

مخاطر ومظاهر الإرهاب الإلكتروني

بقلم الدكتور : محمودي قادة

أستاذ محاضر "أ"

كلية الحقوق والعلوم السياسية جامعة ابن خلدون - تيارت

مقدمة:

أخذت المعلوماتية والكمبيوتر منذ أكثر من عشرين عاما مكانة معتبرة سواء على المستوى الوطني أو الدولي، وسواء على المستوى الخاص والعام حيث أطلق على قرن العشرين بقرن المعلوماتية، فإذا كانت الأسلحة المتطورة والمعدات الحديثة من الأمور الشائعة لممارسة ارتكاب الجريمة فالمستحدث فهذا المجال هو التكثيف استخدام نظم المعلوماتية والوسائل الإلكترونية الحديثة في الأنشطة الإجرامية وإذا كان من إيجابيات هذه الوسائل هي ما تقدمه للدول وأجهزتها الأمنية وللأفراد الكثير من التسهيلات والإمكانات التي تسهم في رفع كفاءتها وتطوير قدراتها على التصدي للجريمة إلا أنها قد حملت في طياتها جانبا تعسفيا أفرزه مستخدميها في استعمالها لأغراض غير مشروعة، حيث أدى هذا التطور التكنولوجي إلى تطوير أساليب ارتكاب الجريمة ومضمونها، حيث تقول "روي جودسون" وهي جبهة بمرکز المعلومات الوطني الأمريكي في هذا الصدد لقد أصبحت الجريمة أكثر قوة بفضل التقنية الحديثة. لذا نجد المنظمات الإجرامية تلجأ إلى هذه التكنولوجيا الحديثة لممارسات أنشطتها الإجرامية المختلفة من بينها ظهر ما نسميه بالإرهاب

الالكتروني الذي يمكن تعريفه بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو جماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق باستخدام الموارد المعلوماتية والوسائل الالكترونية بشتى الصنوف العدوان وصور الإفساد.

أي بمعنى أنه هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة الكترونيا توجه من أجل الانتقام أو الابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة. وعليه فإن الإرهاب الالكتروني يشير إلى عنصرين أساسيين هما فضاء الانترنت والإرهاب وهو يتزايد في الدول المتقدمة والتي تدار بنيتها التحتية بالحاسبات الالكترونية والشبكات المعلوماتية مما يجعلها هدفا سهلا فبدلا من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح لتدمير البنية المعلوماتية بحيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات أو تعطيل أنظمة الدفاع الجوي أو التحكم في خطوط الملاحة الجوي والبرية والبحرية أو شل محطات إمداد الطاقة والماء أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية. لذا يمكن أن نطرح الإشكالية التالية:

في أي مدى تُكْمُنُ مخاطر الإرهاب الالكتروني على الاستقرار الأمن العالمي؟.

المبحث الأول: أسباب الإرهاب الإلكتروني وخصائصه وأهدافه

سنتناول في هذا المبحث دراسة أسباب ارتكاب جريمة الإرهاب الإلكتروني مع بيان لأهم خصائصه وأهدافه، ومن ثم فقد تم تقسيم دراسة هذا المبحث إلى مطلبين، سنتناول في المطلب الأول أسباب الإرهاب الإلكتروني ودوافعه، وفي المطلب الثاني خصائص الإرهاب الإلكتروني وأهدافه

المطلب الأول: دوافع الإرهاب الإلكتروني

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 لجماعات والمنظمات الإرهابية، وبالنظر الشاملة المتوازنة يمكننا القول بأن الأسباب متشابهة والدوافع متداخلة، لذا سنحاول دراسة الأسباب العامة للإرهاب الإلكتروني (الفرع الأول)، ثم الأسباب الخاصة للإرهاب الإلكتروني (الفرع الثاني)

الفرع الأول: الأسباب العامة للإرهاب الإلكتروني

مما لا شك فيه أن أسباب الإرهاب ودوافعه تختلف في درجة أهميتها، وفي مدى تأثيرها باختلاف المجتمعات الدولية، تبعاً

لاختلاف الاتجاهات السياسية، والظروف الاقتصادية والأحوال الاجتماعية، والاختلاف الديني والعقدي، لذا فإن ما يصدق على مجتمع قد لا يصدق بالضرورة على غيره من المجتمعات.

ويمكننا إيجاز أهم أسباب ظاهرة الإرهاب فيما يأتي:

أولاً: الدوافع الشخصية

تتعدد الدوافع الشخصية المؤدية للإرهاب، ويمكن بيان أبرزها فيما يلي:

- 1- الرغبة في الظهور، وحب الشهرة، حيث لا يكون الشخص مؤهلاً فيبحث عما يؤهله باطلا فيشعر ولو بالعدوان والتخريب والتدمير.
- 2- الإحباط في تحقيق بعض الأهداف أو الرغبات أو الوصول إلى المكانة المنشودة، وإحساس الشخص بأنه أقل من غيره وينظر إليه نظرة متدنية، فيلجأ إلى الإرهاب والخروج على النظام.
- 3- افتقاد الشخص لأهمية دوره في الأسرة والمجتمع، وفشله في الحياة الأسرية، مما يؤدي إلى الجنوح واكتساب بعض الصفات السيئة، وعدم الشعور بالانتماء والولاء للوطن.
- 4- الإخفاق الحياتي، والفشل المعيشي، وقد يكون إخفاقاً في الحياة العلمية أو العملية، أو المسيرة الاجتماعية، أو

النواحي الوظيفية، أو التجارب العاطفية، مما يجعله يشعر بالفشل في الحياة.

5- نقمة الشخص على المجتمع الذي يعيش فيه نتيجة ما يراه من ظلم وإهدار لحقوق المجتمع، فيتولد لديه الحقد والاستعداد للقيام بأي عمل يضر المجتمع¹.

ثانياً: الدوافع الفكرية

تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها فيما يلي:

1- الفراغ الفكري، والجهل بقواعد الدين الحنيف، وآدابه وسلوكه.

2- الفهم الخاطئ للدين ومبادئه وأحكامه، وسوء تفسيره، واعتماد الشباب بعضهم على بعض دون الرجوع إلى العلماء، ويقول ابن مسعود "لا يزال الناس بخير ما أخذوا العلم عن أكابرهم وعن أمثائهم وعلمائهم فإذا أخذوه عن صغارهم وشرارهم هلكوا".

3- الجهل بمقاصد الشريعة الإسلامية، وتأويل معانيها بالظن من غير يقين وثبت.

4- التشدد والغلو في الفكر أو ما يصطلح عليه بـ (التطرف)، وهو أمر بالغ الخطورة في أي مجال من المجالات وخصوصاً في الأمور الفكرية، وقد حذر

الإسلام منه حتى ولو كان بلباس الدين يقول النبي محمد: (إياكم والغلو)، كما يقول: (هلك المتنطعون).
5- الانقسامات الفكرية المتباينة بين التيارات المتنوعة والأحزاب المختلفة².

ثالثاً: الدوافع السياسية

إن من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب ما يأتي:

1- السياسات غير العادلة التي تنتهجها بعض الدول ضد مواطنيها، والكبت السياسي الذي تمارسه عليهم، وتهميش دور المواطن وتغييبه عن المشاركة السياسية، وانتهاك حقوقه، وعدم تلبية متطلبات التوازن الاجتماعي، وانعدام تفعيل دور مؤسسات المجتمع المدني.

2- الإحباط السياسي، فإن كثيراً من البلدان العربية والإسلامية لم تكتف بتهميش الجماعات الإسلامية، بل وقفت في وجهها، وتصدت لأربابها، وحصرت نشاطها، وجمدت عطاءها، حتى في بعض البلدان التي تدعي الديمقراطية وحرية الرأي، وهذا من شأنه أن يولد المنظمات السرية، وردود الأفعال الغاضبة التي لا تجد ما تصب فيه غضبها سوى الإرهاب.

3- غياب العدالة الاجتماعية، وعدم المساواة في توزيع الثروة الوطنية، والتفاوت في توزيع الخدمات والمرافق الأساسية، والاستيلاء على الأموال العامة، وانعدام التنمية المستدامة، وإهمال الرعاية و التقصير في أمورهم وما يصلحهم، وانعدام أداء الأمانة، وحفظ الديانة، والنصح للأمة، والصدق مع الرغبة، وتسهيل أمورهم المعيشية، والإنسانية.

4- ما تعانيه بعض المجتمعات والشعوب الدولية من ظلم واضطهاد واختلال، وسيطرة استعمارية، وانتهاك صارخ للحقوق والحرمات، وسلب الأموال والمقدرات، وخرق للقوانين والمواثيق الدولية، مما دفع تلك الشعوب إلى التشدد والتطرف.

5- افتقار النظام الدولي إلى الحزم في الرد على المخالفات والانتهاكات التي تتعرض لها مواثيقه بعقوبات دولية شاملة ورادعة³.

رابعاً: الدوافع الاقتصادية:

إن من أهم الدوافع الاقتصادية المؤدية إلى تفشي ظاهرة الإرهاب ما يلي:

1- تفاقم المشكلات والأزمات الاقتصادية في المجتمعات الدولية، بالإضافة إلى المتغيرات الاقتصادية العالمية،

والاستغلال غير المشروع للموارد الاقتصادية لبلد معين.

2- عدم القدرة على إقامة تعاون ولي جدي من قبل الأمم المتحدة، وحسم المشكلات الاقتصادية الدولية، وعدم القدرة المنظمة على إيجاد تنظيم عادل ودائم لعدد من المشكلات العالمية، مثل: اغتصاب الأراضي، والنهب والاضطهاد، وهي حالة كثير من الشعوب.

3- معاناة الأفراد من المشكلات الاقتصادية المتعلقة بالإسكان والديون والفقر وغلاء المعيشة والتضخم في أسعار المواد الغذائية والخدمات الأساسية، وعدم تحسن دخل الفرد، كل ذلك من العوامل المؤثرة في إنشاء روح التدمير في الأمة، وربما دفعت بعض الشباب إلى التطرف والإرهاب.

4- انتشار البطالة في المجتمع وزيادة العاطلين عن العمل وعدم توفر فرص العمل، من أقوى العوامل المساهمة في امتهان الجريمة والاعتداء والسرقة وتفشي ظاهرة الإرهاب، فالناس يحركهم الجوع والفقر وعدم العمل، ويسكنهم المال والعمل.

5- التقدم العلمي والتقني للأنظمة المصرفية العالمية أدى سهولة انتقال الأموال وتحويلها وتبادلها بين جميع أرجاء العالم عن طريق الشبكة العالمية للمعلومات (internet)، مما

ساعد المنظمات الإرهابية على استغلال الفرصة من أجل تحقيق أغراضهم غير المشروعة⁴.

خامسا: الدوافع الاجتماعية

تتعدد الأسباب الاجتماعية الداعية إلى ظهور الإرهاب ويمكن تصنيف أهمها فيما يأتي:

1- التفكك الأسري والاجتماعي، مما يؤدي إلى انتشار الأمراض النفسية والانحراف والإجرام والإرهاب، لذلك فإن المجتمع المترابط والأسرة المتماسكة تحيط الأشخاص بشعور التماسك والتعاون، ومن شذ عنهم استطاعوا احتواءه وردّه عن الظلم، فالمجتمعات ذات الترابط الأسري لا تظهر بينهم الأعمال الإرهابية بالقدر نفسه الذي تظهر فيه عند المجتمعات المفككة اجتماعيا.

2- غياب التربية الحسنة الموجهة التي توجه الأشخاص لمكارم الأخلاق ومحاسنها، وانعدام التربية الإيمانية القائمة على مرتكزات ودعائم قوية من نصوص الوحي، واستبصار المصلحة العامة ودرء المفسدات الطارئة، بالإضافة إلى قلة القدوة الناصحة المخلصة التي تعود على المجتمع بالنفع والخير وإرضاء الله سبحانه وتعالى وحب الدين والوطن.

- 3- الفراغ الذي هو مفسدة للمرء، وداء مهلك ومتلف للدين والنفس، فإذا لم تشغل النفس بما ينفع شغلتك هي بما لا ينفع، والفراغ النفسي والروحي والعقلي والزماني أرض خصبة لقبول كل فكر هدام غلو وتطرف، فتتغلغل الأفكار وتغزو القلوب فتولد جذورا يصعب قلعها إلا بالانشغال بالعمل الصالح والعلم النافع،
- 4- فقد الهوية المجتمعية والعقيدة الصحيحة للمجتمع، وفقدان العدل وانتشار الظلم بين المجتمع، وعدم الحكم بما أنزل الله، واختلال العلاقة بين الحاكم والمحكوم، وغياب لغة الحوار بين أفراد المجتمع وأطيافه، كل ذلك من الأسباب الاجتماعية المؤدية إلى تفشي ظاهرة الإرهاب.
- 5- غياب دور العلماء وانشغالهم وتقصير بعض أهل العلم والفقه والمعرفة في القيام بواجب النصح والإرشاد والتوجيه للمجتمع⁵.

الفرع الثاني: الأسباب الخاصة للإرهاب الإلكتروني

إن أسباب الإرهاب الإلكتروني ودوافعه كثيرة ومتنوعة، وهي عينا أسباب ظاهرة الإرهاب عموما، لكن يجدر التنبيه إلى أن هناك العديد من العوامل والبواعث الخاصة التي تجعل من ظاهرة الإرهاب الإلكتروني موضوعا مناسبا وسلاحا سهلا للجماعات والمنظمات الإرهابية، ويمكننا بيان أبرز دوافع انتشار الإرهاب الإلكتروني بوجه خاص فيما يلي:

أولاً: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق

إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها، رغبة في التوسيع وتسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية⁶.

ثانياً: غياب الحدود الجغرافية وتدني مستوى المخاطرة

إن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد فرصة مناسبة للإرهابيين، حيث يستطيع محترف الحاسبة الإلكترونية أن يقدم نفسه بالهوية والصفة التي يرغب بها أو يتخفى تحت شخصية وهمية، ومن ثم يشن هجمته الإلكترونية وهو مسترخ في منزله من دون مخاطرة مباشرة، وبعيدا عن أعين الناظرين.

ثالثاً: سهولة الاستخدام وقلة التكلفة

إن السمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام، طيبة الانقياد، قليلة التكلفة، لا تستغرق وقتاً ولا جهداً كبيراً، مما أعطى للإرهابيين فرصة ثمينة للوصول إلى أهدافهم

غير المشروعة، ومن دون الحاجة إلى مصادر تمويل ضخمة، فالقيام بشن هجوم إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة⁷.

رابعاً: صعوبة اكتشاف وإثبات الجريمة الإرهابية

في كثير من أنواع الجرائم المعلوماتية لا يعلم بوقوع الجريمة أصلاً وخاصة في مجال جرائم الاختراق، وهذا ما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، كما أن صعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني، لأنها تعطي المجرم أملاً في الإفلات من العقوبة⁸.

خامساً: الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية.

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعتبر من الأسباب الرئيسية في انتشار الإرهاب الإلكتروني، وكذلك لو وجدت قوانين تجرمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق.

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخرجاتها يعد سبباً مهماً في

تفشي ظاهرة الإرهاب الإلكتروني، حيث يمكن لأي شخص الدخول ووضع ما يريد على الشبكة، وكل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول إلى بعض المواقع المحجوبة، أو إغلاقها وتدميرها يعد نشر الجرم لما يريد فيها⁹.

لكل هذه الأسباب والدوافع أصبح الإرهاب الإلكتروني هو الأسلوب الأمثل والخيار الأسهل للمنظمات والجماعات الإرهابية.

المطلب الثاني: مميزات الإرهاب الإلكتروني

مما لا شك فيه أن الإرهاب الإلكتروني يتفرد بعدد من الخصائص التي يختص بها دون سواء، ويتميز بها عن الكثير من الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق جملة من الأهداف والأغراض غير المشروعة، وفي هذا المطلب سنحاول حصر أهم خصائص الإرهاب الإلكتروني، ثم نبين أبرز أهدافه وأغراضه.

الفرع الأول: خصائص الإرهاب الإلكتروني

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

- 1- إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة.

- 2- يتسم الإرهاب بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود.
- 3- صعوبة اكتشاف جرائم الإرهاب الإلكتروني، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع المثل هذا النوع من الجرائم.
- 4- صعوبة الإثبات في الإرهاب الإلكتروني، نظرا لسرعة غياب الدليل الرقمي، وسهولة إتلافه وتدميره.
- 5- يتميز الإرهاب الإلكتروني بأنه يتم عادة بتعاون أكثر من شخص على ارتكابه.
- 6- أن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية¹⁰.

الفرع الثاني: أهداف الإرهاب الإلكتروني

يهدف الإرهاب الإلكتروني إلى تحقيق جملة من الأهداف غير المشروعة ويمكننا بيان أبرز تلك الأهداف في ضوء النقاط الآتية:

- 1- نشر الخوف والرعب بين الأشخاص والدول والشعوب المختلفة
- 2- الإخلال بالنظام العام، والأمن المعلوماتي، وزعزعة الطمأنينة

- 3- تعويض سلامة المجتمع وأمنه للخطر
- 4- إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بالوسائل الاتصالات وتقنية المعلومات، أو الأموال والمنشآت العامة والخاصة.
- 5- تهديد السلطات العامة والمنظمات الدولية وابتزازها
- 6- الانتقام من الخصوم
- 7- الدعاية والإعلان، وجذب الانتباه، وإثارة الرأي العام
- 8- جمع الأموال والاستيلاء عليها¹¹.

المبحث الثاني: مظاهر الإرهاب الإلكتروني

لبيان أبرز وأهم مظاهر الإرهاب الإلكتروني وأشكاله فإنه من المناسب أن نقسم هذا المبحث إلى مطلبين، حيث نتناول تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية (المطلب الأول)، ثم دراسة إنشاء المواقع الإرهابية الإلكترونية (المطلب الثاني).

المطلب الأول: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب وتبادل الآراء والأفكار والمعلومات صعبا في الواقع، فإنه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيرا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن

معين، ويتبادلوا الحديث والاستماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم أتباعا وأنصارا عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكترونية، لذا سنحاول دراسة الاتصال والتخفي وجمع المعلومات الإرهابية (الفرع الأول) ثم التخطيط والحصول على التمويل للعمليات الإرهابية (الفرع الثاني) مع تبيان أهمية التدريب الإرهابي الإلكتروني (الفرع الثالث).

الفرع الأول: الاتصال والتخفي وجمع المعلومات الإرهابية

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم، نظرا لقلّة تكاليف الاتصال والرسائل باستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال والتخفي، وذلك عن طريق البريد الإلكتروني أو المواقع والمنتديات وغرف الحوار الإلكتروني، حيث يمكن وضع رسائل مشفرة تأخذ طابعا لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هوية، كما أنها لا تترك أثرا واضحا يمكن أن يدل عليه. وتمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما أنها تعتبر موسوعة إلكترونية شاملة متعددة الثقافات، ومتنوعة المصادر، وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر تولي الطاقة، وأماكن القيادة والسيطرة والاتصالات، ومواعيد الرحلات الجوية الدولية،

والمعلومات المختصة بسبل مكافحة الإرهاب، ونحو ذلك من المعلومات التي تعتبر بمثابة الكنز بالنسبة للإرهابيين، نظرا لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية¹².

الفرع الثاني: التخطيط والحصول على التمويل للعمليات الإرهابية

العمليات الإرهابية عمل على جانب من التعقيد والصعوبة، فهي تحتاج إلى تخطيط محكم، وتنسيق شامل، وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية، حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيدا عن أعين الناظرين، مما يسهل على الإرهابيين ترتيب تحركاتهم، وتوقيت هجماتهم.

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية سكانية متقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية، من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة، والقلوب الرحيمة، ومن ثم يتم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، يتم ذلك بواسطة رسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية، بطريقة ذكية وأسلوب مخادع، بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية¹³.

الفرع الثالث: التدريب الإرهابي الإلكتروني

تحتاج العمليات الإرهابية إلى تدريب خاص، ويعد التدريب من أهم هواجس التنظيمات الإرهابية، وقد أنشئت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام- لكن مشكلة اكتشافها ومداهمتها في أي وقت، لذا فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الإرهابي، كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم.

وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة المدمرة. وتقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة، وذلك عن طريق الموقع الإلكتروني أو بواسطة وسائل البريد الإلكتروني من خلال منتديات الحوار وساحاته، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات، ووصولها إلى مختلف شرائح المجتمع.

وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة، فتارة ترسم أهدافا وخططا عامة للتنظيم الإرهابي، وأحيانا تكون للتهديد والوعيد بشن هجمات إرهابية معينة، في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار أو تصريحات صادرة من جهات أخرى¹⁴.

المطلب الثاني: إنشاء المواقع الإرهابية الإلكترونية

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير نمطه الإلكتروني غدا، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، حتى يضمّنوا انتشارا أوسع، وحتى لو تم منع الحصول على بعض هذه المواقع أو تعرضت بعضها للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها. لذا سنحاول دراسة تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية (الفرع الأول) ثم السيناريوهات المحتملة للإرهاب الإلكتروني (الفرع الثاني).

الفرع الأول: تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن هجمات إلكترونية من خلال الشبكات المعلوماتية، بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة

أهداف أساسية غالبا، وهي الأهداف: العسكرية، والسياسية والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها، وعلى رأسها مراكز القيادة والتحكم العسكرية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية، وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية¹⁵.

وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماما دون تدمير المواقع أو اختراقها بشكل دائم، فالتغيرات التقنية، وإلزام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open) source، سواء كان ذلك في مكونات نقطة الاتصال أو في الشبكة أو في البرمجة، جعلت الحلولة دون الاختراقات صعبة جدا، بالإضافة إلى أن هناك منظمات إرهابية يدخل من ضمن عملها ومسؤولياتها الرغبة في الاختراق وتدمير المواقع ومن المعلوم أن لدى المؤسسات من الإمكانيات والقدرات ما ليس لدى الأفراد¹⁶.

ويستطيع قراصنة الحاسبة الإلكترونية (Hackers) التوصل إلى المعلومات السرية والشخصية، واختراق الخصوصية وسرية المعلومات بسهولة، وذلك راجع إلى أن التطور المذهل في عالم الحاسب الآلي والشبكات المعلوماتية يصحبه تقدم أعظم في الجرائم المعلوماتية وسبل ارتكابها، ولا سيما وأن مرتكبيها ليسوا مستخدمين عاديين، بل قد يكونون خبراء في المجال الحاسبة الإلكترونية¹⁷.

ومن المتصور قيام أحد التنظيمات الإرهابية باختراق مواقع معينة بقصد السيطرة والتحكم فيها، وقد هيمن الذعر على

المختصين بمكافحة الإرهاب الإلكتروني عندما تمكن أحد الأشخاص من السيطرة على نظام الحاسبة الإلكترونية في أحد المطارات الأمريكية الصغيرة، وقام بإطفاء مصابيح إضاءة ممرات هبوط الطائرات¹⁸.

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

- 1- ضعف الكلمات السرية فبعض مستخدمي الإنترنت يجد أن بعض الكلمات أو الأرقام أسهل في الحفظ فيستخدمها، مما يسهل عملية كسر وتخمين الكلمات السرية من المخترق.
- 2- عدم وضع برامج حماية كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج والتي تعمل على التنبيه عند وجود حالة اختراق للموقع.
- 3- استضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج وأنظمة غير موثوقة أمنيا ولا يتم تحديثها باستمرار.
- 4- عدم القيام بالتحديث المستمر لنظام التشغيل والذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه، ويستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية¹⁹ تصدرها الشركات المنتجة لها لمنع المخربين من الاستفادة منها.

5- عدم القيام بالنسخ الاحتياطي للموقع (Backup) للملفات والمجلدات الموجودة فيه، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع وعدم إمكانية استرجاعها، ولذلك تبرز أهمية وجود نسخة احتياطية للموقع ومحتوياته خاصة مع تفاقم مشكلة الاختراقات في الآونة الأخيرة، ويعد عام 2002م من أكثر الأعوام اختراقاً، فقد تضاعفت حالات الاختراق والتدمير بسبب اكتشاف المزيد من الثغرات الأمنية في أنظمة التشغيل والبرامج المستخدمة في مزودات الإنترنت وانتشار كثير من الفيروسات²⁰.

وتعد الفيروسات من أخطر آفات الشبكات المعلوماتية، والفيروس عبارة عن برنامج حاسوبي يلحق ضرراً بنظام المعلومات والبيانات، ويقدر على التضاعف والانتشار، والانتقال من جهاز إلى آخر.

وفيروس الحاسبة الإلكترونية يتشابه مع الفيروس الطبيعي من نواح عديدة، فهو يغير خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة، وهو يتكاثر ويتنشر ويغير من شكله تماماً كالفيروس الطبيعي، والفيروسات أنواع متعددة، وهي متدرجة من حيث الأضرار التي تلحقها بالأجهزة بدءاً من الأضرار اليسيرة إلى تدمير النظام بأكمله، ويمكن للإرهابي استخدام

الفيروسات لنشر الدمار عبر الشبكات المعلوماتية والأنظمة الإلكترونية، كما يمكن استخدامها في الاختراق والتجسس أيضا.

الفرع الثاني: السيناريوهات المحتملة للإرهاب الإلكتروني:

لقد قام خبراء الجرائم الإلكترونية والأمن المعلوماتي بوضع أكثر من سيناريو محتمل للهجمات الإرهابية، وأودعوها في البحوث والدراسات والتقارير التي تعالج هذه المسألة، ويمكن تقسيم هذه السيناريوهات إلى ما يأتي:

أولا: استهداف النظم العسكرية والبنية التحتية الاقتصادية

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات، ويعد هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي، والصواريخ النووية، فقد تتوافر لإرهابي المعلومات فرصة فك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية، والأسلحة الفتاكة، فيحدث ما لا يحم عقباه على المستوى العالمي. كما أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة، وانفتاحها على العالم، هدفا مغريا للمجرمين والإرهابيين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالانطباعات

السائدة والتوقعات، والتشكيك في صحة هذه المعلومات أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة، وإضعاف الثقة في النظام الاقتصادي.

ويشمل هذا السيناريو إحداث خلل واسع في نظم الشبكات التي تتحكم بسرّيان أنشطة المصارف وأسواق المال العالمية، ونشر الفوضى في الصفقات التجارية الدولية، إضافة إلى ذلك يمكن إحداث توقف جزئي أو كلي في منظومات التجارة والأعمال، بحيث تتعطل الأنشطة الاقتصادية وتتوقف عن العمل²¹.

ثانياً: استهداف نظم المواصلات وتوليد الطاقة والماء

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها، مما قد ينجم عنه حصول تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى المدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات، وتغيير مواعيد الانطلاق بحيث تسود الفوضى، أو لتصادم هذه القطارات فيما بينها، وكذا بالنسبة للسفن والناقلات والغواصات البحرية²².

ويشمل هذا السيناريو مباشرة سلسلة من الهجمات المعلوماتية على نظم الحواسيب والشبكات المعلوماتية التي تنهض بمهام التحكم بشبكات توزيع الطاقة الكهربائية الوطنية، وينشأ عن مثل

هذه الهجمات تعطيل العيد من موافق الحياة في البلاد، وسيادة
الفوضى، نتيجة لانعدام مصادر الطاقة الكهربائية وشل الحركة في
عموم البلاد، وكذا بالنسبة لشبكات مصادر المياه وطرق توزيعها.

ولا يتوقف الأمر عند هذا الحد فقط، بل هناك العديد من
الأهداف الأخرى التي يمكن للمجرمين والإرهابيين المتمكنين من
خلالها أن يشيعوا الفساد، وينشروا الفوضى في العالم، فهناك على
سبيل المثال شبكات المعلومات الطبية، والتي يمكن من خلال
مهاجمتها واختراقها، ومن ثم التلاعب بها، حصول خسائر بشرية،
ومن أمثلة ذلك في العالم الغربي، ما قام به أحد المجرمين من الدخول
إلى سجلات المستشفيات والتلاعب بملفات المرضى بشكل أدى إلى
حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم، وحتى لو
افترضنا أن شبكات المعلوماتية الخاصة بالمؤسسات الطبية منيعة، فإن
رسالة واحدة تنشر مثلاً بالبريد الإلكتروني، مفادها أن هنالك دماء
ملوثة في المستشفيات وما إلى ذلك، يمكن لها أن تحدث آثاراً مدمرة
على الصعيد الاجتماعي²³.

ثالثاً: الترويع والتجسس الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل
الاتصالات، ومن خلال الشبكة العالمية للمعلومات (Internet)،
وتتعدد أساليب التهديد وتنوع طرقه، وذلك من أجل نشر الخوف
والرعب بين الأشخاص تلك التنظيمات الإرهابية من ناحية، ومن

أجل الحصول على التمويل المالي ولإبراز قوة التنظيم الإرهابي من ناحية أخرى.

والمقصود بالتهديد: الوعيد بشر، وزع الخوف في النفس وذلك بالضغط على إرادة الإنسان وتخويفه من أي ضرر ما سيلحقه أو سيلحق أشخاصا أو أشياء له بها صلة.

وقد يلجأ إرهابي الإلكتروني إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية، بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد (E-mails)، وكذلك التهديد عن طريق المواقع والمتديات وغرف الحوار والدرشة الإلكترونية.

ولقد تعددت الأساليب الإرهابية في التهديد، فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، ونحو ذلك²⁴.

ويقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الإلكتروني بالطريقة العصرية المتمثلة في استخدام الموارد

المعلوماتية والأنظمة الإلكترونية التي جلبتها التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية، وهي: التجسس العسكري والتجسس السياسي، والتجسس الاقتصادي.

وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق، ومن أشهرها البريد الإلكتروني حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، فهناك طرق أخرى لزرع أحصنة طروادة وكذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها، وكذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجة النصوص، كما يمكن للإرهابي استخدام الفيروسات في الاختراق والتجسس المعلوماتي.

ومن الأساليب الحديثة للتجسس الإلكتروني أسلوب إخفاء المعلومات داخل المعلومات، ويتلخص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في إن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية.

ومما يقوم به الإرهابيون اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس

عليها لمعرفة مراسلاتهم ومخاطبتهم والاستفادة منها في عملياتهم الإرهابية، أو تهديدهم لحملهم على إتيان أفعال معينة يخططون لاقترافها²⁵.

خاتمة:

من خلال هذا المقال الذي تكلمنا فيه عن مظاهر وأشكال الإرهاب الإلكتروني الذي أصبح هاجسا يخيف العالم الذي أصبح عرضا لهجمات الإرهابيين عبر الانترنت والذين يمارسون نشاطهم التخريبي من أي مكان في العالم وهذه المخاطر تتفاقم بمرور كل يوم لأن التقنية الحديثة التي يعتمد عليها براء التقنية الذين يتمون إلى الجماعات الإرهابية جد متطورة مقارنة بألية التصدي التقنية التي تعتبر ضعيفة وهي تحتاج إلى اتخاذ الكثير من التدابير والاحترازا لمواجهة الإرهاب الإلكتروني وبالنظر إلى الناحية التشريعية نجد بعض الدول لم تقر بعد قوانين متعلقة بمكافحة الإرهاب الإلكتروني ومن هنا توصلنا إلى:

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

- ضرورة السعي إلى إنشاء منظمة عربية للتنسيق وتبادل خبرات التقنية والتكنولوجيا من أجل مكافحة الإرهاب عبر الشكات المعلوماتية والأنظمة الالكترونية.
- التأكيد على أن الإرهاب الالكتروني يعتبر نموذج يتلاءم مع طبيعة الجريمة المنظمة مما يدعونا أن نقول لا بد على الدول إلى الإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.
- التحذير من تزايد مخاطر الإرهاب الالكتروني لاسيما ما لجأت إليه بعض المنظمات الإرهابية مؤخرا في نشر أعمالها الإرهابية على مواقع الانترنت وذلك بغرض زرع الرعب والخوف هذا من جهة، ومن جهة أخرى التنبيه إلى الهشاشة الأصلية في البنية التحتية للشبكات العالمية للمعلومات مما يمهّد لهجمات إرهابية ربما تؤدي إلى نتائج كارثية على مجتمعات الدولية والاقتصاد العالمي.

الهوامش:

1. غنية باطلي، الجريمة الالكترونية، دراسة مقارنة، منشورات الدار الجزائرية للنشر والتوزيع، الطبعة الأولى، سنة 2015، ص 30
2. علي عدنان الفيل، الإجرام الالكتروني، دراسة مقارنة، منشورات زين الحقوقية، الطبعة الأولى، سنة 2011، ص 66.

3. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول «حماية أمن المعلومات والخصوصية في قانون الإنترنت»، والمنعقد بالقاهرة في المدة من 2-4 يوليو، 2008، ص 11.
4. علي عدنان الفيل، المرجع السابق، ص 68.
5. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الثالثة، ص 69.
6. نبيل صقر، جرائم الكمبيوتر والانترنت في التشريع الجزائري، دار الهلال للخدمات الاعلامية، دون طبعة، ص 120.
7. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، الطبعة الأولى، دن سنة، ص 17.
8. غنية باطلي، المرجع السابق، ص 44.
9. عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، ص 12.
10. Jean François casile, le code pénal à l'épreuve de la délinquance informatique, presse universitaires, D'AIX, Marseille, PUAM, 2002, P97.
11. عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، ص 13.
12. علي عدنان الفيل، المرجع السابق، ص 80.
13. السامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، سنة 2007، ص 49.
14. Mohamed bozabar, la criminalité informatique sur l'internet, journal of law academic, N: 01, volume 26, faculté de droit, université du Koweit, 2002, P44.
15. موزة المزروعى، الاختراقات الإلكترونية خطر كيف نواجهه، مجلة آفاق اقتصادية، الإمارات العربية المتحدة، العدد (9) 2008، ص 54.
16. محمود عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الإنترنت)، منظور أمني، بحث مقدم إلى مؤتمر القانون والكمبيوتر

- والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3/5/2000، ص 42.
17. سهير حجازي، التهديدات الإجرائية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي، الإمارات العربية المتحدة، العدد (91).
18. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد في المدة من 2-4/6/2008، ص 19.
19. حذرت شركة مايكروسوفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز وتقول الشركة: إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجية، ودعت المستخدمين إلى تركيب برنامج ترقيعي لحل المشكلة، جريدة الرياض، العدد (12542)، السبت 20/8/1423هـ، ص 19.
20. جريدة الرياض، العدد (12460)، يوم الاثنين 26/5/1423هـ، ص 32.
21. د. عماد علي الخليل، التكتيف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الإنترنت (دراسة علمية في ظل أحكام قانون العقوبات الأردني)، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت الذي نظمته كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الاستراتيجية ومركز تقنية المعلومات بجامعة الإمارات العربية المتحدة في الفترة 1-3/5/2000، ص 4.
22. عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، ص 21. وكذلك علي عدنان الفيل، المرجع السابق، ص 92.
23. عدنان علي الفيل، المرجع السابق، ص 95.
24. عبد الله بن عبد العزيز بن فهد العجلان، المرجع السابق، ص 22.
25. عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من 2-4/6/2008، ص 23.

