسلام وطرق مكافحتها»، موقع وزارة الأوقاف السعودية، (٢٠١٠).

٩- عبد الصبور عبد القوي علي: «الجريمة الإلكترونية والجهود الدولية للحد منها»، كلية الحقوق،جامعة بني سويف،جمهورية مصر العربية (٢٠٠٨).

١٠-علي بن فايز الجحني«، مقدمة حول ظاهرة الإرهاب»، جامعة نايف العربية للعلوم الأمنية، كلية التدريب، قسم البرامج التدريبية (٢٠٠٨).

١١-كريمة شافي جبر محمود: «الإرهاب المعلوماتي»، مركز المستنصرية للدراسات العربية والدولية، مجلة كلية الآداب، العدد ٩٦،(٢٠١٠).

١٢-فيليب سيب ودانا جانبك: «جيل ما بعد القاعدة: دور الإعلام الجديد في انتشار ظاهرة الإرهاب»، عرض رضوى عمار، مركز الكاشف للمتابعة والدراسات الاستراتيجية (٢٠١١).

١٣-ممدوح عبد الحميد عبد المطلب: «جرائم استخدام شبكة المعلومات العالمية:الجريمة عبر الإنترنت»، مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة (٢٠٠٠).

١٤-مصطفى محمد موسى: «التنظيمات الإرهابية وشبكة الإنترنت»؛ الندوة العلمية: «استشراف التهديدات الإرهابية»، مركز الدراسات والبحوث، قسم الندوات،جامعة نايف العربية للعلوم الأمنية (٢٠٠٧).

١٥-هايل ودعان الدعجة: «الإرهاب في العصر الرقمي»، مؤتمر جامعة الحسين بن طلال الدولي للإعلام والإرهاب، الأردن (٢٠٠٨).

١٦-يوسف بن أحمد الرميح: «الإرهاب والجريمة الإلكترونية بالمجتمع السعودي»، جامعة القصيم (٢٠١٤).

ثانياً: المراجع الأجنبية:

1- Clay Wilson, Computer attack cyber terrorist, vuluer abilities and policy issues congress (report congress. 17 Oct. 2003).

2- D.M. Trent, "Hackers, Crackers, and Trackers ", American Legion Magazine. (February, 1997).

3- Rapalus, P. Ninety percent of survey respondents detect cyber attacks. Computer Security Institute. [Online]. Available: http://www.gocsi.com/prelen_000321.htm.(2005)