

الارهاب الالكتروني: الأشكال والدوافع

أ/ شعني صابرة - جامعة تبسة

ملخص:

مع نمو شبكة الانترنت في كل من حجمها ووظيفتها شهد العالم تغييرا هائلا في كل من طبيعة التهديدات ومستوى النشاط الهجومي الموجه ضد الانترنت والانظمة المتصلة به.

ومع بداية موجة الانتشار التكنولوجي عالميا وتساعد مستوى الاهتمام بقطاع تكنولوجيا الاتصال والمعلومات بوصفها مدخلا مهما لتحقيق نمو اقتصادي سريع، جاء ظهور التهديد بالاستخدام السلبي لتلك المعطيات التكنولوجية من قبل مهددات كثيرة: مثل امكانية استخدام تلك المعطيات في التحضير او القيام او التنسيق او التعبئة او الحشد للعمل الارهابي، وقد ظهرت مسميات تعبر في مجملها عن أنشطة غير سلمية للفضاء الالكتروني على نحو يؤثر في طبيعته ودوره، ويؤثر بالتالي على اهمية الاستراتيجية في النظام الدولي، ومن ضمن تلك المسميات وأهمها وأشهرها " الارهاب الالكتروني "

Résumé.

Avec la croissance de l'Internet à la fois en taille et en fonction du monde est témoin d'un énorme changement dans la fois la nature des menaces et du niveau d'activité offensive dirigée contre l'Internet et des systèmes connexes, et avec le début d'une vague de diffusion technologique à l'échelle mondiale et la hausse du niveau d'intérêt dans le secteur des technologies de la communication et de l'information comme une contribution importante à réaliser une croissance économique rapide, est venu à l'émergence de la menace de l'utilisation négative de ces données technologiques par de nombreuses menaces: tels que la possibilité d'utiliser ces données pour préparer ou faire, le format ou l'emballage ou la foule à travailler Le terroriste, ont des noms reflètent dans son intégralité pour les activités espace-mail non pacifiques d'une manière affecte la nature et le rôle ont émergé, et donc d'affecter l'importance de la stratégie dans le système international, et au sein de ces titres, le plus important et le plus célèbre «terrorisme cybernétique» la

مقدمة.

إن انتشار شبكة الانترنت وتطورها فتح مجالات عديدة للاستفادة منها ولكن في نفس الوقت أدى ذلك الى نشر ثقافة منافية لعادات وطباع الكثير من المجتمعات وخاصة العربية منها نتيجة للانفتاح الذي فرضته هذه التقنيات وأيضا نتيجة إلى توفير المعلومات التي يمكن استخدامها فيما يحقق مصلحة للبشرية وأيضا ما يحقق ضررا لها مؤسسة لانتشار الجريمة المعلوماتية، ولعل أخطر هذه الجرائم في الوقت الراهن هو جريمة الارهاب الالكتروني.

فالإرهاب الالكتروني يتميز عن غيره من أنواع الارهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الالكترونية التي جلبتها التقنية في عصر المعلومات، لذا فان الأنظمة الالكترونية والبنية التحتية المعلوماتية هي هدف الارهابيين.

ولما كان الارهاب الالكتروني يشير إلى عنصرين أساسيين وهما فضاء الانترنت، والارهاب، إضافة إلى الفضاء الالكتروني او العالم الافتراضي والذي يشير الى التمثيل الرمزي والمجازي للمعلومات. وهو المكان الذي تعمل فيه أجهزة وبرامج الحاسبة الالكترونية والشبكات المعلوماتية، فالسؤال الذي سوف نحاول الاجابة عليه من خلال هذه الدراسة - المتواضعة - ما المقصود بالإرهاب الالكتروني؟، وما يميزه عن الارهاب التقليدي؟

المبحث الاول : مفهوم الارهاب الالكتروني وتحديد أركانه

ومن خلال هذا المبحث سوف نتعرض الى مطلبين نخصص الاول الى تعريف الارهاب الالكتروني والثاني الى اركان جريمة الارهاب الالكتروني .

المطلب الأول: تعريف الارهاب الالكتروني

قبل التعرض الى تعريف الارهاب الإلكتروني باعتباره جريمة عصرية كان لزاما علينا أن نتعرض الى أهم المحاولات لتعريف الجريمة التقليدية على اعتبار أن الإرهاب الإلكتروني يعتبر امتداد للجريمة التقليدية.

الفرع الاول: تعريف الارهاب التقليدي (الارهاب بشكل عام)

الارهاب في اللغة العربية مصدر أرهب يرهب ارهابا وترهيبا، وأصله مأخوذ من الفعل الثلاثي رهب بكسر الهاء ويرهب رهبة ورهبا بضم الراء أي خاف، ورهب الشيء اي خافه، وأرهبه واسترهبه أخافه، وترهبه توعده، والرهبة تعني الخوف والفرع.

وقد جاء في تاج العروس الارهاب بالكسر يعني الازعاج والاختافة¹

أما مجمع اللغة العربية في معجمه الوسيط فقد أطلق على الإرهابيين أنه وصف يطلق على الذين يسلكون سبيل العنف لتحقيق أهدافهم، ويعني الإرهاب في اللغات الأجنبية القديمة حركة من الجسد تفزع الآخرين².

وتجدر الإشارة الى ان المجتمع الدولي لم يصل الى غاية اليوم الى تعريف جامع مانع متفق عليه للإرهاب وهذا راجع الى تنوع أشكاله وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، الا ان هذا لا يمنعنا من التعرض لبعض المحاولات حول تعريف هذه الظاهرة الاجرامية الخطيرة.

فقانون العقوبات المصري عرف الإرهاب بأنه " كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجا اليه الجاني تنفيذا لمشروع إجرامي فردي أو جماعي بهدف الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر اذا كان من شأن ذلك إيذاء الاشخاص أو القاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو امنهم للخطر أو الحاق الضرر بالبيئة أو بالاتصالات او بالمواصلات او بالأموال او المباني او بالأموال العامة او الخاصة او احتلالها او الاستيلاء عليها او منع او عرقلة ممارسة السلطات العامة او دور العبادة او معاهد العلم لأعمالها او تعطيل تطبيق الدستور او القوانين او اللوائح"³.

أما قانون العقوبات الاردني فقد عرف الإرهاب في نص المادة 147 في الفقرة الاولى منها على انه " استخدام العنف أو التهديد باستخدامه أيا كانت بواعثه وأغراضه يقع تنفيذا لعمل فردي أو جماعي بهدف الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر اذا كان من شأن ذلك ايقاع الرعب بين الناس وترويعهم أو تعريض حياتهم للخطر أو الحاق الضرر بالبيئة أو المرافق أو الاملاك العامة او الاملاك الخاصة او المرافق الدولية والبعثات الدبلوماسية او باحتلال اي منها او الاستيلاء عليها او تعريض الموارد الوطنية للخطر او تعطيل تطبيق الدستور والقوانين"⁴.

المشرع الجزائري عرف الإرهاب في المرسوم التشريعي رقم 92-03 المؤرخ في 1992/09/30 ذلك بقوله " انه أية مخالفة تستهدف امن الدولة ووحدة الإقليم، واستقرار المؤسسات وسيرها العادي بواسطة عمل هدفه زرع الخوف في وسط السكان وخلق انعدام الأمان والمساس بالأشخاص والممتلكات..."⁵ وأورد المشرع الفعل والعمل كتعبير عن السلوك الإجرامي، وقد نصت المادة 87 مكرر من قانون العقوبات الأمر رقم 95-11 المؤرخ في فبراير 1995 يعتبر فعلا إرهابيا أو تخريبيا في مفهوم هذا الأمر. " كل فعل يستهدف امن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي عن طريق أي عمل غرضه ما يأتي :

- بث الرعب في أوساط السكان وخلق جو انعدام الأمن من خلال الاعتداء المعنوي والجسدي على الأشخاص أو تعريض حياتهم أو أمنهم للخطر أو المس بممتلكاتهم.
- عرقلة حركة المرور أو حرية التنقل في الطرق والتجمهر أو الاعتصام في الساحات العمومية.
- الاعتداء على رموز الأمة والجمهورية ونش أو تدنيس القبور.
- الاعتداء على وسائل المواصلات والنقل والملكيات العمومية والخاصة والاستحواد عليها أو احتلالها دون مسوغ قانوني⁶
- أما عن الفقه فمجمع البحوث الإسلامية بالزهر عرف الارهاب بأنه: "ترويع الأمنين وتدمير مصالحهم ومقومات حياتهم والاعتداء على أموالهم واغراضهم وحياتهم وكرامتهم الانسانية، بغيا وفسادا في الارض"
- وعرف مجمع الفقه الاسلامي التابع لرابطة العالم الاسلامي الرهاب بأنه: "العدوان الذي يمارسه افراد او جماعات او دول بغيا علة الانسان في دينه ودمه وعقله وماله وعرضه ويشمل صنوف التخويف والأذى والتهديد والقتل بغير حق وما يتصل بصور الحراية واخافة السبيل وقطع الطريق وكفعل من افعال العنف او التهديد يقع تنفيذ لمشروع اجرامي فردي او جماعي، ويهدف الى القاء الرعب بين الناس او ترويعهم بإيذائهم او تعريض حياتهم او امنهم او اموالهم للخطر، ومن صنوفه الحاق الضرر بالبيئة او بأحد المرافق والاملاك العامة او الخاصة، او تعريض احد الموارد الوطنية او الطبيعية للخطر، فكل هذا من صور الفساد في الارض التي نهى اله سبحانه وتعالى المسلمين عنها"⁷
- الاتفاقية العربية لمكافحة الارهاب عرفته بأنه: "كل فعل من افعال العنف او التهديد به أيا كانت دوافعه او اغراضه يقع تنفيذا لمشروع اجرامي فردي او جماعي ويهدف الى القاء الرعب بين الناس او ترويعهم بإيذائهم او تعريض حياتهم او حرياتهم او امنهم للخطر او الحاق الضرر بالبيئة أو بأحد المرافق او الاملاك العامة او الخاصة او احتلالها او الاستيلاء عليها او تعريض الموارد الوطنية للخطر"⁸
- هذا ونشير إلى أن تعريف الارهاب الذي جاءت به كل من الاتفاقية الدولية لمكافحة الارهاب في جنيف عام 1937 وكذلك الاتحاد الاوروبي عام 2002 لا يختلف على التعريفات السابقة كون الأعمال الارهابية أعمال تتسم بالعنف والتخريب وهدفها الترويع والإخافة.

الفرع الثاني: تعريف الارهاب الالكتروني.

إذا سلمنا بفكرة مفادها ان مفهوم الارهاب كمصطلح تقليدي اصبح واضح الى حد ما، فإن الارهاب الإلكتروني كمفهوم مستحدث يكتنفه الكثير من الغموض، وذلك انه يعتمد على تقنية أنظمة المعلومات من حيث وسيلة ارتكابه ومن حيث دور الفاعل فيه وطبيعة سلوكه، وفضلا عن ذلك فان نتائجه تطول امن المعلومات وتقنية أنظمة المعلومات بالإضافة الى ما يتسبب به من اضرار واسعة الانتشار وعظيمة الاثر على المجتمعات والافراد⁹.

وقد كان اول استخدام لكلمة الارهاب الالكتروني في فترة الثمانينات في دراسة "Barry Collin" التي خلص فيها الى صعوبة تعريف ظاهرة الارهاب التكنولوجي بدقة وايضا الاساليب والحلول المطلوبة لمواجهته، وكذلك تحديد دور الكمبيوتر والانترنت في العمل الارهابي.

وفي بداية التسعينات صدر تقرير عن الاكاديمية الوطنية الامريكية للعلوم عن امن الكمبيوتر جاء فيه: "نحن بصدد مخاطر متزايدة بسبب اعتماد الولايات المتحدة على اجهزة الكمبيوتر، حيث غدا بإمكان الارهابيين احداث تدمير اكبر بالاعتماد على لوحة المفاتيح اكثر من استخدام القنبلة، وقد يتسبب ذلك في بيرل هاربر الكتروني جديد"¹⁰

وطبقا لتعريف وكالة المخابرات المركزية الأمريكية فان الارهاب الالكتروني هو: "أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر وبرامجه، والبيانات والمعلومات والتي تنتج من عنف ضد الاهداف المدنية عن طريق جماعات دون قومية او عملاء سريين"¹¹.

أما مركز حماية البنية التحتية القومية الامريكية فقد عرف الارهاب الالكتروني على ان "عمل اجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر وبرامجه، والاتصالات السلكية واللاسلكية ينتج عنه تدمير او تعطيل الخدمات لبث الخوف، بهدف ارباك وزرع الشك لدى السكان، وذلك بهدف التأثير على الحكومة او السكان لخدمة اجندة سياسية او اجتماعية او ايديولوجية"¹²

وهناك من عرفه بأنه "هجمات غير قانونية وتهديدات بالهجوم ضد اجهزة الحاسبات والشبكات والمعلومات المخزنة وذلك لكي توظف لتخويف او اجبار حكومة او شعبها بهدف تعزيز أهداف سياسية او اجتماعية، ولكي يكون ارهابا يجب ان ينتج عنه تجاه الافراد او الممتلكات او على الاقل التسبب في ضرر ينتج عنه توليد الخوف.

أما مركز الدراسات الاستراتيجية والدولية فيعرف الإرهاب الإلكتروني على أنه: "استخدام أدوات شبكات الكمبيوتر لتعطيل البنية التحتية القومية مثل الطاقة، المواصلات، عمليات الحكومة، أو إكراه أو ترهيب الحكومة، أو السكان المدنيين"¹³.

وزارة الدفاع الأمريكية هي الأخرى وضعت تعريفا للإرهاب الإلكتروني مفاده: "أنه عمل إجرامي يتم الأعداد له باستخدام أجهزة الحاسبات ووسائل الاتصالات، ينتج عنه عنف وتدمير أو بث الخوف تجاه تلقي الخدمات، بما يسبب الارتباك وعدم اليقين، وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة"¹⁴.

وعلى ذلك ومما سبق يمكن تعريف الإرهاب الإلكتروني: "العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الافراد على الانسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى صنوفه وصور الإفساد في الأرض"¹⁵.

فالإرهاب الإلكتروني اذا يعتمد على استخدام الامكانيات العلمية والتقنية، واستغلال وسائل والشبكات المعلوماتية من اجل تخويف وترويع الآخرين، والحاق الضرر بهم، أو تهديدهم، مثل ما حصل في عام 2000، حينما أدى انتشار فيروس الحاسوب "I Love you" الى اتلاف معلومات قدرت قيمتها حوالي 10 مليارات دولار امريكي، اما في عام 2003 فقد أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسبات الالكترونية، وقدر مجلس اوربا في الاتفاقية الدولية لمكافحة الاجرام عبر الانترنت كلفة اصلاح الاضرار التي تسببها فيروسات المعلوماتية بنحو 12 مليار دولار امريكي سنويا¹⁶.

المطلب الثاني: أركان جريمة الإرهاب الإلكتروني.

كغيرها من الجرائم الأخرى فان جريمة الارهاب الإلكتروني تقوم بقيام أركانها وسوف نركز على كل من الركن المادي والمعنوي .

الفرع الاول : الركن المادي في جريمة الارهاب الإلكتروني

يأخذ الركن المادي في جريمة الارهاب الإلكتروني العديد من الصور والأشكال، وهي تتوافر بتحقيق امكانية ايقاع الفعل باستخدام تقنية أنظمة المعلومات، وفي كل حالة يرتبط فيها النشاط موضوع الفعل بنطاق الكتروني يعتمد عليه شريطة تحقق ما يلي:

- أولا: استخدام قدر كافي من العنف التهديدي، ومفهوم العنف في هذه الجريمة الالكترونية مستحدث اي ذو بعد معنوي، بمعنى ان ينظر الى العنف كنتيجة لسلوك معنوي الكتروني، ويظهر في مدى قدرة الفاعل

- على استخدام تقنية أنظمة المعلومات بقدر كاف لإيقاع الضرر المقصود، اما التهديد بالعنف فامر ممكن في ظل بيئة الكترونية¹⁷.
- **ثانيا:** ان يكون من شأن استخدام هذا العنف او التهديد به ايقاع الرعب بين الناس او تعريض حياتهم الى الخطر
- **ثالثا:** ان يتبع تنفيذاً لعمل فردي او جماعي.
- ومن أشكال السلوك المادي القادر على اظهار الارهاب الالكتروني الى حيز الوجود كجرائم مستوجبة العقاب ومن ذلك:
- استخدام العنف او التهديد باستخدامه بهدف تعريض امن المجتمع الى الخطر او الاخلال بالنظام العام فيه، او الحاق الضرر بالبيئة، او بالمرافق العامة، او الحاق الضرر بالموارد الوطنية، او تعطيل أحكام الدستور والقوانين، وفي هذه الحالات يكفي فقط احتمال وقوع الضرر.
- القيام بأية عملية مصرفية الكترونية داخلية او خارجية تتعلق بإيداع الاموال لدى البنوك من احدى المؤسسات المالية شريطة ان تكون لهذه الاموال شبهة الصلة بعمل اراهابي.
- استخدام العنف او التهديد باستخدامه بهدف تعطيل الاتصالات او أنظمة الحاسوب، او بهدف اختراق شبكات تقنية أنظمة المعلومات او التشويش عليها¹⁸.
- هذا وقد اشارت الاتفاقية العربية لمكافحة جرائم تقنية نظم المعلومات في المادة 15 منها الى العديد من السلوكيات التقنية المتعلقة بالإرهاب وهي كما يلي:
- نشر افكار ومبادئ جماعات اراهابية والدعوة لها والمرتكبة بواسطة تقنية المعلومات.
- تسهيل العمليات الارهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الارهابية بواسطة تقنية المعلومات
- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في العمليات الارهابية بواسطة تقنية المعلومات....¹⁹.

الفرع الثاني : الركن المعنوي في جريمة الارهاب الالكتروني.

إذا كانت الجريمة بشكل عام تقوم على الركن المعنوي القائم على عنصري العلم والارادة، فان الارهاب الالكتروني لا يكفي فيه القصد العام، اذ لا يكفي علم الفاعل بالسلوك الجرمي الذي يرتكبه، واردة ارتكاب هذا السلوك لقيام الجريمة بل لا بد من ثبوت القصد الخاص، بالإضافة الى القصد العام في حق الفاعل، هذا القصد الخاص الذي يتمثل في الارهاب الالكتروني بالغرض الارهابي، فلا بد من ان يتوافر في نية الفاعل وهو يقدم على استخدام تقنية نظم

المعلومات ان يوقع او يهدد بإيقاع احد الاغراض المعلنة في نصوص التجريم، لما سيقدم عليه من فعل الكتروني فان لم يتوافر ذلك لم تقم الجريمة.²⁰

المبحث الثاني: أسباب الارهاب الالكتروني وأساليبه

لقد ادت كثرة أسباب ودوافع الارهاب الالكتروني الى تنوع الأساليب والأشكال التي تتخذها جريمة الارهاب الالكتروني كما يلي:

المطلب الاول: الاسباب الخاصة بالإرهاب الالكتروني.

إن أسباب الارهاب الالكتروني ودوافعه كثيرة ومتنوعة وهي عينها اسباب ظاهرة الارهاب عموماً، لكن يجدر التنبيه إلى ان هناك العديد من العوامل والبيئات الخاصة التي تجعل من ظاهرة الارهاب الالكتروني موضوعاً مناسباً وسلاحاً سهلاً للجماعات والمنظمات الارهابية.

الفرع الاول: ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق.

إن شبكات المعلومات مصممة في الاصل بشكل مفتوح دون قيود او حواجز أمنية عليها، رغبة في التوسع وتسهيل دخول المستخدمين، وتحتوي الانظمة الالكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الارهابية استغلال هذه الثغرات في التسلل الى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية الارهابية²¹

الفرع الثاني: غياب الحدود الجغرافية وتدني مستوى المخاطرة.

ان غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة الى عدم وضوح الهوية الرقمية للمستخدم المستوطن في بيئته المفتوحة يعد فرصة مناسبة للإرهابيين، حيث يستطيع محترف الحاسوب ان يقدم نفسه بالهوية والصفة التي يرغب بها او يتخفى تحت شخصية وهمية، ومن ثم يشن هجومه الالكتروني وهو مسترخي في منزله من دون مخاطرة مباشرة وبعيدا عن أعين الناظرين²²

الفرع الثالث: سهولة الاستخدام وقلة التكلفة.

إن السمة العولمية لشبكات المعلومات تتمثل في كونها وسيلة سهلة الاستخدام، طيبة الانقياد قليلة الكلفة لا تستغرق وقتاً ولا جهداً كبيراً، مما هياً للإرهابيين فرصة ثمينة للوصول الى اهدافهم غير المشروعة، ومن دون الحاجة الى مصادر تمويل ضخمة فالقيام بشن هجوم ارهابي الكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة²³.

الفرع الرابع: صعوبة اكتشاف وإثبات الجريمة الإرهابية

حيث ان الكثير من الجرائم المعلوماتية يصعب فيها العلم بوقوع الجريمة، اصلا لان الجاني كثيرا ما يستخدم اسما مستعارا، وهذا ما يساعد الارهابي على الحركة بحرية داخل المواقع التي يستهدفها، قبل ان ينفذ جريمته، بالإضافة الى ان هذه الجرائم صعبة الاثبات لأنها لا تترك أثرا ماديا بسبب امكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثواني قليلة، وصعوبة الاثبات هذه تعتبر من أقوى الدوافع المساعدة على ارتكاب جريمة الارهاب الالكتروني²⁴.

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

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالية حول الجرائم المعلوماتية والارهاب الالكتروني يعتبر من الاسباب الرئيسية في انتشار الارهاب الالكتروني، وكذلك لو وجدت قوانين تجرime متكاملة فان المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الارهابي في بلد آخر به قوانين جد صارمة وهنا تثار مشكلة تنازع القوانين والقانون الواجب التطبيق²⁵.

كما أن عدم وجود جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتسيطر على مدخلاتها ومخارجاتها يعد سببا مهما في نقشي ظاهرة الارهاب الالكتروني، حيث يمكن لكل شخص الدخول ووضع ما يريد على الشبكة وكل ما تملكه الجهات التي تحاول فرض الرقابة هو المنع من الوصول الى بعض المواقع المحجوبة، او اغلاقها وتدميرها بعد نشر المجرم لما يريده فيها.

ولكل هاته الأسباب أصبح الارهاب الالكتروني هو الأسلوب الأمثل والخيار الاسهل للمنظمات الارهابية.

المطلب الثاني: أساليب الارهاب الالكتروني.

من الصعب تحديد أشكال او مظاهر الارهاب الالكتروني فطبيعة هذا النوع من الجرائم تتطلب التصنيف نظرا لأنها تستخدم تكنولوجيا تتطور يوما بعد يوم، فالإرهاب الالكتروني يرتبط بالمستوى المتقدم الذي تحتله وسائل الاتصال وتقنية المعلومات في جميع مجالات الحياة، وفي العالم بأسره، ومن خلال الانظمة الالكترونية والشبكات المعلوماتية اتخذ الارهاب أبعادا جديدة وازدادت خطورته على المجتمع الدولي.

الفرع الأول: البريد الإلكتروني

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

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

وكذلك يقوم الإرهابيون باستغلال البريد الإلكتروني في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر المراسلات الإلكترونية. ومما يقوم به الإرهابيون أيضا اختراق البريد الإلكتروني للآخرين وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية²⁶.

الفرع الثاني: انشاء مواقع على الانترنت.

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

والموقع هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل Hyper text mark up language (HTML) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (Browser WWW)

ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة²⁷.

وتسعى الجهات الرسمية، والمؤسسات، والشركات، وحتى الأفراد إلى إيجاد مواقع لهم حتى وصل عدد المواقع على الانترنت في شهر أكتوبر 2000 إلى أكثر من 22 مليون موقع.

إن الشبكة العنكبوتية (World Wide Web) أو نظام الويب الذي ابتكره العالم الإنجليزي تيم بيرنرس1989م يركز على فكرة تخزين معلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت، ومن هنا أطلقت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجاناً عبر شبكة الإنترنت في عام 1991 م، واعتمد في المرحلة الأولى عام 1993 م، من خلال برامج التصفح.

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

لقد وجد الإرهابيون بغيتهم في تلك الوسائل الرقمية في ثورة المعلوماتية، فأصبح للمنظمات الإرهابية العديد من المواقع على شبكة المعلومات العالمية الإنترنت، فغدت تلك المواقع من أبرز الوسائل المستخدمة في الإرهاب الإلكتروني²⁸.

الفرع الثالث: تدمير المواقع.

تدمير المواقع يقصد به: الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي (Server-PC) أو مجموعة نظم مترابطة شبكياً بهدف تخريب نقطة الاتصال أو النظام وليس هناك وسيلة تقنية أو تنظيمية يمكن تطبيقها وتحول تماماً دون تدمير المواقع أو اختراق المواقع بشكل دائم، فالمتغيرات التقنية وإمام المخترق بالثغرات في التطبيقات والتي بنيت في معظمها على أساس التصميم المفتوح لمعظم الأجزاء (Open source) سواء كان ذلك في مكونات نقطة الاتصال أو النظم أو الشبكة أو البرمجة، جعلت الحيلولة دون الاختراقات صعبة جداً، إضافة 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 الأفراد.

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

إن عملية الاختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي²⁹.

الفرع الرابع: التجسس الإلكتروني.

يقوم 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 حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاث أهداف رئيسية: التجسس العسكري، والتجسس السياسي، والتجسس الاقتصادي³⁰.

وفي عصر المعلومات ومع وجود وسائل التقنية الحديثة فإن حدود الدولة مستباحة بأقمار التجسس والبعث الفضائي، وقد تحولت وسائل التجسس

التقليدية الى الطرق الالكترونية وهذا بعد ظهور الشبكات المعلوماتية وانتشارها عالميا.

وتجدر الإشارة الى انه ليس كل اختراق للمواقع يعتبر من قبيل الارهاب الالكتروني فقط لو كان هذا التجسس يهدف الوصول الى اسرار ومعلومات امن الدولة واعطائها الى دولة اخرى معادية، او استغلال هذه الاسرار بما يضر الوحدة الوطنية والمصالح العامة .

خاتمة

أصبح الإرهاب الإلكتروني هاجسا يخيف العالم الذي أصبح عرضة لهجمات الإرهابيين عبر الإنترنت الذين يمارسون نشاطهم التخريبي من أي مكان في العالم، وهذه المخاطر تتفاقم بمرور كل يوم، لأن التقنية الحديثة وحدها غير قادرة على حماية الناس من العمليات الإرهابية الإلكترونية والتي سببت أضرارا جسيمة على الأفراد والمنظمات والدول. ولقد سعت العديد من الدول إلى اتخاذ التدابير والاحترازاات لمواجهة الإرهاب الإلكتروني، إلا أن هذه الجهود قليلة ولا تزال بحاجة إلى المزيد من هذه الجهود المبذولة لمواجهة هذا السلاح الخطير.

فالإرهاب الإلكتروني أصبح خطرا يهدد العالم بأسره، ويكمن الخطر في سهولة استخدام هذا السلاح مع شدة أثره وضرره، فيقوم مستخدمه بعمله الإرهابي وهو في منزله أو مكتبه، أو في مقهى، أو حتى من غرفته في أحد الفنادق

الهوامش:

- ¹ ابن فارس معجم مقاييس اللغة، الطبعة الأولى، دار الكتب العلمية، 1420 هـ/ 1999.
- ² علي عدنان الفيل، الاجرام الالكترونية- دراسة مقارنة، الطبعة الاولى، منشورات زين الحقوقية، بيروت، 2011، ص 53.
- ³ قانون العقوبات المصري المعدل بالقانون رقم 97 لسنة 1992.
- ⁴ قانون العقوبات الأردني المعدل بالقانون رقم 54 لسنة 2001.
- ⁵ المرسوم التشريعي رقم 29-03 المؤرخ في 1992/09/30
- ⁶ الأمر 95-11 المؤرخ في 25 فبراير 1995 .
- ⁷ علي عدنان الفيل، مرجع سابق، ص 55.
- ⁸ الاتفاقية العربية لمكافحة الارهاب الصادرة في القاهرة عام 1998.
- ⁹ اسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان- الاردن، 2014، ص 321.
- ¹⁰ عادل صادق، استخدام الارهاب الالكتروني في الصراع الدولي، دار الكتاب الحديث، القاهرة، 2015، ص 104.
- ¹¹ عادل صادق، نفس المرجع، ص 106.

- ¹² عادل عبد الصادق، قمة تونس العالمية للمعلومات: استمرار الوضع الراهن" مجلة تعليقات مصرية الكترونية، مركز الدراسات السياسية والاستراتيجية بالأهرام العدد 22، 44/11/2005، متوافرة في موقع: www.ahrm.rg.eg/acpss/ahram/2005/11/22/COMMO.HTM
- ¹³ عادل صادق، استخدام الارهاب الالكتروني في الصراع الدولي، مرجع سابق، ص 106.
- ¹⁴ عادل صادق، استخدام الارهاب الالكتروني في الصراع الدولي، مرجع سابق، ص 106.
- ¹⁵ عبد الرحمان السند، وسائل الارهاب الالكتروني-حكمها في الاسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر العالمي عن موقف الاسلام من الارهاب، جامعة الامام محمد بن سعود الاسلامية، ص 5 .
- ¹⁶ علي عدنان الفيل، مرجع سابق، ص 60.
- ¹⁷ اسامة احمد المناعسة، جلال محمد الزعبي، مرجع سابق، ص 323.
- ¹⁸ اسامة احمد المناعسة، جلال محمد الزعبي، نفس المرجع، ص 324.
- ¹⁹ اسامة احمد المناعسة، جلال محمد الزعبي، نفس المرجع، ص 327.
- ²⁰ اسامة احمد المناعسة، جلال محمد الزعبي، نفس المرجع، ص 328.
- ²¹ عبد الله بن عبد العزيز بن فهد العجلان، الارهاب الالكتروني في عصر المعلومات، بحث مقدم الى المؤتمر الدولي الاول حول حماية امن المعلومات والخصوصية في قانون الانترنت، القاهرة يومي 4، 2008/06/، ص 11.
- ²² علي عدنان الفيل، مرجع سابق، ص 72
- ²³ أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، الطبعة الاولى، مكتبة الوفاء القانونية، الاسكندرية، 2011، ص 227.
- ²⁴ علي عدنان الفيل، مرجع سابق، ص 73.
- ²⁵ عبد الله بن عبد العزيز بن فهد العجلان، مرجع سابق، ص 12.
- ²⁶ عبد الرحمان السند، مرجع سابق، ص 5.
- ²⁷ مصطفى يوسف كافي، ماهر عودة الشمائلة، محمود عزت اللحام، الاعلام والارهاب الالكتروني، الطبعة الاولى، دار الاعصار العلمي، عمان-الاردن، 2015، ص 154.
- ²⁸ عبد الرحمان السند، مرجع سابق، ص 9.
- ²⁹ عبد الرحمان السند، مرجع سابق، ص 11.
- ³⁰ علي عدنان الفيل، مرجع سابق، ص 97.