الإرهاب الإلكترونى: الظاهرة والتداعيات "الاستخدام من قبل التنظيمات الجهادية"

إنجى المهدى*

لقد تطورت الظاهرة الإرهابية تطورًا نوعيا كبيرا فى أساليبها وصورها ووسائلها، حيث بات الإرهابيون يستخدمون أدوات التكنولوجيا الحديثة ووسائلها للتخطيط للعمليات الإرهابية، ومن أجل بث الكراهية وخطابات التطرف والتحريض على العنف وإقصاء الغير، إضافة إلى استخدامها لتجنيد الأتباع والحصول على التمويل اللازم. فظهر الإرهاب الإلكترونى إلى حيز الوجود، متخذا بعدا جديدا يختلف عن الإرهاب التقليدى، وبحيث صارت إمكانات الفضاء الإلكترونى الواسع تسخر ليس فقط لارتكاب الجرائم الإرهابية التقليدية، بل ولاستحداث جرائم جديدة لم تشهدها الجماعة الدولية من قبل.

تقدم الورقة البحثية دراسة عميقة لظاهرة الإرهاب الإلكترونى، وكيف يمكن استخدامه من قبل التنظيمات المتطرفة، من خلال دراسة نقاط عديدة: كالمفهوم والخصائص، وأسباب تصاعد انتشار الظاهرة، وما يمثله الإرهاب الإلكترونى من مخاطر وتهديدات، وأخيرا استغلال الجماعات المتطرفة له، وذلك لوضع نقاطا على حروف فى طريق المواجهة والتصدى لمثل هذا الخطر الكبير على السلم والأمن الدوليين.

مقدمة

بات الإرهاب الدولى واحدا من أخطر التحديات التى تواجه الجماعة الدولية، وصار ظاهرة انتشرت وتفاقمت منذ ستينيات القرن العشرين، مما دعا البعض إلى وصفه بالظاهرة التى أصبحت تهدد سلم العالم وأمنه واستقراره. ولعل أكثر صور الإرهاب خطورة فى الآونة المعاصرة، هو الإرهاب الالكترونى الذى نتج عن التزاوج ما بين الإرهاب والفضاء الالكترونى أو السيبرانى. والواقع، أنه على الرغم من الإجماع

* أستاذ العلوم السياسية المساعد، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

المجلة الاجتماعية القومية، المجلد الثامن والخمسين، العدد الأول، يناير ٢٠٢١.

الدولى الواسع على خطورة ظاهرة الإرهاب عموما، والإرهاب الإلكترونى بصفة خاصة، فإن إجماعا مماثلا حول تعريف هذه الظاهرة وبيان أسبابها ودوافعها غير متحقق، مما حال دون التصدى لها، منعا وقمعا، بالدرجة المطلوبة من الفاعلية والحسم[١].

وتسعى الورقة البحثية إلى فهم أعمق لظاهرة الإرهاب الإلكترونى، وكيف يمكن استخدامه من قبل التنظيمات المتطرفة، من خلال دراسة نقاط عديدة: كالمفهوم والخصائص، وأسباب تصاعد انتشار الظاهرة، وما يمثله الإرهاب الإلكترونى من مخاطر وتهديدات، وأخيرا استغلال الجماعات المتطرفة له، وذلك لوضع النقاط على الأحرف فى طريق المواجهة والتصدى لمثل هذا الخطر الكبير على السلم والأمن الدوليين.

لقد تطورت الظاهرة الإرهابية تطورًا نوعيا كبيرا فى أساليبها وصورها ووسائلها، حيث بات الإرهابيون يستخدمون أدوات التكنولوجيا الحديثة ووسائلها للتخطيط للعمليات الإرهابية، ومن أجل بث الكراهية وخطابات التطرف والتحريض على العنف وإقصاء الغير، إضافة إلى استخدامها لتجنيد الأتباع والحصول على التمويل اللازم. فظهر الإرهاب الإلكترونى إلى حيز الوجود، متخذا بعدا جديدا يختلف عن الإرهاب التقليدى، وبحيث صارت إمكانات الفضاء الإلكترونى الواسع تسخر ليس فقط لارتكاب الجرائم الإرهابية التقليدية، بل ولاستحداث جرائم جديدة لم تشهدها الجماعة الدولية من قبل.

ويستخدم الإنترنت فى أغراض إرهابية فى ست فئات رئيسية تتداخل فى بعض الأحيان، وهى: الدعاية (بما يشمل التجنيد، والدفع باتجاه التطرف، والتحريض على الإرهاب)، والتمويل، والتدريب، والتخطيط (بما يشمل التخطيط عبر الاتصالات السرية والمعلومات المستمدة من مصادر علنية، والتنفيذ، والهجمات الإلكترونية[٢].

ويكمن الخطر الحقيقى للإرهاب الإلكترونى فى واقع سهولة استخدام هذا السلاح من جانب، واتساع نطاق ضرره وانتشار آثاره المدمرة إلى مدى قد يتجاوز الحدود الوطنية للدول من جانب آخر. ويعزى ذلك، فى واقع الأمر، إلى أمرين، هما:

- أولا: سهولة ولوج الإرهابيين إلى الإنترنت بمواقعه ومنصاته المختلفة من أى مكان، منزلا كان أو مقهى أو مكتبة عامة، أو حتى دور السينما.
- ثانيا: "الموصولية العالمية" ويقصد بها القدرة الفائقة لشبكة الإنترنت على تحقيق التواصل افتراضيا بين أناس فى مختلف أنحاء العالم، واستغلال التنظيمات والجماعات الإرهابية لهذه الإمكانات الاستثنائية للاتصال بأعضائها والموالين لها ولو كانت تفصل بينهم محيطات وقارات، وفى عجز بين من مؤسسات وآليات العدالة الجنائية التقليدية عن مساءلتهم وملاحقتهم قضائيًا[٣].

أولا: مفهوم الإرهاب الإلكترونى

يعد الإرهاب الإلكترونى أحد المصطلحات الحديثة نسبيا، التى ارتبطت بتطور تكنولوجيا المعلومات وتوسع استخدام شبكة الإنترنت عالميا. وقد بدأ الحديث عن الإرهاب الإلكترونى فى ثمانينيات القرن الماضى، ومنذ ذلك الحين، بدأت أبعاد مصطلح الإرهاب الإلكترونى تتطور وتتداخل مع غيرها من المصطلحات والمفاهيم التى ترتبط بالتطور التكنولوجى، وثورة المعلومات، وشبكة الإنترنت مثل: الحرب الإلكترونية، والجريمة الإلكترونية، والقرصنة الإلكترونية وغيرها من المفاهيم والمصطلحات. لكن يظل "الإرهاب الإلكترونى" رغم حداثته النسبية ينتمى، فى نهاية المطاف، إلى الظاهرة الأم والمفهوم العام وهو "الإرهاب" الذى يعد قديما قدم الإنسان نفسه، فهو ظاهرة عرفها الإنسان منذ قرون بعيدة". فالإرهاب كفعل ينتمى إلى استخدام العنف أو التهديد أو التلويح به من أجل بث الرعب والخوف فى نفوس الآخرين.

إن الإرهاب الإلكترونى هو الأكثر حداثة وأيضا تطورًا عند مقارنته بأشكال الإرهاب المعروفة الأخرى مثل الإرهاب التقليدى، الإرهاب النووى، الإرهاب الكيماوى، الإرهاب البيولوجى التى نلقى عليها الضوء فيما يلى:[٤]

١- **الإرهاب التقليدى:** وهو يقوم على استخدام العنف ونشر الخوف والذعر وإيقاع خسائر بشرية ومادية من أجل تحقيق أهداف سياسية. وقد شهد الإرهاب التقليدى تطورا كبيرا بفعل التطور التكنولوجى والعولمة وسرعة التنقل والاتصالات؛ لتسع آثاره التخريبية أكثر من أى وقت مضى.

٢- **الإرهاب النووى:** وهو يقوم على استخدام مواد أو أسلحة نووية من جانب جماعات إرهابية وجماعات الجريمة المنظمة.

٣- **الإرهاب الكيماوى:** وهو يقوم على استخدام المواد والغازات الكيماوية من جانب جماعات إرهابية، ويتسم الإرهاب الكيماوى بالبساطة والسهولة بسبب سهولة تصنيع المواد الكيماوية وسهولة استخدامها مقارنة مع الإرهاب النووى على سبيل المثال.

٤- **الإرهاب البيولوجى:** وهو يقوم على الاستخدام المتعمد للمواد والعوامل البيولوجية الخطرة مثل البكتيريا أو الفيروسات أو السموم، من جانب جماعات إرهابية كسلاح لإيقاع خسائر بشرية كبيرة، ومن الأمثلة على تلك المواد الجمرة الخبيثة، والسموم البكتيرية، وأمراض مثل الكوليرا والطاعون وغيرها.

٥- **الإرهاب الإلكترونى:** وهو أحدث أنواع الإرهاب ويقوم على استخدام شبكة الإنترنت وشبكات المعلومات وأجهزة الكمبيوتر وما يرتبط بها من تطورات تكنولوجية متسارعة من أجل التخويف والإرغام والتخريب لتحقيق أهداف سياسية. ويمثل الإرهاب الإلكترونى أحد مظاهر الدمج والربط بين استخدام كل من العنف لتحقيق أهداف سياسية، وتوظيف التكنولوجيا الحديثة فى مجالات الاتصال والمعلوماتية، والتى تعد من أبرز آليات العولمة[٥].

ويمكننا تعريف الإرهاب الإلكترونى بأنه: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وتنتج عنها آثار تخريبية مدمرة مكافئة لآثار الأفعال المادية للإرهاب"، وذلك وفقا لبارى كولين الذى ناقش ديناميكية الإرهاب هذه باعتبارها تجاوزًا للواقع المادى إلى العالم الافتراضى و"تقاطع والتقاء العالمين". وكولين هو أول من استخدم هذا المفهوم خلال عقد الثمانينيات من القرن العشرين[٦]. كما عرفه جيمس لويس لاحقا، بأنه: "استخدام أدوات شبكات الحاسوب فى تدمير أو تعطيل البنى التحتية الوطنية المهمة، مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين"[٧].

وقد ظهر مصطلح "الإرهاب الإلكترونى" أو ما يطلق عليه البعض "الإرهاب السيبرانى"، كما ذكرنا فى ثمانينيات القرن الماضى. كان المصطلح يشير إلى تلك الهجمات التى يستخدم فيها الكمبيوتر ضد اقتصاد وحكومة الولايات المتحدة، ثم اتسع مع بداية التسعينيات التى شهدت نموًا متزايدًا فى انتشار أدوات تكنولوجيا الاتصال والمعلومات دوليا. وظهرت العديد من الدراسات التى تناولت المخاطر المحتملة التى تواجه الدول الغربية خاصة الولايات المتحدة فى اعتمادها الكبير على التكنولوجيا وأجهزة الكمبيوتر[٨].

وأول من استخدم المصطلح هو بارى كولين الباحث فى معهد الاستخبارات والأمن فى جامعة كاليفورنيا. وقد أطلق كولين مصطلح الإرهاب باعتباره مصطلحا جديدا، يعبر عن ظاهرة حديثة، فى ذلك الوقت، تربط بين الفضاء الإلكترونى Cyberspace، والإرهاب Terrorism. وقد تطور المصطلح وازداد الاهتمام به خلال سنوات التسعينيات من القرن الماضى، عندما بدأ استخدام الإنترنت فى الانتشار من جانب الحكومات والمؤسسات والأفراد؛ حيث بدأ ينتشر تدريجيا فى معظم التعاملات حول العالم، باعتباره الأسرع والأقل فى التكلفة والوقت والجهد. لكن على الجانب الآخر، ومع اتساع استخدام شبكة الإنترنت، اتسعت وانتشرت المخاطر والتهديدات الإلكترونية المرتبطة به.

وبناء على ما سبق يمكن أن ننتهى إلى عدة صفات للإرهاب الإلكترونى: باعتباره نشاطًا أو فعلاً هجوميًا إجراميًا متعمدًا أو مقصودًا؛ يقوم به فرد أو جماعة أو دولة؛ عمل يتم لأغراض سياسية أو عرقية أو دينية؛ يستخدم وسائل التكنولوجيا الحديثة؛ يوقع أضرارا بالممتلكات العامة أو الخاصة؛ وأخيرا يهدف إلى إدخال الرعب أو الخوف والفزع لتحقيق غايات إرهابية[٩].

وتجدر الإشارة إلى مصطلحات عدة يستخدمها المتخصصون والأكاديميون للتعبير عن استخدام التنظيمات الجهادية والجماعات الإرهابية للإنترنت لتحقيق أغراضها الإرهابية– وهو ما سيتم التطرق إليه لاحقا فى الجزء الأخير من الدراسة، ومنها "الإرهاب الرقمى" أو "الإرهاب الافتراضى" أو الإرهاب الشبكى" جنبا إلى جنب مع الاستخدام الشائع "الإرهاب الإلكترونى"، وذلك للإشارة إلى ظاهرة واحدة: وهى امتلاك التنظيمات والجماعات الإرهابية لأدوات المعرفة التقنية الحديثة واستغلالها لاختراق الفضاء الإلكترونى وتحقيق أهدافها السياسية أو الاقتصادية أو الاجتماعية أو الدينية. ويمكن اعتبار اختلاف التسمية لذات الظاهرة بسبب تطورها بوتيرة سريعة من جانب، فضلا عن اختلاف وجهات النظر إليها إعلاميا وأمنيا وقانونيا وسياسيا ونفسيا واجتماعيا من جانب آخر[١٠].

إن الإرهاب الإلكترونى، بهذا المعنى، هو ظاهرة عالمية تشكل إحدى صور الجرائم الإلكترونية العابرة للحدود الوطنية، تمس على نحو مباشر أمن الدول، حيث تستخدم التنظيمات والجماعات الإرهابية الإنترنت لاختراق الحواسيب الآلية للمؤسسات والمرافق الحيوية العسكرية والاقتصادية والثقافية للدولة/ للدول المستهدفة، كالبنوك والبورصات العالمية والمطارات والموانئ وغيرها، والاطلاع على بياناتها المخزونة والتجسس عليها وتدميرها وإرسال رسائل تدميرية للحكومة لقبول مطالبها، على نحو يهدد أمن الدول العسكرى والاقتصادى.

يتسم الإرهاب الإلكترونى، بمجموعة من الخصائص الرئيسية التى تميزه عن مفهوم الإرهاب فى صورته التقليدية. ونشير إلى أهمها فيما يلى:

١- **جرائم ناعمة:** بمعنى العزوف عن استخدام العنف فى معناه التقليدى الحموى، والاستعاضة عنه بأدوات التكنولوجيا الحديثة، أو ما يمكن تسميته soft violence، لتحقيق لدوافع الإرهاب.

٢- **يسر الاتصال بين الجناة:** يسر الاتصال بين أفراد التنظيم الإرهابى الواحد، دونما حاجة إلى الاجتماع، وسهولة التنسيق عن بعد فيما بينهم لتنفيذ الجرائم الإرهابية.

٣- **المهارة التقنية:** توافر قدر من المهارة والخبرة بتكنولوجيا المعلومات لدى الإرهابيين، أفراد، كانوا أو جماعات، تمكنهم من توظيف شبكة الإنترنت لخدمة أغراضهم الإرهابية على كافة المستويات، تخطيطًا ودعاية وتمويلاً وتدريبا وتنفيذا(١١).

٤- **سهولة التخفى:** بمعنى تنوع أساليب عمل الجماعات والتنظيمات الإرهابية وقدرتها الفائقة على التخفى من خلال إنشاء الحسابات والمواقع الوهمية وتجديدها من حين إلى آخر، دون أن يكون بمقدور الأجهزة الأمنية تعقبها أو الوصول إليها بسهولة.

٥- **قوة التأثير:** سهولة تواصل أفراد الجماعات الإرهابية مع الجمهور، وبخاصة فئة الشباب، عبر صفحات المنتديات وغرف الدردشة، وبذل الجهود للتأثير عليهم وإقناعهم بشرعية أهدافها وترويج التبريرات بشأن أعمالها وأنشطتها، الأمر الذى ساعد على اتساع نطاق عمليات التجنيد والتعبئة، والتى ضمت فئات من الجنسين، فى الآونة المعاصرة، بالمقارنة بالإرهاب التقليدى.

٦- **فداحة الخسائر:** فداحة الخسائر الناتجة عن الإرهاب الإلكترونى والتى تكاد تكون أضعاف الخسائر التى تحدثها الجرائم الإرهابية التقليدية، سواء من حيث الأرواح أو الممتلكات، لا سيما فى الدول التى تعتمد بشكل كبير على تكنولوجيا المعلومات(١٢).

٧- **الطبيعة العابرة للحدود:** يتميز الإرهاب الإلكترونى، كذلك، بالطابع العابر للحدود، ليس فقط من حيث آثارهَا وأضرارهَا، بل أيضا، من حيث مراحل إعداده وتنفيذه، فقد يتم التخطيط للجريمة الإرهابية بدولة، ويتم جمع التمويل اللازم لتنفيذهـــا ورصده بدولـــة أخـــرى، ويتم التنفيذ بدولـــة ثالثـــة. ويختلف الإرهاب الإلكترونى بهذه السمة، عن الجرائم الإلكترونية الأخرى والتى عادة ما تحدث فى نطاق محلى، كما ينتمـــى الإرهـــاب الإلكترونى، فى المقابـــل، على أثـــر هذه الخاصية إلى طائفة الجرائم المنظمة عبر الوطنية(١٣).

٨- **تعدد الأغراض وتنوعها:** وإضافة، لم يعد هدف الإرهاب الإلكترونى مقصورا على تحقيق مآرب سياسية وحسب، مثلما هو معتاد بالنسبة للإرهاب التقليدى، وإنما أضحت له أغراض أخرى متعددة، وربما قد يكون فى مقدمتها الأغراض الاقتصادية أو الانتقامية أو الدينية.

٩- **جرائم عمدية:** تتسم جرائم الإرهاب الإلكترونى، كذلك، بكونها جرائم عمدية، ترتكب بعد تدبير وتخطيط مسبقين، ولا تحدث بشكل عشوائى عفوى أو على سبيل الخطأ(١٤).

١٠- **صعوبة إثباتها لسرعة غياب الدليل:** إن المعلومات التى يحملها الإنترنت تكون فى شكل رموز مخزنة على وسائط تخزين ممغنطة ولا تقرأ إلا بواسطة الحاسب الآلى، وهو ما يجعل الدليل الكتابى أو المقروء، أمرًا يصعب بقاؤه أو إثباته لأن الجانى مرتكب هذه الجريمة لا يترك وراءه أى أثر مادى خارجى ملموس يمكن فحصه، الأمر الذى يجعل من العسير على المحققين الجريمة ومعرفة مرتكبيها، بخلاف الجريمة التقليدية التى عادة ما تترك وراءها دليلا ماديًا أو شهادة شهود أو غيرها من أدلة الإثبات.

ثانيا: أسباب تصاعد انتشار ظاهرة الإرهاب الإلكترونى

أما فيما يتعلق بدوافع جرائم الإرهاب الإلكترونى، فهى لا تختلف، كأصل عام، عن دوافع ارتكاب الجرائم الإرهابية عموما. غير أن ما يعنينا فى هذا الخصوص، هو استعراض أسباب تصاعد انتشار جرائم الإرهاب الإلكترونى، وتحول الجماعات والتنظيمات الإرهابية نحو استخدام ثورة الاتصالات وتكنولوجيا المعلومات فى ارتكاب جرائمها المختلفة. ويعزى ذلك، فى حقيقة الأمر، إلى جملة من الاعتبارات نشير إلى أهمها على النحو التالى:

١- **أسباب تقنية:** تتعلق بضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للاختراق من خلال الثغرات المتاحة بها. والسبب فى ذلك، هو أن شبكات المعلومات مصممة فى الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها، مما يمكن أفراد الجماعات والتنظيمات الإرهابية من التسلل إلى البنية التحتية للمؤسسات والمرافق الحيوية للدولة المستهدفة وتخريبها بسهولة ويسر، إضافة إلى صعوبة التعرف على الهوية الإلكترونية للإرهابى، حيث يقوم بشن هجومه بهوية وشخصية وهمية يتستر ورائها للتخفى عن أعين الأجهزة الأمنية، بل ويغيرها من حين إلى آخر[١٥].

٢- **أسباب اقتصادية:** تتعلق برخص التكلفة ويسر الاستخدام، فيكفى للقيام بهجوم إلكترونى توفر حاسوب متطور متصل بشبكة معلوماتية متطورة فقط لا غير، ولا يستغرق تنفيذ هذا الهجوم، فى أغلب الأحيان، سوى ثوان معدودة لإصدار الأمر وتفعيله.

٣- **أسباب قانونية وتنظيمية:** تتصل بضعف البنية التشريعية، على المستويين الوطنى والدولى، التى تكفل المواجهة الفعالة لجرائم الإرهاب الإلكترونى وفى إطار من الرقابة على الاتصالات عبر الإنترنت. بالإضافة إلى نقص خبرة

بعض الأجهزة الأمنية وجهات التحقيق والملاحقة المعنية فى مجال التعامل مع مثل هذه الجرائم التى لم تشهدها الجماعة الدولية من قبل.

٤- **صعوبة اكتشاف وإثبات الجريمة الإرهابية:** نظرًا لسرعة غياب الدليل الرقمى وسهولة إتلافه وتدميره، علاوة على صعوبة السيطرة على المعلومات المتبادلة والمنشورة عبر الإنترنت، وكذا صعوبة فرض الرقابة على مجمل الاتصالات التى تتم من خلال الشبكة، الأمر الذى وفر للإرهابيين ملاذات آمنة لمباشرة أنشطتهم الإرهابية عبر الفضاء الإلكترونى، دون خوف أو قلق من أن ترصدهم الأجهزة الأمنية المعنية(١٦).

٥- **زيادة الاعتماد على تكنولوجيا المعلومات** فى مختلف ميادين الحياة المعاصرة، نظرًا لكفاءتها العالية فى معالجة البيانات، فأصبحت القاعدة التى يرتكز عليها عمل العديد من المرافق الحيوية للدولة مثل المستشفيات والمطارات والبنوك وغيرها. الأمر الذى جعلها أهداف جذابة وسهلة للإرهاب الإلكترونى، بالنظر إلى ما يخلقه الخلل بنظم الحواسيب الآلية هذه من فوضى عارمة، فباتت الجماعات والتنظيمات الإرهابية تستخدمه بسهولة ويسر لتحقيق دوافعها دون اللجوء المباشر إلى القوة ولو باستخدام رصاصة واحدة. ولهذه المخاطر وجاهتها فى نظر بعض الدول حتى أن المخابرات العامة الألمانية قد أبدت مخاوفها من قيام الجماعات الإرهابية المتطرفة باعتداءات على شبكات الحاسبات الغربية باستخدام الإنترنت(١٧).

ثالثا: مخاطر الإرهاب الإلكترونى وتهديداته

ينطوى الإرهاب الإلكترونى على تهديد جديد يجب أن يؤخذ بجدية فائقة. ذلك أنه فضلا عن تهديده للأنظمة المعلوماتية لمؤسسات الدولة المستهدفة، فإنه يعرض، كذلك، حياة الناس وسلامتهم للخطر بشكل غير مباشر، وتتبين هذه الخطورة، إذا علمنا أن التنظيمات والجماعات الإرهابية يمكنها من خلال الضغط على زر واحد

فقط بلوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق تلك التى يمكن أن ينتجها استخدام المتفجرات، الأمر الذى ينتج عنه تعطيل المحركات الرئيسية للدولة/ للدول المستهدفة والإضرار بمواطنيها وأمنها القومى.

وفى هذا السياق، عبر ستيف دوربين الرئيس التنفيذى لمنتدى أمن المعلومات عن أنه: "خلال السنتين القادمتين، سيتعين على رواد الأعمال اتخاذ قرارات معقدة حيال حماية معلوماتهم وأنظمتهم الحيوية. كما أن المنظمات التى ستدرك هذه البيئة المعقدة سريعة التغيير، هى فقط التى سيمكنها البقاء ثابتة ومستقرة ضد انقضاض الهجمات الإلكترونية القوية المستمرة. فخلال السنوات القادمة، ستهتز أسس العالم الرقمى المعاصر بشدة. سوف يضاف المهاجمون من ذوى الموهبة والعزم إلى تلك التغيرات الجذرية فى طريقة إنجاز المنظمات لأعمالها ... ليشكلا معا تهديدا حتى لأعتى المؤسسات، ولن تصمد منها إلا ذات الاستعدادات القوية[١٨].

وتشمل صور مخاطر الإرهاب الإلكترونى على أمن الدول ومواطنيها، على سبيل المثال، ما يلى[١٩]:

١- التسلل إلى الأنظمة الأمنية للدولة وشلها وتعطيل أنظمة الاتصال بين القيادة والوحدات المركزية أو بين الأجهزة الحساسة بالدولة وبعضها البعض.

٢- اختراق المنظومة الخاصة للأسلحة الاستراتيجية ونظم الدفاع الجوى، وفك شفرات التحكم بتشغيل منصات إطلاق الصواريخ والأسلحة النووية وغيرها من الأسلحة الفتاكة.

٣- استهداف محطات توليد الطاقة والماء، وشل نظم الحواسيب والشبكات المعلوماتية التى تنهض بمهام التحكم فى شبكات توزيع المياه والطاقة الكهربائية بالدولة المستهدفة، الأمر الذى ينتج عنه تعطيل العديد من المرافق الحيوية، وشل الحركة فى عموم البلاد.

٤- تعطيل أنظمة التحكم بخطوط الملاحة الجوية والبحرية والبرية، وإحداث خلل ببرامج هبوط الطائرات وإقلاعها، أو إيقاع تصادم بين القطارات، أو السطو على

السفن والناقلات والغواصات البحرية، وما يستتبعه ذلك من عواقب وخسائر وخيمة على المستويين البشرى والمادى.

٥- اختراق النظام المصرفى للدولة والبورصة للاستيلاء على الأموال المتاحة بها لتغطية التمويل اللازم للأعمال الإرهابية.

٦- إحداث خلل واسع فى نظم الشبكات التى تتحكم بسريان أنشطة المصارف وأسواق المال العالمية، وإشاعة الفوضى بمنظومة صفقات التجارة الدولية، على نحو تتعطل معه الحياة الاقتصادية بالدولة المستهدفة تعطلا شبه تامة.

٧- مهاجمة شبكات المعلومات الطبية واختراقها والتلاعب بها، لحقن المرضى بأدوية أو علاجات مميتة مثلاً أو التلاعب فى نسب الأدوية التى يتلقونها على نحو يوقع خسائر فى أرواح المدنيين.

٨- شل محطات الطاقة الكبرى والهجوم الإلكترونى على مصانع الكيماويات والأدوية وغيرها من السلع الحيوية والتلاعب بخطوط تشغيلها ونسبها للإضرار بالصحة العامة(٢٠).

وقد يكون من المفيد، ونحن بمعرض الحديث عن مخاطر الإرهاب الإلكترونى، أن نلقى الضوء على بعض الجرائم الإرهابية التى حدثت بمختلف أنحاء العالم باستخدام الإنترنت ونظم المعلومات، وذلك لاستعراضه آثارها البالغة على الدول والمجتمعات التى منيت بها.

أ- تسريبات ما عرف باسم " إعصار ويكيليكس" فى عام ٢٠١٠، إذ تم استغلال شبكة الإنترنت العالمية فى تسريب وثائق تحوى معلومات سرية للغاية متداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم(٢١).

ب- الهجوم الإلكترونى على حلف الناتو عام ١٩٩٩ أثناء الحرب على كوسوفا، وقصف أجهزة الكمبيوتر الخاصة بمؤسسات الحلف بعدد لا يحصى من رسائل

البريد الإلكترونى والفيروسات، مما تسبب فى بطء مواقع الحلف وتعطيلها لعدة ساعات على نحو هدد الأمن القومى للدول الأعضاء[٢٢].

ج- كما أعلن الكرملن الروسى أن موقع الرئاسة الروسية قد تعرض لهجوم عنيف من قبل الإرهابيين أدى إلى تعطله، كما عطلوا العمل بموقع البنك المركزى الروسى.

د-ومن هذه الأمثلة أيضا، ما حدث فى إيطاليا عام ١٩٩٨، حينما تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء دمرت فيه مراكز المعلومات الخاصة بها.

هـ- أدى انتشار فيروس الحاسوب "I love you" فى عام ٢٠٠٠، إلى إتلاف معلومات قدرت قيمتها بنحو ١٠ مليارات دولار أمريكى، وفى العام ٢٠٠٣، أشاع فيروس "بلاستر" الدمار فى نصف مليون جهاز من أجهزة الحاسوب. وقدر "مجلس أوروبا فى الاتفاقية الدولية لمكافحة الإجرام عبر الإنترنت" كلفة إصلاح الأضرار التى تسببها فيروسات المعلوماتية بنحو ١٢ مليار دولار أمريكى سنويًا.

و-كما مُنيت عدد من المصارف العملاقة بخسائر اقتصادية فادحة نتيجة لاختراق حسابات العملاء وإجراء تحويلات مالية ضخمة منها لحسابهم، مستغلين الثغرات بالنظام الحاسوبى لهذه المصارف وفقا لدراسات مؤسسةB2B International وشركة كاسبرسكي لاب الرائدة فى مجال الأمن المعلوماتى.

ز- إضافة إلى ما تقدم، واجهت شركة سونى Sony العملاقة فى نوفمبر عام ٢٠١٤ واحدا من أكبر انتهاكات الخصوصية فى العالم، حيث قامت مجموعة من القرصنة أو الهاكرز التابعة لجماعة حراس السلام Guardians of Peace، التابعة لكوريا الشمالية بغزو إلكترونى هائل على أجهزة الكمبيوتر الخاصة بالشركة والمئات من خوادمها بواسطة البرمجيات الخبيثة التى اخترعتها تلك المجموعة، مما كلف الشركة نحو ١٠٠ مليون دولار أمريكى لإصلاح الأمر[٢٣].

وهكذا يستخدم الإرهاب الإلكترونى كنمط من أنماط الاحتجاج ضد بعض الدول القومية بما تحمله من هويات أو قيم يرى منفذو الهجمات الإرهابية الإلكترونية ضرورة مهاجمتها. ومن ثم فالإرهابيون الإلكترونيون يحتاجون إلى دوافع مهمة قوية (كعناصر اجتماعية أو سياسية أو ثقافية أو دينية مختلفة تسهل توظيف القوة البشرية الأساسية من أجل نشر رسالتهم وأيدلوجيتهم للجماهير، والقدرة على الوقوف، والنهوض ضد الدولة ذات التنظيم الجيد والقوى.

وقد رصدت بعض الدراسات الجوانب الأكثر أهمية لمخاطر الإرهاب الإلكترونى على أمن الدول القومية، وهى، التهديد السياسى/الأمنى، والتهديد الاجتماعى، والتهديد الاقتصادى.

رابعا:استغلال الجماعات المتطرفة للإرهاب الإلكترونى

هناك حالات محدودة قد يستخدم الإرهاب الإلكترونى بين الجماعات المتطرفة بعضها البعض، وهو ما يتجلى إبان المنافسة بين الجماعات الإرهابية المتشابهة فى أسسها العقائدية أو الفكرية مثل تنظيم القاعدة وتنظيم داعش، إذ يمكن القول إن داعش ترى فى تنظيم القاعدة عدوا له رغم أن داعش كان فى الماضى جزءا من القاعدة واستلهم العديد من استراتيجياتهم التى يستخدمونها اليوم. ومن ثم فلدى داعش هدف أو هاجس للتفوق على القاعدة، ويرى كثيرون أنه نجح فى تلك المهمة لاسيما وأنه تمكن من تحقيق هدف إنشاء "الخلافة" الأمر الذى يساعد داعش فى اجتذاب المانحين والمجندين على حساب القاعدة[٢٤].

وتتبدى فى هذا السياق ملامح الحلقة المفرغة للمنافسة بين التنظيمات المتطرفة حيث يتقدم تنظيم إرهابى فيما يتراجع آخر. ففى الحين الذى تدهورت فيه قدرات داعش التنظيمية والعسكرية بشكل كبير نتيجة الجهود الدولية للتخلص من وجوده الفعلى فى العراق وسوريا، يسعى تنظيم القاعدة للنهوض من جديد واستقطاب المتطرفين من مختلف أنحاء العالم من أجل ضمهم للتنظيم بقالبه الجديد ومن ثم

يعاود نشاطه وبقوة فى الفضاء الإلكترونى؛ حيث تظهر مساعيه لاسترداد نفوذه عبر الترويج وقتذاك لنجل مؤسس التنظيم حمزة بن لادن الذى يمتلك جاذبية ونفوذا وشعبية قد تفوق تلك التى يمتلكها زعيم القاعدة أيمن الظواهرى الذى خفت وهج التنظيم أثناء زعامته، ورغم تقلص قدرات داعش على الأرض ما زال بإمكانه إيجاد معاقل أخرى أو تحويل عملياته لتصبح سيطرة على العمليات الإرهابية عن بعد، مثل مساعية إنشاء خلافة إلكترونية(٢٥).

فى هذا السياق يمكن القول إن حركة الإرهاب الإلكترونى فى صبغته الجهادية ستشهد فى المستقبل المنظور حالة من التنافس بين قطبين متمايزين ومتنافسين، لا يقف أى منهما على شفا الانكسار، ولا من المحتمل أن يقبل أحدهما بشرعية الطرف الآخر فى السنوات القادمة، وهذا من شأنه الحفاظ على الانقسام بينهما. فى هذا السياق يتوقع أن يواصل تنظيم داعش تبنى استراتيجية إنشاء ملاذ آمن افتراضى– "الخلافة الافتراضية"– مع التأكيد على استمراريتها، وتنسيق الهجمات الخارجية. تمثل هذه الخلافة الافتراضية مجتمع أنصار داعش، يقودهم خليفة (أبو بكر البغدادى وقتذاك)، ولكن على الفضاء السيبرانى، مع الاستمرار فى بث دعاياتها ممهورة بشعار "الخلافة الإسلامية". أما من جهة القاعدة، فستواصل محاولات التموضع فى صورة الجماعة الأكثر اعتدالا، وكسب تعاطف الجمهور فى مناطق نشاط التنظيم. كما من المرجح أن تركز شبكة القاعدة على تجنيد أعضاء "داعش" المحبطين، بدلا من محاولة الوصول إلى تقارب معها(٢٦).

وتجدر الإشارة إلى أن القاعدة هى أولى التنظيمات الإرهابية التى استخدمت الإنترنت فى سبيل الدعاية والتجنيد، ولكن قلّ هذا الاستخدام حاليا لسببين الأول هو مؤشر على اختلاف مفهوم الجهاد داخل التنظيم وبالتالى انعكاس هذا الاختلاف على التواجد الرقمى للتنظيم. الثانى هو أن القاعدة لم تتمكن من التنافس على الإنترنت مع الأجيال الشابة من الجهاديين، وبالتالى انخفضت أهمية وجودها على الإنترنت بشكل كبير.

إن متابعة ممارسات الفاعلين المختلفين على صعيد الفضاء الافتراضى توضح أن استخدام ميكانيزمات الإرهاب الإلكترونى غالبا ما تهدف إلى تحقيق أحد أو بعض أو ربما كل الأغراض التالية:

١- تخويف وإرهاب الأعداء

كما سبقت الإشارة يعد عنصر الخوف من الأركان المفصلية للإرهاب بأنواعه المختلفة ومنها الإرهاب الإلكترونى، إذ يوجه ممارسو هذا النمط من الهجمات الإرهابية قسما واضحا من جهودهم وخطاباتهم إلى أعدائهم أو خصومهم المفترضين، لاسيما أجهزة الدول المستهدفة ومؤسساتها، وذلك بهدف إضعاف مواقف تلك الكيانات والتأثير على هيبتها، وإظهارها بمظهر العاجز فى مقابل قوتها.

كما تستهدف الجمهور أو الرأى العام فى تلك الدول بغرض بث الرعب والضغط على جمهور معين عبر تقديم صورته المخيفة عن طرق أسلوب الترهيب، بعبارة أوضح يستخدم الإرهابيون الحرب النفسية ضد الجمهور، من خلال المعلومات المغلوطة والصور المزعجة التى تهدف إلى زرع الخوف. فعلى سبيل المثال يرى كثيرون أن تنظيم القاعدة زعم على مواقعه على الإنترنت أن هجمات الحادى عشر من سبتمبر تسببت فى أضرار مادية ونفسية تفوق كثيرا تلك التى تسبب بها فى الحقيقة [٢٧].

٢- نشر الفكر وتجنيد الأنصار

غالبا ما يسعى ممارسو الإرهاب الإلكترونى المؤدلجون إلى الترويج لأفكارهم ونشرها على قطاع واسع عبر الفضاء الافتراضى. وتعد وسائل التواصل الاجتماعى من الوسائل المهمة للتنظيمات المسلحة لنشر أفكارها وكسب متعاطفين وأتباع جدد للانضمام لصفوف المقاتلين فى تلك الجماعات، ومن ثم، تولى تلك الجماعات اهتماما متزايدا لحساباتها على مواقع التواصل الاجتماعى، وغيرها من الوسائط والمنصات الإعلامية الشبكية، وهى غالبا ما تستهدف فئتين من المتلقين، هما

المتعاطفون مع الفكر الجهادى وغالبيتهم من الشباب لاستمرار الحصول على دعمهم، والرأى العام المحايد من أجل تأكيد نفوذ التنظيمات الجهادية فى المجتمع بغرض الحشد والتأييد[٢٨].

غالبا ما يهدف ممارسو الإرهاب الإلكترونى فى هذا السياق إلى خلق كتلة من الجمهور ينصهر معهم فى مواقفهم واتجاهاتهم وسلوكهم، ومن ثم تنميط وعى الأفراد وقولبته ليتوافق مع النظام القيمى الخاص بهم وممارساتهم ورؤيتهم للصراع، من خلال اختـراق المنظومة القيمية والثقافيـة وتطبيع مرجعيتهم الفكريـة والعقائديـة مع المستخدمين، وإنتاج خطاب القوة والسلطة والهيمنة على المجال العام الإلكترونى وتحويل شبكات التواصل الاجتماعى إلى عنوان للهوية الإلكترونية. فى هذا السياق يمكن القول إن تنظيم داعش نجح فى تحويل مواقع التواصل الاجتماعى إلى عنوان لهويته الإلكترونية ووسيلة للاختراق الأيديولوجى والقيمي الذى يستهدف بالإضافة إلى اختراق المؤسسات السيادية، إلى اختراق المنظومة القيمية والثقافية للأفراد ونشر النسق القيمي للتنظيم واستمالة المستخدمين إلى صفوفه وهو ما تسمح به مواقع التواصل الاجتماعى انطلاقًا من فضائها المفتوح الذى يتميز بالتفاعلية والمشاركة ويعطى شعورا بالحرية والقوة والسلطة.

وتشير بعض التقارير إلى أن التنظيم له ما يقرب من ٩٠ ألف صفحة باللغة العربية على موقع التواصل الاجتماعى الفيسبوك و٤٠ ألف بلغات أخرى، إضافة إلى موقعه الذى دشنه التنظيم بسبع لغات[٢٩].

كما كان ينشط تنظيم داعش فى العراق وسوريا، اعتمادا على تلك الوسائل الاتصالية لدعم أهداف التنظيم، والتى يتم الترويج لها من خلال الإعلام المركزي للتنظيم، ومنها "مركز الفجر للإعلام"، و"مؤسسة الفرقان الإعلامية"، والتى تعد وسيلة أساسية وشبه وحيدة فى الترويج والنشر. وشهدت بعض الصفحات الإلكترونية ما أسماه البعض "البيعة الافتراضية" لزعيم تنظيم داعش من جانب آلاف الجهاديين، أثر إعلان الناطق باسم التنظيم عن تأسيس "دولة الخلافة"، فى المناطق التى يوجد فيها

التنظيم فى العراق وسوريا، وظهرت صفحات على شبكات التواصل الاجتماعى من بينها "بيعة أمير المؤمنين أبوبكر البغدادى"، وإعلان الولاء الشرعى للأمير أبوبكر البغدادى" وغيرها، مما ساهم فى انتشار التنظيم وتوسيع دائرة مؤيديه(٣٠).

يرى الخبراء أن عملية استقطاب وتجنيد أتباع جدد عبر الفضاء الافتراضى، تتم عبر ثلاث مراحل تتعلق الأولى بالتأثير الوجدانى فى الشخص المستهدف من خلال إثارة العاطفة والنعرة والغيرة الدينية بحجة الدفاع عن القيم المقدسة الدينية أو البحث عن عالم مثالى كفكرة "الخلافة" أو "المدينة الفاضلة"، وفى تلك المرحلة يتم توظيف النصوص الدينية الأصلية بشكل واضح. أما المرحلة الثانية، فيظهر فيها بشكل جلى دور شبكات التواصل الاجتماعى فى نقل المعلومات والبيانات التى تعبر فقط عن وجهة نظر الجماعات القائمة بالاستقطاب. المرحلة الثالثة هى العمل على تحويل الفكر إلى سلوك عن طريق التغيير السلوكى للشخص المستهدف لتحويله من مجرد متعاطف إلى فاعل عبر إقناعه بالمشاركة في أرض القتال الفعلى، أو القيام بعمليات انتحارية بعد عملية التعرض لغسيل المخ تحت دعوى رفعة الجماعة والانتقال إلى العالم الأفضل(٣١).

وتركز غالبية الجماعات الفاعلة فى هذا السياق على مجموعتين من الأشخاص المستهدفين هما النشء والنساء. فغالبا ما يهتم ممارسو الإرهاب الإلكترونى باستقطاب ولفت انتباه الأشخاص بدءا من سن الخامسة عشر، ليكونوا الجيل الجديد فى تنظيماتهم، من خلال عرض أشرطة فيديو عن تاريخ هذه التنظيمات، وفيديوهات تحمل عبارات حماسية مثل "أنت تشعر بأنك تريد أن تحمل سلاحا، والكفاح، وقتل المحتلين"، وتعمل على إقناعهم بأن الجنة تنتظر الشهداء الجدد.

وفى سبيل ذلك يخلق الإرهابيون واقعا افتراضيا جديدا من خلال وسائل التواصل الاجتماعى التى يتداولون من خلالها ما يقومون بإنتاجه من مواد جذابة لفئة الشباب تحديدًا، مثل مقاطع فيديو على YouTube، وموسيقى البوب والراب والرسوم المتحركة، وكلها تهدف إلى ترويج ونشر أفكار تلك الجماعات. أى إن الإرهابيين

يقومون بتطوير رواية وصورة وعلامة تجارية يمكنهم تحريرها وتجميلها من خلال وسائل الإعلام الاجتماعية[٣٢].

وتجدر الإشارة فى هذا السياق إلى التقارير الصادرة عن جمعية آفاق للأمن الداخلى لتونس، والتى تشير إلى أن المواقع الإلكترونية ذات التوجه المتطرف والإرهابى تستقطب نحو ألف شاب فى السنة بما يعادل٣ شبان يوميا، وهو رقم مرتفع يعكس خطورة الظاهرة التى تزداد حدتها، وهم يمثلون نحو٤٠٪ من مجموع الشباب المستقطب وهم من الطلبة والتلاميذ المتفوقين الذين تتراوح أعمارهم بين ١٧ و٢٨ سنة والذين يدرسون الاختصاصات العلمية كالطب الفيزياء والكيمياء حيث تقوم هذه الجماعات باستثمار مهاراتهم العلمية لأغراض تخريبية[٣٣].

أما فيما يخص تجنيد النساء، فتعد تجربة فرع القاعدة فى السعودية جديرة بالدراسة، حيث عمل يوسف العييرى على تكثيف وجود التنظيم على الإنترنت كما عمل عبد العزيز المقرن بعد مقتل العييري على تأسيس موقع جهادى مخصص للمرأة سمى موقع "الخنساء"، وقد عمل الموقع على تجنيد النساء للانضمام لتنظيم القاعدة من خلال شبكة الإنترنت، وكان يشرف عليه نساء يؤمن بالسلفية الجهادية، وقد نشطت النساء الجهاديات مؤخرا فى العالم الافتراضى، وتعد قضية" مليكة العروض" التى مثلت أمام المحكمة فى بلجيكا نموذجا للناشطات الجهاديات على الشبكة العنكبوتية، وثمرة لجهود التنظيم على دمج المرأة فى المشروع الجهادى فى العالم الواقعى وصناعة كتائب الاستشهاديات اللواتى نفذن عمليات انتحارية فى مناطق مختلفة.

٣-التمويل

يمكن للإرهابيين الإلكترونيين استغلال الفضاء الشبكى فى الحصول على التمويلات اللازمة لدعم نشاطات جماعاتهم وذلك من خلال عدد من الصور. فمن ناحية أولى، يمكن للإرهابيين جمع الأموال عبر دعوة الأنصار والمتعاطفين مع أفكارهم لمساندتهم

ماديا، ويتضح ذلك فى حالة الجماعات الإسلامية المتطرفة التى توظف بعض الفتاوى والآراء الفقهية التى تبيح التضحية بالأموال والأنفس، وهو ما يتيح للإرهابيين الحصول على تبرعات تصل لحسابات مجهولة أو بالأحرى مجهلة. وفى هذا السياق قد تخدم الجمعيات الخيرية والمنظمات غير الحكومية للقيام بأنشطة مالية غير مشروعة لتمويل الأنشطة الإرهابية. وقد زاد الاعتماد على الإنترنت فى هذه الأنشطة مؤخرا، بيد أنه فى الماضى كان الإرهابيون يعتمدون على وسائل أخرى. فعلى سبيل المثال كان تنظيم القاعدة يقوم بإرسال تسجيلات فيديو للهجمات التى يقوم بها على أقراص مدمجة إلى الجهات المانحة، كشكل من أشكال الإعلان عن التبرعات المستقبلية وإظهار أن الأموال المخصصة قد تم استخدامها بنجاح. أما اليوم فإن الإنترنت ووسائل الإعلام الاجتماعية يمكنها القيام بتلك الوظيفة بل وتستطيع الوصول إلى نطاق أوسع من المؤيدين[٣٤].

يستخدم تويتر على نطاق واسع لجمع التبرعات للجهاد. على سبيل المثال في ٢٦ فبراير ٢٠١٤ أطلق الشيخ عبد الله المحيسنى، وهو رجل دين سعودى انضم إلى المجاهدين فى سوريا، حملة لجمع التبرعات على تويتر لشراء ذخيرة لقتال "الألوية الإسلامية" فى سوريا. ووفقا لتغريدات مختلفة من الحساب، تم التبرع بأكثر من ٢٦٠٠٠ ريال سعودى. كما كانت هناك حملة سابقة تحمل عنوان "المشاركة فى الجهاد مع أموالك". وفى إطار حملات التبرعات على تويتر يتم توزيع صور تبرعات مثل قطع من الذهب والسيارات الفاخرة إلى جانب صور الأسلحة التى تم شراؤها من عائداتها[٣٥].

من ناحية ثانية، يستخدم ممارسو الإرهاب الإلكترونى المنصات الشبكية لتسهيل تبادل التحويلات المالية فيما بينهم، فى ظل سهولة استخدام تلك المواقع لتحويل الأموال مع عدم إمكانية التحقق من هوية متلقى تلك التحويلات المالية.

كما تتحدث الكثير من التقارير عن استخدام الإرهابيين الإلكترونيين للتجارة عبر وسائل الإعلام الاجتماعية، فعلى سبيل المثال يتم استخدام الفيسبوك من قبل

الجماعات الإرهابية النشطة لشراء وبيع الأسلحة الثقيلة والبنادق والذخيرة. ومن بين الأسلحة التى تم بيعها بنجاح عبر الإنترنت أنظمة الدفاع الجوى المحمولة وتحديدا بعض أنواع قاذفات الصواريخ القادرة على إسقاط الطائرات المدنية والعسكرية. الذى تم بيعه مقابل ٦٧.٠٠٠ دولار أمريكى على الصفحة المسماة "سوق الأسلحة الأولى فى ريف إدلب بسوريا، وعلى الصفحة ذاتها بيعت قاذفة قنابل يدوية من نوع - AGS 17- Era السوفييتى مقابل ٣٨٠٠ دولار أمريكى، فضلا عن كاميرات حرارية" تستخدم للصيد فى الليل(٣٦).

من ناحية ثالثة، أضحى للإرهابيين الإلكترونيين اهتمام خاص بالعملات الافتراضية وخاصة العملات المشفرة التى يكون المتعاملون بها شبه مجهولين مثل بيتكوين وزكاش ومونيرو وإثيريوم، وهى عملات قادرة على حجب هويات القائمين بالعمليات وتحويل الأموال فى كافة أنحاء العالم بطرق ناجحة، وتعد بيتكوين هى العملة المشفرة الأكثر شيوعا. وكان أحد مناصرى داعش أصدر وثيقة بعنوان "بيتكوين وصدقة الجهاد" حدد فيها الأحكام الشرعية لاستعمال هذه العملة الافتراضية وشرحت الوثيقة كيفية استخدام هذه العملة الافتراضية وإنشاء الحسابات المالية على الإنترنت، ونقل الأموال دون لفت انتباه أحد، على اعتبار أن المتبرع لا يستطيع تحويل أموال لشخص مشتبه به أو موضوع على لائحة الإرهاب، ولكنه يستطيع التحويل إلى حساب رقمى لا يعلم أحد من يملكه. والأمثلة على ذلك عديدة، فقد أعلنت إندونيسيا مثلا إن أفرادا من الموالين لتنظيم داعش قاموا بمبادلات مع أشخاص فى سوريا بطريقة بيتكوين بايبال(٣٧).

٤-التدريب والدعم اللوجيستى

تعتبر شبكة الإنترنت وسيلة للاتصال بالغة الأهمية بالنسبة للمنظمات الإرهابية، حيث تتيح لهم حرية التنسيق الدقيق لشن هجمات محددة، وذلك منذ هجمات ١١ سبتمبر

٢٠٠١، التى استخدم فيها أعضاء منظمة القاعدة البارزين الإنترنت بشكل مكثف فى التخطيط وتنسيق أعمال ومهام كل عنصر إرهابى(٣٨).

كما نجحت داعش فى التخطيط والتنسيق لعملياتها الإرهابية الكبرى فى أوروبا، وخاصة فى فرنسا وبلجيكا، من خلال شبكات المعلومات ومواقع التواصل الاجتماعى لا يمكن رصدها، بل وتمحى بعد قراءتها مباشرة من خلال أجهزة ألعاب الفيديو المتصلة عبر الإنترنت، وأدت هذه العمليات الإرهابية لمقتل نحو ٢٠٠ شخص فى نوفمبر ٢٠١٥، وفشلت أجهزة المخابرات الأوروبية فى رصد العمليات قبل وقوعها لكنها اكتشفت هويات منفذيها من خلال هواتفهم المحمولة ومكالماتهم المتبادلة مع أفراد المنظمة(٣٩).

من ناحية ثانية يعد التدريب الافتراضى أو تقديم الدعم الفنى للارهابيين عبر الإنترنت من أبرز ملامح ميكانيزمات الإرهاب الإلكترونى، حيث يمكن الزعم بوجود تراكم معرفى على الفضاء الشبكى تسعى الجماعات الإرهابية من خلاله إلى تقديم إرشادات وطرق صنع القنابل اليدوية والأسلحة الكيماوية الفتاكة وأساليب التفخيخ والتفجير... إلخ.

فعندما أصدر تنظيم القاعدة موقعه الرسمى الأول «معالم الجهاد» بالعام ٢٠٠٠ بدأ تنظيم القاعدة فى عقد أول معسكر تدريبى افتراضى على الإنترنت وهو معسكر البتار الذى ظهر بتبنى يوسف العبيرى زعيم القاعدة فى الجزيرة العربية، وهو عبارة عن مجلة إلكترونية تدريبية أخرج فيه تنظيم القاعدة ٢٢ عددا، ولكنه توقف نظرا لمقتل العبيرى الذى كان مسئولًا عن إدارة الموقع الإلكترونى ولم يعط أحدا مفاتيح إدارته. وحتى الآن يقوم الجهاديون بنشر حلقات تدريبية فى كافة المجالات المرتبطة بعملياتهم العسكرية على تلك المواقع والصفحات التابعة لهم(٤٠).

كذلك نشرت داعش دليلا فى عام ٢٠١٥ بعنوان "آليات البقاء على قيد الحياة فى الغرب: دليل المجاهدين" يهدف لتدريب ناشطيها على إخفاء هوياتهم، وتعلم أساليب البقاء على قيد الحياة، ونقل المتفجرات والهروب بعد الهجمات(٤١).

فى هذا السياق يتصاعد الحديث عن دور ما يسمى بالمخططين الافتراضيين، الذين يلعبون دورا مهمًا فى تنسيق العمليات الإرهابية عن بعد، وذلك من خلال تقديم الإرشاد والدعم المرحلى لمنفذى تلك العمليات من خلال خطوات تشمل مثلا التواصل مع عصابات الجريمة المنظمة لشراء الأسلحة للخلية الإرهابية، تحديد المكان الذى سيتم تنفيذ العمليات فيه والتواصل مع المنفذين لتسلم السلاح. فضلا عن إعطاء التوجيهات لتنفيذ العملية الإرهابية. فى بعض الأحيان، يقوم المخطط الافتراضى بتعريف عدد من العناصر المتطرفة ببعضها البعض، ليكون خلية إرهابية صغيرة، وذلك لدفعهم لتنفيذ عمليات إرهابية. ففى سبتمبر ٢٠١٦، ألقت السلطات الفرنسية القبض على خلية من النساء، حاولن وضع سيارة مليئة بالمتفجرات قرب كاتدرائية "نوتردام"، وقد كان المخطط المسؤول عنهم هو "راشد قاسم"، وهو المخطط المسؤول عن تنفيذ العمليات الإرهابية فى أوروبا. وفى بعض الحالات، قام المخطط الافتراضى بتزويد متطرف أمريكى يدعى "منير عبد القادر" بعنوان جندى لكى يقتله ذبحا وإن لم ينجح هذا المخطط(٤٢).

٥-التجسس والحصول على الوثائق والمعلومات

يستخدم الإرهابيون الإلكترونيون مواقع التواصل الاجتماعى كأداة لتحديد الأشخاص المستهدفين والتعرف عليهم ومراقبة تحركاتهم، وهو ما يكون له أهمية خاصة فى إطار عمليات الاغتيالات التى تطال بعض رموز الأجهزة الأمنية أو السياسية فى الدول المستهدفة، وذلك إما بمراقبة من يمتلك حسابات على تلك المواقع، أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، مع ضمان سرية المراقبة (٤٣).

٦-تحقيق الأضرار المباشرة

لا يزال تنفيذ العمليات الهجومية أو التخريبية على أرض الواقع هدفا مهمًا وجوهريا للإرهاب الإلكترونى، وهو ما يمكن تحقيقه عادة عبر استهداف البنى التحتية للدول

المستهدفة التى تعتمد على أجهزة الحاسوب الرقمى بهدف تعطيلها أو إيقافها عن العمل. تشير قراءات التاريخ أن أول عملية هجوم فى ذلك السياق جاءت فى يونيو عام ١٩٨٢ عندما انفجر أحد خطوط أنابيب الغاز السوفيتية فى سيبيريا فيما يعتبر أول حالة تم رصدها لأضرار البنية التحتية المادية نتيجة الاستخدام المتعمد لأحد أكواد الكمبيوتر الخبيثة، بحسب بعض المصادر، كانت المخابرات المركزية الأمريكية CIA هى من خططت لشراء السوفييت برنامج التحكم فى خط أنابيب الغاز.. الذى تم التلاعب فيه لتخريبه.. بالإضافة إلى أن ما تلا تلك الواقعة من استخدامات ناجحة مزعومة لأكواد الكمبيوتر من أجل تحقيق دمار مادى بهدف إثارة الخوف [٤٤].

يهدف الإرهابيون فى هذا الصدد إلى التأثير فى أكواد برامج الكمبيوتر وإفساد وظائف نظام المعلومات لإتلاف أو تدمير الأصول الافتراضية والمادية. فالتلاعب بالمعلومات أو إفسادها قد يؤدى إلى تقديم معلومات خاطئة، وإثارة الارتباك وعدم الثقة فى الأنظمة الحيوية. قرصنة تم تصميمها من أجل تعطيل المواقع وتخريب حياة الغربيين الطبيعية (المعتمدة على الإنترنت)، القائمة على البنية التحتية الحيوية التى تدعم الأنظمة الطبية، والمرافق، والنقل والأنظمة المالية بشكل خاص.. كما يشمل أيضا أنشطة أكثر إزعاجا مثل تشويه المواقع، وهجمات الحرمان من الخدمة، والاتصال غير المصرح به وكشف المعلومات السرية. فمثلا عند اندلاع الاضطرابات فى سوريا فى مطلع عام ٢٠١٢، اقترح أبو حفص السنى، وهو كاتب كبير فى المواقع الجهادية وأحد مؤيدى تنظيم القاعدة والمجاهدين فى كل مكان، القيام بأعمال القتال السيبرانى ضد النظام السورى. وفى مقال مفصل نشر على الإنترنت فى شهر فبراير من العام نفسه، عدد السنى العديد من الطرق التى يمكن للمجاهدين من خلالها مهاجمة نظام بشار. ودعا الهاكرز المحترفين مثل " Red Virus" و"Omar OX" وغيرهم من "الهاكرز الجهاديين" إلى شن الجهاد الإلكترونى ضد النظام السورى[٤٥].

وفى أسوأ الحالات، قد يتسبب فى إحداث آثار كارثية على البيئة التحتية الحيوية، والتى قد ينتج عنها الموت والدمار. أى خلق تأثيرات حركية مساوية للأعمال

الإرهابية التقليدية. وعلى الرغم من عدم وقوع هجمات إرهابية سيبرانية شديدة التدمير حتى الآن، قد ينخرط لإحداث أضرار مادية ضخمة وتخريب اقتصادى فى البنية التحتية الحيوية مثل شبكات الكهرباء، وأنظمة توزيع النفط والتخزين، وأنظمة مياه الصرف الصحى العامة، وأنظمة المراقبة الجوية، والأنظمة المالية وخاصة شبكات الصراف الآلى (ATM) والعديد من تلك الأنظمة الحيوية إما لأنها تتصل بالإنترنت بصورة مباشرة أو متصلة بطريقة غير مباشرة من خلال الوسائط القابلة للنقل. وقد دعا مقطع فيديو لتنظيم القاعدة يرجع لعام ٢٠١١، المجاهدين السيبرانيين المهرة إلى الهجوم على أنظمة المعلومات الحيوية من خلال شن غارة معلوماتية على غرار غارات الحادى عشر من سبتمبر". شمل الفيديو مقابلات مترجمة مع الخبراء السيبرانيين فى الولايات المتحدة يشرحون فيها كيف يمكن لمثل هذه الهجمات أن تتسبب فى أضرار كبيرة للبنية التحتية الحيوية الداعمة للحياة[٤٦].

الخاتمة

إن العديد من الدراسات اتفقت فيما بينها على عدم وجود تعريف مقبول دوليًا لمصطلح "الإرهاب الإلكترونى". ويعود ذلك إلى العديد من الأسباب. فلا يوجد اتفاق بالأساس حول مفهوم "الإرهاب" الذى يعد المفهوم الرئيسى الذى اشتق منه مصطلح "الإرهاب الإلكترونى". ويرجع بعض الباحثين عدم وجود تعريف متفق عليه للإرهاب الإلكترونى، والخلط بينه وبين المصطلحات الأخرى القريبة منه إلى انتشار المصطلح بسرعة وعلى نطاق واسع، مع تزايد استخدامه من قبل رجال القانون والأكاديميين ووسائل الإعلام للإشارة إلى حالات محددة ومشابهة وليس دائما بصورة دقيقة. فعلى سبيل المثال، اعتبرت كل من الهجمات على البنية التحتية لتكنولوجيا المعلومات والتسلط عبر الإنترنت إرهابا عبر الإنترنت، فى حين أن تلك الهجمات يجب تعريفها بشكل صحيح على أنها جرائم إلكترونية. وعليه فإن الارتباك فى تحديد المصطلح عادة ما يرجع إلى حقيقة أن الأساليب التى يستخدمها مجرمو الإنترنت والإرهابيون

الإلكترونيون يمكن أن تكون متشابهة، على الرغم من أن الأهداف قد تكون مختلفة[٤٧].

وفى السياق ذاته، فإن الإرهاب الإلكترونى ليس مجرد حرب معلومات إرهابية، ذلك أن المنظمات الإرهابية الحديثة تتقن استخدام الإنترنت فى نشر الدعاية وتجنيد عناصر جديدة. ونشير هنا إلى مصطلح "الجهاد الإلكترونى": وهو شكل من أشكال الحرب التى تشن عبر شبكة الإنترنت، وتستند إلى أسس أيديولوجية وتسعى لتحقيق أهداف محددة وهى تنفذ بشكل دقيق ومنظم على شبكة الإنترنت. وقد تبين أن "القراصنة الإسلاميين" يحافظون على التواصل فيما بينهم بشكل ثابت ويتشاركون المعلومات ويتبادلون الخبرات، ويتناقشون حول الاستراتيجيات والأهداف المفترضة[٤٨].

ختاما، هناك قلق متزايد بشأن إساءة استخدام تقنية المعلومات والاتصالات على أيدى الإرهابيين، وخاصة الإنترنت والتقنيات الرقمية الجديدة، لارتكاب أعمال إرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها. وقد شددت الدول الأعضاء على أهمية التعاون بين الجهات المتعددة ذات العلاقة فى مواجهة هذا التهديد، بما فى ذلك بين الدول الأعضاء والمنظمات الدولية والإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدنى.

وفى القرار ٢٣٤١ لعام ٢٠١٧، يهيب مجلس الأمن بالدول الأعضاء إلى "إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافى من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار فى حالات الطوارئ "[٤٩].

ومع تصاعد المهددات المرتبطة بالإرهاب الإلكترونى وتصاعد المخاوف من التطور المستمر فى الأدوات التى تستخدمها التنظيمات الإرهابية وتطور إمكاناتها اتجهت الحكومات والمؤسسات إلى محاولة صياغة تدابير استباقية تحول دون تعرضها لهجمات إلكترونية محتملة، أو تصلح من خلالها قصور تسبب فى هجمات سابقة، وأصبح الإنفاق على الأمن الإلكترونى يمثل نسبة لا يستهان بها من الناتج المحلى الإجمالى للدول، لقد بلغت نسبة الإنفاق فى إسرائيل٠,٣٠٪ من الناتج المحلى وهى أعلى نسبة بين الدول محل الدراسة، تليها المملكة المتحدة، ثم سنغافورة، ثم اليابان، وقد تساوت نسبة الإنفاق فى أستراليا مع الولايات المتحدة الأمريكية، وبلغت (٠,١٩٪) من الناتج المحلى الإجمالى(٥٠).

منذ السنة المالية ٢٠٠٢ إلى عام ٢٠١٧، أنفقت الولايات المتحدة ١٦ فى المئة من ميزانيتها التقديرية كاملة كجزء من مكافحة الإرهاب، وقد بلغ تمويل مكافحة الإرهاب – وهو مصطلح واسع يشمل جهود الأمن الداخلى على مستوى الحكومة، وبرامج التمويل الدولية، والحروب فى أفغانستان والعراق وسوريا – حوالى ٢,٨ تريليون دولار بين السنة المالية ٢٠٠٢ و ٢٠١٧ حسب دراسة مركز ستيمسون Stimson، هذا يبلغ فى المتوسط ١٨٦,٦ مليار دولار سنويا على مدار ١٥ عاما. وعلى سبيل المقارنة، يزيد هذا الرقم على النفقات الدفاعية الشاملة لعام ٢٠١٧ فى روسيا والهند وكوريا الجنوبية مجتمعة(٥١).

وقد خصصت الولايات المتحدة ١٤,٩٨ مليار دولار كميزانية مخصصة للأمن الإلكترونى، وإن تصاعد الإنفاق على الأمن الالكترونى من قبل الحكومة الأمريكية بما يزيد على مليار دولار فى عام ٢٠١٩ مقارنة بعام ٢٠١٧، بينما بلغت الميزانية المخصصة للأمن الإلكترونى فى الولايات المتحدة فى عام ٢٠١٨ ١٤,٤ مليار دولار، ويلاحظ أن الاتجاه العام للإنفاق على الأمن الإلكترونى متزايد خلال الفترة (٢٠١٠– ٢٠١٨)، وقد وصل الانفاق إلى ٤٣,٥ مليار دولار عام ٢٠١٤ مع ظهور تنظيم (داعش)، ثم زاد بمقدار ٥,٥ مليار دولار ليصل إلى ٤٩ مليار فى ٢٠١٥.

ونظرا لتزايد التهديدات فقد وصل الإنفاق على الأمن الإلكترونى إلى ٦٦ مليار دولار عام ٢٠١٨[٥٢].

وقد أشار التقرير الصادر عن مركز الدراسات الاستراتيجية والدولية (CSIS)، بالشراكة مع مؤسسة مكافى McAfee فى عام ٢٠١٧، إلى التأثير الاقتصادى للجريمة السيبرانية، وهو تقرير عالمى يركز على التأثير الكبير للجريمة السيبرانية على الاقتصادات فى جميع أنحاء العالم. إلى أن ما يقرب من ٦٠٠ مليار دولار، أى ما يقرب من واحد فى المائة من إجمالى الناتج المحلى العالمى، يتم اهداره بسبب جرائم الإنترنت كل عام، وهو ما يزيد على نتائج دراسة عام ٢٠١٤ التى قدرت الخسائر العالمية بنحو ٤٤٥ مليار دولار، ويعزو التقرير النمو على مدار ثلاث سنوات إلى المجرمين الإلكترونيين الذين يعتمدون بسرعة على تقنيات جديدة ويسهل نمو الجريمة السيبرانية مع قيام الجهات الفاعلة بتعزيز الأسواق السوداء وزيادة الاعتماد على العملات الرقمية[٥٣].

ومن المتوقع أن يشهد قطاع الأمن الإلكترونى نموا سريعا، ومن المرجح أن تظل أوروبا ومنطقة آسيا والمحيط الهادئ أكبر مستوردى حلول الأمن السيبرانى من المملكة المتحدة. وتستثمر الصين والهند بشكل كبير فى التكنولوجيا الأمنية فى جميع أنحاء المدن والبنية التحتية الوطنية، لذا من المرجح أن تقدم فرصا للموردين، بما فى ذلك من المملكة المتحدة[٥٤].

فيما يتصل بالإرهاب الإلكترونى بصوره وأساليبه المختلفة، فما هو غنى عن البيان، أن الجهود المبذولة وطنيا ودوليا لمكافحته، إنما تواجه تحديا جوهريا يتمثل فى حقيقة عدم وجود صك قانونى عالمى يسهم فى تحديد المشكلة أو الظاهرة محل التحليل تحديدا دقيقا يمكن البناء عليه لتجريمها والمعاقبة عليها.

ومن شأن وجود هذا الصك، أن يلزم الدول الأعضاء فى الأمم المتحدة باتخاذ تدابير معينة، على كافة أساليب الإرهاب الإلكترونى، على نحو محدد على غرار الأعمال المجرمة فى الصكوك التسعة عشر المعتمدة عالميا فى مجال مكافحة

الإرهاب. وهنا أستعير مقولة مهمة للأمين العام السابق للأم المتحدة بان كى مون: "الإنترنت هى خير مثال يوضح كيف يمكن للإرهابيين أن يمارسوا نشاطهم على نحو عابر للحدود حقا، وتصديا له ينبغى على الدول أن تفكر وتعمل على نحو عابر للحدود أيضا".

المراجـــع والهوامش

١- Vida M. Vilić, "Cyber Terrorism on the Internet and Social Networking: Athreat to Global Security", International Scientific Conference n Information Technology and Data- Related Research, **SINTEZA**, January 2017, p. 69, at: http://www.researchgate.net/publication/317753784_cyber_terrorism_on_the_internet_and_social_networking_a_Threat_to_Global_Security.

٢- لمزيد من التفاصيل لكل فئة من الفئات، انظر:

تقرير "استخدام الإنترنت فى أغراض إرهابية"، صادر عن مكتب الأمم المتحدة المعنى بالمخدرات والجريمة بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، ٢٠١٣، ص ص ٣-١٢.

https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

٣- المرجع السابق، ص ٣.

٤- عادل عبد الصادق، الإرهاب الالكترونى القوة فى العلاقات الدولية: نمط جديد وتحديات مختلفة (القاهرة: مركز الدراسات السياسية والاستراتيجية بالأهرام، ٢٠٠٩). ص ص ٣٧-٣٨.

٥- المرجع السابق، ص ٣٧.

٦- For more details, see: Sarah Gordon, Richard Ford, Cyber Terrorism?, Symantec Security Response, **White paper**, p. 4, at:

https://www.symantec.com/avcenter/reference/cyberterrorism.pdf and see also, Barry C. Collins, The Future of Cyber Terrorism, **Crime and Justice International**, March 1997, pp. 15-18.
at:http://www.cjimagazine.com/archives/cji4c18.html?id=415.

٧- Lewis, A., James, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”, Washington DC: **Center for Strategic and International Studies**, 2002, p. 1, at:

https://csisprod.s3.amazonaws.com/s3fspublic/legacy_files/files/media/csis/pubs/021101 risks of cyberterror.pdf.

٨- عادل عبد الصادق، مرجع سابق، ص ص ١١٠-١١١، انظر أيضا:

JonalanBrickey, "Defining Cyber terrorism: Capturing a Broad Range of Activities in Cyberspace", **CTC Sentinel**, August 2012, Volume 5, Issue 8, https://bit.ly/2SgELy0.

٩- Deana Shick, Eric Hatleback and Leigh Metcalf, "Declaring War on Cyber Terrorism, …or Something like That", **Carnegie Mellon University**, SEI Insights, February 1, 2018.at:

https://insights.sei.cmu.edu/cert/2018/02/declaring-war-on-cyber-terrorismorsomething-like-that.html.

١٠- سماح عبد الصبور، "الإرهاب الرقمى، أنماط استخدام الإرهاب الشبكى"، أبو ظبى: **مركز المستقبل**، دورية اتجاهات الأحداث، العدد ٢، سبتمبر ٢٠١٤.

١١- خالد حنفى على، الإنترنت وتصدير الإرهاب، مجلة السياسة الدولية، السنة ٤١، العدد ١٦٢، أكتوبر ٢٠٠٥.

١٢- موسى مسعود أرحومة، "الإرهاب والإنترنت"، **مجلة جامعة الجلفة للدراسات والأبحاث**، العدد ٤، ٢٠١١، ص ١٦٨، متاح على الرابط:

.https://search.mandumah.com/Record/152501

١٣- JomponPitaksantayothin, "Cyber Terrorism Laws in United States, the United Kingdom and Thailand: A comparative study", March 2018, at: https://www.researchgate.net/publication/323748019 Cyber Terrorism Laws in the United States the United Kingdom and Thailand A Comparative Study/citations.

١٤- د. وجيه الدسوقى المرسى، "الأساليب الإلكترونية الحديثة التى تستخدمها التنظيمات الإرهابية فى الجرائم الإرهابية"، بحث مقدم إلى ندوة: دور مؤسسات المجتمع المدنى فى التصدى للإرهاب، **الرياض: جامعة نايف العربية للعلوم الأمنية**، ٢٠١٤، ص ١٤٤.

١٥- KuboyeOluwafemi Samuel et al, **International Journal of Computer Science and Mobile Computing,** Vol.3 Issue.5, May2014, p. 1084, at: https://ijcsmc.com/docs/papers/May2014/315201499b12.pdf.

١٦- Gabriel Weimann, Cyber Terrorism: How Real is the Threat**?, United States Institute of Peace**, Special Report, December 2004, pp. 2-6, at:

https://www.usip.org/publications/2004/05/cyberterrorism-how-real-threat

١٧- مشار إليه فى: محمد محمد الألفى، "العوامل الفاعلة فى انتشار جرائم الإرهاب على الإنترنت"، ورقة مقدمة إلى ورشة عمل: أمن المعلومات والتوقيع الإلكترونى، القاهرة: المنظمة العربية للتنمية الإدارية، ٢٠١٠، متاح على الرابط:http://search.mandumah.com/Record/120812 100

١٨- Tara Seals, "Cyber Terrorism, Set to be Top Threat by 2020", **Info security group**, at: https://www.infosecuritymagazine.com/news/cyberterrorism-top-threat-by-2020.

١٩- سارة بوحادة، أثر الإرهاب الإلكترونى على أمن واستقرار الدول، **جامعة قاصدى مرباح**، الجزائر: المدرسة الوطنية العليا للعلوم السياسية، ٢٠١٩، متاح على الرابط: https://manifest.univouargla.dz/index.php/archives/facult%C3%A9-de-droit-et-des-sciences-politiques/197-laconference-internationale-sur-mondialisation-de- information-politique-et-s%C3%A9curit%C3%A9-nationale-desetats-nations-en-d%C3%A9veloppement-11-04-2019.html.

٢٠- المرجع السابق.

٢١- شيريهان نشأت المنيرى، "عرض لندوة: الإرهاب الإلكترونى: مخاطر جرائم الإنترنت على استقرار النظام الدولى"، **مجلة السياسة الدولية**، مايو ٢٠١٢، متاح على الرابط:

NewsQ2450/aspx/http://www.siyassa.org.eg

٢٢- **BBC**, "Kosovo Info Warfare Spread", January 15, 2014, at: http://news.bbc.co.uk/2/hi/science/nature/308788.stm.

٢٣- Charlotte Mellgard, "The Silent War of Cyber Terrorism", **Vanderbilt Political Review,** Nov. 10, 2015, at: http://vanderbiltpoliticalreview.com/the silent-war-of-cyber-terrorism

٢٤- Sofia Karadima, "New Trends Ln Terrorism: The Use Of Social Media, Cyber--Terrorism, The Role of Open Source Intelligence and The Cases Of Rightwing Extremism and Lone Wolf Terrorism", **Master Thesis**, University Of Piraeus,

2016, pp. 47-48.http://dione.lib.unipi.gr/xmlui/handle/unipi/9315?locale-attribute=en.

٢٥- Ibid.

٢٦- محمد جمعة، ""داعش" و"القاعدة".. قطبان متمايزان فى عام ٢٠١٩"، **مصراوى**، ٩ يناير ٢٠١٩.

https://www.masrawy.com/Author/index/124/

٢٧- SafiaKaradima, "New Trends in Terrorism". op.cit., p.20.

٢٨- Editorial board, "A new Threat in Cyber Dimension: ISIS and the Cybercaliphate",**Mediterranean Affairs**, May 29, 2015, at:

https://www.mediterraneanaffairs.com/a-new-threat-in-cyber-dimension-isis-and-the-cybercaliphate/

٢٩- سارة بوحادة، مرجع سبق ذكره، ص ١٨٤.

٣٠- A new threat in cyber dimension: ISIS and the Cybercaliphate",op.cit.

٣١- عادل عبد الصادق، "٣ مراحل يستخدمها الإرهابيون لتجنيد الشباب"، **حفريات**، ٢٠١٨/٩/١٠.

https://www.hafryat.comhttps://www.hafryat.com/ar/blog/

٣٢- Sofia Karadima, op.cit., p. 2.

٣٣- سارة بوحادة، مرجع سبق ذكره، ص ١٨٤.

٣٤- Sofia Karadima, op.cit., p. 21.

٣٥- Idahosa Stephen Osaherumwen, “International Terrorism: The Influence of Social Media in Perspective”, **WWJMRD** 2017; 3(10): pp. 86-91, at: www.wwjmrd.com International Journal Peer Reviewed Journal Refereed Journal Indexed Journal UGC Approved Journal Impact Factor MJIF: 4.25 e-ISSN: 2454-6615.

٣٦- Ibid.

٣٧- "الإرهاب فى عصر البتكوين.. التقدم على الدولة بخطوات"، **صحيفة العربى اللندنية**، ٢١/ ٢٠١٧/٠٦.

٣٨- أيسر محمد عطية، "الآليات الحديثة للحد من الجرائم المستحدثة "الإرهاب الالكترونى وطرق مواجهته"، بحث مقدم إلى الملتقى العلمى المعنون (الجرائم المستحدثة فى ظل المتغيرات والتحولات الإقليمية والدولية)، المملكة الأردنية الهاشمية، **كلية العلوم الإستراتيجية**، ٢-٢٠١٤/٩/٤، ص ١٣.

٣٩- أيمن حسين، الإرهاب الإلكترونى أخطر معارك حروب الفضاء" الوطن، ٢٠١٧/١/١٤. .http://alwatan.com/details/166324

٤٠- محمد مختار قنديل، "كيف ساعد «مارك زوكربيرغ» الجماعات الإرهابية حول العالم؟"، **إضاءات**، ٠٦/ ٢٠١٦/٠٢ : https://www.ida2at.com/category/politics/ 197

٤١- Ahmet S. Yayla," How to Counter ISIS Wolf-pack", **Modern Diplomacy,** August 25, 2017, at: https://moderndiplomacy.eu/2017/08/25/how-to-counter-isis-wolf-packs/

٤٢- شادى عبد السلام، "الإرهاب عن بعد: نمط تنظيمى جديد لاستهداف الدول الغربية والآسيوية"، **مركز المستقبل**، ١٠ مارس ٢٠١٨، https://futureuae.com/ar-AE/Release/ReleaseArticle/551/

٤٣- A new Threat in Cyber Dimension: ISIS and the Cybercaliphate",op.cit.

٤٤- Lee Roberts, "Cyberterrorism: Defining the New Vector for the Tactics of Fear",**CSPS**, February 16, 2018, at: http://csps.gmu.edu/2018/02/16/cyberterrorism-defining-the-new-vector-for-the-tactics-offear

٤٥- JonalanBrickey, "Defining Cyber terrorism: Capturing a Broad Range of Activities in Cyberspace", **Combating Terrorism Center**, August 2012, volume 5, Issue 8, at:https://ctc.usma.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace.

٤٦- Ibid.

٤٧- أحمد يوسف الجميلى، "القدرات السيبرانية"، **مركز صنع السياسات للدراسات الدولية والاستراتيجية**، ١٩ يونيو ٢٠١٨، على الرابط: https://bit.ly/2EGR3aD

٤٨- عادل عبد الصادق، الإرهاب الإلكترونى القوة فى العلاقات الدولية: نمط جديد وتحديات مختلفة، مرجع سابق، ص ص ١٤٢- ١٤٣.

٤٩- "أمن الفضاء الإلكترونى"، **مكتب مكافحة الإرهاب، الأمم المتحدة**، ولمزيد من التفاصيل عن وثائق الأمم المتحدة حول الأمن السيبرانى، ومبادرات أمن الفضاء الإلكترونى، انظر:

https://www.un.org/counterterrorism/ar/cybersecurity

-٥٠ Nikolai Dobberstein and others, "Benchmarking Cybersecurity Spend as percent of GDP, Cybersecurity in ASEAN: An Urgent Call to Action", **A.T. Kearney, Inc.**,p.15, at: https://www.southeast-asia.kearney.com/article/?/a/cybersecurity-in-asean-an-urgent-call-to-action.

-٥١ Aaron Mehta, Here's how much the US has spent fighting terrorism since 9/11, **Defense News**, May 16, 2018, at:

https://www.defensenews.com/pentagon/2018/05/16/heres-how-much-the-us-has-spent fighting-terrorism-since-911

-٥٢ Spending on cybersecurity in the United States 2010-2018", **Statista Research Department**, April 1, 2015, at:

https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

-٥٣ James Andrew Louis, "Economic Impact of Cybercrime- At $600 Billion and Counting - No Slowing Down", **CSIS**, February 21, 2018, at: https://www.csis.org/analysis/economic-impact-cybercrime

-٥٤ Defence and Security organization, **Department for International Trade**, " UK Defence and Security Export Statistics for 2017", 31 July 2018, at: https://www.gov.uk/government/statistics/defence-and-security-exports-for-2017

Abstract

CYBER TERRORISM : PHENOMENON AND REPERCUSSIONS AND JIHADIST ORGANIZATIONS USING IT

Ingy El Mahdy

Terrorism has developed evolued in numerous ways in its: methods, images and means.Terrorists use modern technology tools to plan terrorist operations, to spread hatred and extremist speeches, incitement to violence and exclusion of others, and to recruit followers and obtain the necessary funding. Cyber terrorism has emergd and taken on a new dimension that differs from traditional terrorism, so that the vast potentials of cyberspace are harnessed not only to commit traditional terrorist crimes, but also to commit new crimes that the international community has not witnessed before.

This research paper presents a deep study of the phenomenon of Cyber terrorism, and how it can be used by extremist organizations, by studying many points: such as the concept, the characteristics, the reasons for the escalation of the phenomenon, the risks and threats posed by cyber terrorism, and finally the exploitation of it by extremist groups, in order to figure out the ways of confronting such a great danger to International peace and security.