مركز البيان للدراسات والتخطيط
Al-Bayan Center for Planning and Studies

الإرهاب الإلكتروني أسبابهُ وطرق العلاج

طالب جبار حسن – زينب كاطع ناهض

سلسلة إصدارات مركز البيان للدراسات والتخطيط

الإرهاب الإلكتروني أسبابهُ وطرق العلاج

طالب جبار حسن* - زينب كاطع ناهض**

المقدمة

يمثل الإرهاب بجميع أشكاله تهديداً خطيراً للأمن الوطني والدولي على حد سواء؛ نظراً لما له من آثار كبيرة على أمن المواطنين واستقرارهم، وعلى الإمكانات الاقتصادية، وعلى الهيبة السياسية للدولة في محيطها الإقليمي والدولي، وتتضح تلك الخطورة بجلاء عبر ما يعتنقه الإرهابيون من فكر هدّام، إذ يعتقدون أن فكرهم هو الصائب وبقية الأفكار الإنسانية ضالة؛ لذلك فهم يسعون جاهدين لنشر فكرهم وعقيدتهم حتى لو تطلب ذلك ارتكاب أعمال إجرامية وحشية، فهم يرومون نشر مشروعهم بأية وسيلة كانت ما دامت تؤدي إلى تحقيق دولتهم المنشودة، ولما كانت الجريمة تتصف بالصفات نفسها ومنذ اقترافها من لدن الإنسان الأول فلا شك بأن وسيلة تنفيذها وارتكابها تختلف وتتطور عبر الزمن، فمن غير المعقول أن تقع جريمة بواسطة سلاح ناري قبل ألفي عام؛ لأن تلك الأداة لم تكن موجودة أصلاً، إلا أنه بتقدم الزمن وتطور العلم وتوالي الاختراعات التي ابتكرها العقل البشري غدا من الممكن أن يلجأ المجرمون عموماً والإرهابيون خصوصاً إلى استعمال التقنيات الحديثة لتنفيذ عملياتهم الإجرامية، فمع ظهور وسائل تقنية المعلومات ومنها الحاسوب، وكذلك ظهور الشبكات المعلوماتية وأهمها شبكة الإنترنت، ونتيجة لما تقدمه هذه التقنية الحديثة من خدمات كبيرة سعى الإرهابيون إلى الاستفادة منها ولكن لصالح الشرّ؛ بحيث أصبحت شبكة الإنترنت خير وسيلة إعلامية لنشر أفكارهم وللدعاية لعقائدهم، وتسهيل الاتصال بينهم، أو تنسيق عملياتهم، أو حتى بتوظيفها في تنفيذ أنشطة إرهابية من قبيل التجسس، وتدمير الفعاليات الإلكترونية للدول والمؤسسات، وابتكار أساليب وطرق إجرامية متقدمة، لينشأ بذلك نمط جديد من الإرهاب يدعى الإرهاب الإلكتروني.

* طالب دكتوراه جامعة بغداد/ كلية العلوم السياسية. ** ماجستير علوم سياسية/ جامعة بغداد كلية العلوم السياسية.

أهمية الدراسة

تستمد هذه الدراسة أهميتها من خطورة موضوع (الإرهاب)، وما يفرضه من تهديدات على الأمن الوطني للعديد من دول العالم، مثلما يستمد أهميته كذلك من المكانة التي باتت تشغلها الشبكة الدولية للمعلومات في المنظور الاستراتيجي لهذه الدول؛ بالنظر لاعتمادها المتزايد عليها في الكثير من أنشطتها، بنحو يجعل أي عمل إرهابي يطال هذه الشبكة يمكن أن يخلف دماراً كبيراً لاقتصاديات تلك الدول وأمنها الوطني وسيادتها الإقليمية.

ونظراً لما تشكله الشبكة الدولية للمعلومات من بيئة خصبة لاستقطاب كل أشكال التفاعلات على الصعيد المعلوماتي، مثلت بالمقابل بيئة مناسبة أيضاً لممارسة العمليات الإرهابية ونشرها على اختلاف صورها، ومن هنا تحدّدت مشكلة الدراسة في الكشف عن مفهوم هذا الوجه الجديد من الإرهاب الدولي وما أسبابه، وما يستخدمه من أساليب تقنية لتهديد أمن البلدان، وما يمكن أن تتسلح به هذه البلدان من طرق لمعالجة هذا التهديد.

كان من نتيجة التطور التكنولوجي والاعتماد الكبير على وسائل الاتصال في تبادل المعلومات وتقديم الخدمات ظهور نوع جديد من الإرهاب، وهو الإرهاب الإلكتروني، وبات من أخطر أنواع الجرائم التي ترتكب عبر شبكة المعلومات الدولية، واتخذ عدة اشكال وأنواع، فضلاً عن تنوع الأساليب المستخدمة من لدن مرتكبيه؛ وبذلك شكل الإرهاب الإلكتروني بيئة استيراتيجة ملائمة لاستقطاب أشكال جديدة من الصراع وانتشاره على المستويين الداخلي والدولي؛ مما يتطلب ذلك تنسيقاً إلكترونياً عالي المستوى بين الأجهزة الأمنية؛ لإيجاد سبل لمكافحته والحدّ من خطورته.

ماهية الإرهاب الإلكتروني

أولاً: مفهوم الإرهاب الإلكتروني

بادئ ذي بدء نعرف مفهوم الإرهاب بنحو عام، إذ يمكن القول بعدم وجود اتفاق بين الأفراد والجماعات على تحديد مفهوم الإرهاب؛ لأنه عملية صعبة وشائكة لصدورها عن أسس نفسية تابعة لذات فاعلها؛ وعليه عرف الإرهاب أنه «استيراتيجية عنف منظم ومتصل من خلال جملة من أعمال القتل، والاغتيال، وخطف الطائرات، واحتجاز الرهائن، وزرع المتفجرات وما شابه ذلك من أفعال، أو التهديد بها، وتهدف إلى خلق حالة من الرعب العام، وذلك بقصد تحقيق أهداف سياسية»[1].

أما الإرهاب الإلكتروني فقد أثار أيضاً جدلاً بشأن مفهومه، ويمكن تعريفه على أنه «العدوان، أو التخويف، أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادرة من الدول، أو الجماعات، أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، بغير حق بشتى صنوف وصور الإفساد في الأرض»[2].

ثانياً: أنواع الإرهاب الإلكتروني

هناك عدة أنواع من الإرهاب الإلكتروني تتمثل فيما يأتي:[3]

1. الدخول غير المشروع في نظم معالجة البيانات وقواعدها، سواء أحدث هذا الدخول تلاعباً أو لا.

1- هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، ط1، دار الكتب العلمية، بيروت، 2005، ص: 26.

2- ضرغام جابر عطوش ال مواش، جريمة التجسس المعلوماتي (دراسة مقارنة)، ط1، المركز الطولي للدراسات والبحوث العلمية، مصر، 2017، ص: 92.

3- أحمدي بو جليطة بو علي، الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي: دراسة للتجربتين السعودية والقطرية، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد (16)، جامعة حسيبة بن بو علي الشلف، الجزائر، 2016، ص: 183.

2. الاعتداء على المواقع الإلكترونية سواء أكان ذلك بمسح، أم تعديل بيانات، أم التلاعب فيها، أم إعادة تشغيل النظام.

3. انتهاك السرية والخصوصية لبيانات الشخصية والأضرار بصاحبها.

4. الاعتداء على الأموال الإلكترونية، وهي الأموال المتداولة إلكترونيا، مثل عمليات سحب الأموال التي تقوم بواسطة الصراف الآلي أو الهاتف المصرفي بواسطة الإنترنت للبنوك وإيداعها.

5. تزوير أو تقليد التوقيع الإلكتروني التي هي عبارة عن رموز تميّز صاحب هذا التوقيع، ويعدّ وسيلة تعتمد في المعاملات الإلكترونية، ويقوم مقام التوقيع الكتابي.

وهناك من يقسم الإرهاب الإلكتروني بطريقة مغايرة استناداً إلى موضوعين: الأول من حيث مرتكبوه، والثاني من حيث موضوعه، فمن حيث مرتكبوه يقسم على إرهاب إلكتروني فردي، وهو الذي يقوم به فرد؛ بغية تحقيق هدف أو أهداف محددة، وإرهاب إلكتروني جماعي تقوم به جماعة بشرية معينة لتحقيق أهداف محددة، وهناك إرهاب إلكتروني دولي الذي تقوم به دولة أو أكثر ضد مواطنيها أو ضد دولة أخرى[4].

أما من حيث موضوعه فيقسم على: الإرهاب الإلكتروني الديني، إذ يمارس الإرهاب الإلكتروني لتشويه صورة الدين الإسلامي ونشر ما يسيء إلى الشريعة الاسلامية عبر شبكة الانترنت، للسيطرة على ادمغة الشباب غير الواعي لاستغلالهم وتحريف عقائدهم، وما يزال الدين الإسلامي يخوض الكثير من الصراعات الطائفية والمذهبية، والدليل وجود الكثير من المواقع الإلكترونية التي تشوه صورة الإسلام والمسلمين، والنوع الثاني هو الإرهاب الإلكتروني الفكري، إذ يستخدم الإرهابيون شبكة الإنترنت لنشر مبادئهم وأفكارهم الضالة التي تفسد العقول وتحرف العقائد، وتقوم بتعليم المتعاطفين

4- علي عبد المحسن البغدادي، الإرهاب دراسة في المنهج المعرفي تفكيك البنية المعرفية للإرهاب بوصفها محتوى لكل مظاهر المشكلة، المجلة السياسية والدولية، العددان (36-35)، الجامعة المستنصرية، 2017، ص: 657.

معهم تصنيع الأسلحة والقنابل، والقيام بعمليات إرهابية على أرض الواقع وفي أماكن محددة[5].

وهذا النوع من الإرهاب الفكري تم استخدامه من قبل داعش، فقد منحت هذه التقنية للإرهابيين (داعش) إمكانية بناء تشكيلات منجمة وعلى نطاق عالمي ليس فقط في العراق وسوريا، إذ استفادت هذه الجماعات من الخدمات التي تعدها تقنية الاتصالات أن يحصلوا على مستوى واسع من القدرات العديدة، واستقطاب أعداد كبيرة من المقاتلين المحليين، وبذلك استطاع داعش عن طريق الحرب الإلكترونية من امتلاك الإمكانات الضخمة سواء عبر التبرعات التي حصل عليها من بعض البلدان الإقليمية أو الدولية أو عبر سيطرته على مواقع استيراتيجية تضم حقول نفط وغاز أو وضع اليد على أموال الدولة كما حصل في الموصل[6].

وقد كشف تقرير أن داعش الإرهابي لديه (90 ألف) صفحة باللغة العربية على مواقع التواصل الاجتماعي Facebook، و(40 ألفاً) بلغات أخرى، فضلاً عن موقعه الذي دشنه التنظيم بـ7 لغات؛ لابتزاز الشباب وضمهم لصفوفه فحوالي (3400) شاب انضم إلى صفوف داعش عن طريق حملات التنظيم الإلكترونية[7]. وجدير بالذكر أن أهم موقعين لداعش هما مؤسسة الفرقان، ومركز الفجر الإعلامي الذي يشرف عليهما بعض العراقيين، والكثير من العرب[8].

5- زين العابدين عواد كاظم الكردي، جرائم الإرهاب الإلكتروني (دراسة مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2018، ص: 88-87.

6- علي جاسم محمد التميمي، الإرهاب الإلكتروني وأثره على المجتمع، المجلة السياسية والدولية، العددان (34-33)، الجامعة المستنصرية، 2016، ص: 499.

7- بوحادة سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2016، ص: 7.

8- عبد الرحمن البكري، داعش ومستقبل العالم بين الوضع السياسي والحديث النبوي الشريف، دار الغرباء للنشر، ألمانيا، 2014، ص: 108.

أسباب الإرهاب الإلكتروني وأساليبه وطرق العلاج

أولاً: أسباب الإرهاب الإلكتروني

هناك تنوع في أسباب ارتكاب الإرهاب الإلكتروني، إذ توجد أسباب عامة، وأخرى خاصة.

أ- الأسباب العامة للإرهاب الإلكتروني:

1- الأسباب السياسية: يعدّ الدافع السياسي من أهم الأسباب المحفزة على الإرهاب الإلكتروني، إذ إن ممارسة السلطة السياسية في الدولة من لدن شخص واحد وتهميش المواطنين وتغييبهم عن المشاركة السياسية، فضلاً عن المساس بحقوق الإنسان، وعدم ظهور الشفافية الكافية في رفع الحواجز بين الحكومة والمجتمع؛ لتبدو السياسة أكثر قبولاً في جو ديمقراطي عام، إذ إن غياب الديمقراطية وحرية الرأي والتعبير والمشاركة من شأنه أن يولد الحركات والمنظمات السرية، وردود الأفعال الغاضبة من قبل الأفراد المطالبة في الحصول على حقوقها المفقودة، وذلك بطرق وأساليب شتى ومنها الإرهاب الإلكتروني[9]. وأثبتت الوقائع أيضاً أن النزاعات القائمة بين دولتين غالباً ما تودي إلى تبادل العمليات الإرهابية الإلكترونية بينها، وهذا ما حدث في ظل النزاع القائم بين أمريكا وكوبا، إذ حاولت الطبقة السياسية الأمريكية ربط الجزيرة الكوبية بالإرهاب الإلكتروني، وذلك بعد بضعة أيام من تسلّم (جورج دبليو بوش) السلطة، بحجة أن كوبا تمثل خطراً غير مباشر على الأمن القومي للولايات المتحدة، ولها القدرة على شن هجمات إلكترونية على البنية التحتية للقوة العظمى، وهو ما جعل أمريكا تضع مجتمعها الخاضع للإعلام بدرجة عالية ضد الجزيرة[10].

9- عبد الصمد سعدون عبد الله، ليلى عاشور حاجم، ظاهرة الإرهاب في عصر المعلوماتية الرقمية: مبررات الحدث وسبل المواجهة، مجلة قضايا سياسية، العدد (1)، جامعة النهرين، 2012، ص: 15-14.

10- أليهاندرو كاسترو أسين، إمبراطورية الإرهاب، ترجمة وفيقة ابراهيم، ط1، شركة المطبوعات للتوزيع والنشر، بيروت، 2012، ص: 155-154.

وفي ظل النزاع السياسي القائم بين دول الخليج العربي الذي حصل في العام 2017 اختراق لوكالة الأنباء القطرية من قبل الإمارات، ونشرت تصريحات للشيخ تميم، وقد وظفت الدول الأربع السعودية، والبحرين، والإمارات، ومصر هذه التصريحات ضد قطر وقطعت العلاقات معها[11].

2- الأسباب الاجتماعية: من المسلم به أن السلوك الإجرامي في حقيقته ظاهرة اجتماعية، وهذا السلوك نتيجة لتفاعل عدة عوامل اجتماعية تعود في أصلها إلى الأسرة والمدرسة والأصدقاء والعمل، فكل بيئة من هذه لها أثر لا يستهان به في توجيه الفرد نحو ارتكاب الجرائم بأنواعها ومنها الإرهاب الإلكتروني؛ لأن الإنسان بطبعه كائن قابل للتأثير والتأثّر والتغيير والتغيّر، ويرى بعض علماء الاجتماع كالعالم (إميل دوركهايم)، والعالم (ثورستن سيلين) أن الحضارة الحديثة والحياة العصرية من الأسباب الاجتماعية التي تدفع بالفرد نحو ارتكاب السلوك الإجرامي، لأن المجتمع المتحضّر له أثر فعال في زيادة الجريمة؛ بسبب قلة اهتمامه بمهماته التي ينبغي أن يقوم بها تجاه الأفراد، كالاعتناء بهم، وتربيتهم تربية سليمة[12].

3- الأسباب الاقتصادية: نظراً لدور الاقتصاد المحوري في الحياة الدولية كونه القوة الأساسية في تحديد أنماط التفاعلات وتوزيع مراكز القوة والتأثير على الخارطة الدولية، فإنه لا يمكن تجاوز ما له من دور آخر في تقديم تفسيرات موازية لظاهرة الإرهاب، على تخوم الظلم الذي يخلقه التفاوت في توزيع الموارد والقدرات الاقتصادية سواء أكان بين الدول أم بين أفراد الدولة الواحدة، إذ إن معاناة الأفراد من المشكلات الاقتصادية الخاصّة بالفقر والبطالة والتضخم في أسعار المواد الغذائية والخدمات الأساسية؛ كل ذلك من العوامل المؤثرة في إنشاء روح التذمر ودفع الأفراد والجماعات للجوء إلى وسائل الإرهاب[13].

11- أسامة أبو أرشد، الموقف الأمريكي من الأزمة الخليجية، مجلة سياسات عربية، العدد (27)، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2017، ص: 24.

12- زين العابدين عواد كاظم الكردي، مصدر سبق ذكره، ص: 110-109.

13- سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مجلة جامعة كربلاء العلمية، العدد(3)، جامعة كربلاء، 2016، ص: 62.

ب- الأسباب الخاصة للإرهاب الإلكتروني

يمكن تشخيص هذه الأسباب بالآتي[14]:

1- انخفاض تكلفة الآليات الإلكترونية مقترنة بالأدوات التقليدية التي تتم بها العمليات الإرهابية كالقنابل، والمتفجرات، والأسلحة المتطورة.

2- غياب الحدود الجغرافية والحواجز المكانية في الفضاء الإلكتروني يعدّ فرصة مناسبة للإرهابيين.

3- ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق يوفر للإرهابيين سبيلاً لمهاجمتها لتحقيق أهدافهم، فقد تقوم الجماعات الإرهابية بمهاجمة شبكات الحاسب الآلي الخاصة بالحكومات أو الشركات الخاصة أو الأفراد.

4- غياب السيطرة والرقابة على الشبكات المعلوماتية يعدّ من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، ففي الكثير من الأحيان يصعب على أجهزة الشرطة ملاحقة القائمين بعمليات الإرهاب الإلكتروني والتعرّف على هويتهم.

ثانياً: أساليب الإرهاب الإلكتروني

تعمد الجماعات والتنظيمات الإرهابية اتباع عدة أساليب ووسائل في أهدافها ومآربها الإرهابية، وهذا ما سنبحثه باختصار:

1- إنشاء مواقع على الإنترنت: ينشئ الإرهابيون مواقع لهم على شبكة الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، وقد سهّل الإنترنت هذه العملية كثيراً، وفتح أمام الجماعات المتطرفة إمكانية الالتقاء في أماكن متعددة في وقت واحد؛ لتبادل الحديث، وتجنيد الأتباع عبر منتديات

14- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، ط 1، المكتب العربي للمعارف، القاهرة، 2016، ص: 37-36.

الحوار وما يعرف بغرف الدردشة، ومن الأمثلة على بعض المواقع الإلكترونية العربية التي قام بإنشاها وتصميمها بعض التنظيمات الإرهابية: موقع نداء وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث (11 أيلول 2001)، ومن خلاله تصدر البيانات الإعلامية للقاعدة، وموقع ذروة السنام، وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة، والبتار وهي مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة وتختص بالمعلومات العسكرية والميدانية والتجنيد[15].

2- البريد الإلكتروني: يعدّ من أكثر الوسائل المستخدمة في الإرهاب الإلكتروني، إذ يتم استخدامه في التواصل بين الإرهابيين، وتبادل المعلومات بينهم، بل إن كثيراً من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها [16].وجدير بالذكر أن المصادر الغربية تشير إلى أن (توم ميتزقر) أحد أشهر المتطرفين الأمريكيين العنصريين، ومؤسس مجموعة المقاومة الإيرانية البيضاء، كان من أوائل المؤسسين لمجموعة بريد الكتروني للتواصل مع أتباعه، وبث أفكاره عام 1985 [17].

3- أنظمة الهاكرز أو الاختراق: يقوم الإرهابيون المبرمجون الذين يسمون بـ(الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية والاعتداء على البنية التحتية المعلوماتية للمؤسسات الحكومية والخاصة على حد سواء، ومن أشهر برامج الهاكرز (web cracker4)، و(buster net)، و(net bus haxporf)[18].

15- أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة علمية مقدمة إلى الملتقى العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، كلية العلوم الاستيراتيجية، **عمان**، 2014، ص: 18-16.

16- سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استيراتيجيات الأمن القومي، ورقة علمية مقدمة إلى (مؤتمر الجرائم المستحدثة-كيفية إثباتها ومواجهتها)، المركز القومي للبحوث الاجتماعية والجنائية، مصر، 2010، ص: 3.

17- علي جاسم محمد التميمي، مصدر سبق ذكره، ص: 490.

18- مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، العدد (5)، جامعة الناصر، اليمن، 2015، ص: 135.

ويعدّ علم الاختزال من الطرق الحديثة في التجسس الإلكتروني، إذ يعمل المتجسس الإرهابي على تسريب المعلومات الرقمية الحساسة ونقلها عن طريق إخفائها –في بداية الأمر– في وسيط إلكتروني دون إحداث أي تغيير أو تشويه بالرسالة المرسلة، بحيث لا يمكن اكتشافها والتفطن لها حتى لو تم ضبط الشخص متلبساً بالجريمة، وتعدّ من أخطر طرق التجسس ولاسيما عند استخدامها من قبل الإرهابيين[19].

هذا وقد ازدهرت في السنوات الأخيرة صناعة جاسوسية تكنولوجية كاملة، وأصبح رجال التجسس التكنولوجي مجهزين بأحدث الأجهزة، فهناك لاقطة أجهزة (الانسر ماشين)، ويمكنها التقاط رسائل الانسر ماشين من على هاتف الشخص المستهدف، وجهاز تحكم تم تطويره لحساب وكالة الأمن القومي الأمريكي، يستطيع رصد رسائل البريد الإلكتروني الصادرة والواردة، وتعمل شركات مثل: (راي ثيون) المتعهد العسكري لإحدى وكالات التجسس الخاصة مع (اس ثري اي) من أجل تطوير معدات تكنولوجيا عسكرية لإحدى منشآت وحدة نشاطات حرب المعلومات البرية التابعة للجيش الأمريكي لاستخدامها في مجال (الاستخبارات التنافسية)، أما منظار (الاندر دور) المزود بجهاز الرؤية الليلية فيستطيع من يستخدمه أن يشاهد غرفة بأكملها من الداخل[20].

4– طريقة الفيروسات لتدمير أنظمة المعلومات: تقوم التنظيمات الإرهابية بمحاولة تخريب نقطة الاتصال أو النظام عبر شبكة الإنترنت الخاصة بالأفراد والمؤسسات العسكرية والمدنية والشركات الخاصة، عن طريق صنع أنواع من الفيروسات الجديدة التي تسبب ضرراً كبيراً لأجهزة الكمبيوتر والمعلومات التي تم تخزينها على هذه الأجهزة، وتعدّ الفيروسات أو الديدان من أخطر الأسلحة التي تستخدمها المجاميع الإرهابية في شن هجوماتها الإلكترونية، ويزداد الخطر إذا دخلت على خط المواجهة والإرهاب الإلكتروني دول بإمكانيات واسعة، والمثال على ذلك الفيروسات

19– عبادة الحارث خليل قمر، فن الاختزال بين الحقيقة والخيال، جامعة الحسين بن طلال، الأردن، 2015، ص: 5.

20– ممدوح الشيخ، التجسس التكنولوجي: سرقة الأسرار الاقتصادية والتقنية، مكتبة بيروت، سلطنة عمان، 2007، ص: 71.

(ستاكسنت) التي طورتها الولايات المتحدة الأمريكية وإسرائيل للنيل من البرنامج النووي الإيراني وتعطيله، وهو الأمر الذي ينطبق على إرهاب الدولة طالما كان هذا العمل غير مشروع ولتحقيق أغراض سياسية دون أن تعلن حالة الحرب بين هذه الدول[21].

وبهذا يمكن القول إن الفضاء الإلكتروني يستخدم لممارسة أنواع القوة، ومن أبرز أنماط ممارسة القوة في الفضاء الإلكتروني «نمط القوة الصلبة» عبر استخدام مقدراته وأدواته في عمل تخريبي، كقطع كابلات الاتصال، أو تدمير أنظمة الاتصالات، أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بنحو يهدد أمن الدولة والسكان، وهناك «نمط القوة الناعمة»، وذلك بدعم دوره في إدارة العمليات النفسية والتأثير في الرأي العام، وتكوين التحالفات الدولية؛ مما شكل ثورة معلوماتية هائلة لا حدود لها، ما دام عكفت عليها أجهزة الاستخبارات الكبرى للحصول عليها أولاً، والبحث فيها ثانياً، وتوظيف نتائجها ثالثاً[22].

5- القنابل المعلوماتية: يمكن تقسيمها على نوعين: القنابل المنطقية التي تعرف بأنها البرمجية التي يتم تداولها بكثرة في البرمجيات سواء المقتناة أو عبر الإنترنت، وهي عبارة عن جزء سري من البرمجية ينفجر فيبطل عملها، والقنابل الزمنية وهي برمجية توضع في النظام المعلوماتي لتنفجر في تأريخ معيّن يحدده صانعها لتسبب أضراراً للنظام المعلوماتي[23].

21- سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص: 63.

22- نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدولة»، مجلة مركز بابل للدراسات الإنسانية، العدد (2)، جامعة بابل، 2018، ص: 200.

23- زين العابدين عواد كاظم الكردي، مصدر سبق ذكره، ص: 120.

وفضلاً عن الأساليب السابقة توجد أساليب أخرى مستحدثة انتهجها الإرهاب في العصر الراهن، وهي[24]:

1- أسلوب التغطية بالقول: يعدّ من أساليب التشفير الخاصة بتغيير الصوت واللغة، التي انتهجها الإرهاب، وتكون متعارف عليها لدى تلك الجماعات الإرهابية، ويغلب عليها أسلوب البساطة لأغراض التمويه.

2- أسلوب التغطية بالعمل: تقوم تلك الجماعات بإخفاء الشخصية الحقيقية للشخص إلى شخص آخر كأن يكون ريفياً، أو أجنبياً أو غير ذلك، وتكون لهولاء اهتمامات بالبرامج فيجذب الضحية المراد إيقاعها، وتكون أساليب التغطية بالعمل بالملبس ونحوه.

3- الأسلوب المختلط: الذي يجمع بين الأسلوبين المذكورين آنفاً.

ثالثاً: طرق علاج الإرهاب الإلكتروني

إن استخدام الإنترنت لأغراض إرهابية ظاهرة عابرة للحدود الوطنية تتطلب اتخاذ تدابير متكاملة للتصدي لها، وتوجد هناك عدة طرق للوقاية من الإرهاب الإلكتروني أهمها[25]:

1- تشفير البيانات باستخدام تقنية (wired equivalent privacy)، وباستخدام مفتاح كبير للتشفير يصعب كسره واختراقه، على أن يتم تغييره دورياً.

2- تغيير الكلمات السرية لنقاط الوصول من المنتجات المشتراة من الشركات المصنعة بكلمات

24- حسن تركي عمير، جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسة، عدد خاص، جامعة ديالى، 2013، ص: 332.

25- علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، ورقة علمية مقدمة إلى المؤتمر الدولي الأول (العلوم الشرعية تحديات الواقع وافاق المستقبل، كلية العلوم الشرعية، سلطنة عمان، 2018، ص: 1287-1286.

سرية وصعبة تجمع بين الحروف الصغيرة والكبيرة والأشكال بحيث يصبح صعباً اختراق الشبكة مستقبلاً.

3- استخدام بعض برامج مكافحة التجسس الشهيرة، مثل برنامج: (ad aware) الذي يعد من أشهر برامج مكافحة التجسس، إذ يعمل على إزالة ملفات التجسس غير المرغوب فيها مباشرة.

4- استخدام تقنية (mac address) عوضاً من (ip address)؛ لحماية الشبكات اللاسلكية الداخلية لصعوبة اختراقها.

وفضلاً عن ذلك تم تطوير وسائل تقنية جديدة بهذا الصدد، ومنها برامج الجدار الناري وهو عبارة عن برامج، أو جهاز يوفر سياجاً أمنياً ما بين الحاسب الآلي وشبكة الإنترنت أو شبكة حاسبات أو بين شبكة حاسبات وأخرى، حيث يتم إخضاع جميع عمليات الدخول والخروج من وإلى الشبكة لسيطرة الجدار الناري، وظهر أول جدار حماية للشبكات عام 1980، وهناك أيضاً الشبكة الافتراضية، وهي شبكة خاصة بشركة أو منشأة يتم إنشاؤها فوق شبكة عامة، وتعمل على أسس فنية مختلفة، وسميت افتراضية لأن ليس لها وجود مادي، وأنها لا تستمر لوقت طويل، وإن كان بعضها مستمراً، يضاف إلى ذلك تطوير أجهزة تعمل على الخصائص البيولوجية للإنسان والتي لا تسمح بالوصول إلى النظام المعلوماتي إلا لأشخاص مصرح بهم، مثل استخدام بصمة الإبهام، والصوت، وخط اليد، وحدقة العين[26].

هذا واتخذت الدول على عاتقها سن التشريعات لمعالجة موضوع الإرهاب الإلكتروني فتم توقيع الاتفاقيات الدولية الجماعية في مجال مكافحة الإرهاب الإلكتروني، ومنها الاتفاقية الدولية لمكافحة الإرهاب والجريمة الإلكترونية التي وقعتها عام 1999 أكثر من (26)دولة، وكذلك اتفاقية (بودابست 2001) للجرائم الإلكترونية التي تعكس الجهد الواسع والمميز للاتحاد الأوروبي ومجلس أوروبا، وتبعها اتفاق الدول الصناعية الثماني الكبرى في مؤتمرها السنوي بألمانيا عام 2007 على

26- ضرغام جابر عطوش ال مواش، مصدر سبق ذكره، ص: 78-74.

خطة لمواجهة الإرهاب الإلكتروني على مستوى العالم، إلى جانب إصدار الإعلانات الدولية، وسن القوانين الوطنية[27].

وتعدّ السويد أول دولة تسن تشريعات خاصة بجرائم بالحاسب الآلي، إذ صدر قانون البيانات السويدي عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، فضلاً عن شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، ثم تبعتها الولايات المتحدة الأمريكية، إذ شرّعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي عام 1976[28].

وقد استحدثت الولايات المتحدة الأمريكية قسم محاربة جرائم الكمبيوتر والإرهاب الإلكتروني في مكتب التحقيقات الفدرالي عام 1998؛ لحماية خصوصية المعلومات إذ تحرّض الولايات المتحدة على حماية هذه الخصوصية، ولذلك يقول مدير مركز معلومات الخصوصية الإلكترونية في واشنطن «إن الخصوصية ستكون بالنسبة إلى اقتصاد المعلومات في القرن القادم مثل حماية المستهلك والهموم البيئية بالنسبة إلى المجتمع الصناعي في القرن العشرين»[29].

أما بريطانيا فتأتي ثالثةً من حيث الدول التي تسن قوانين خاصة بجرائم الحاسب الآلي، إذ أقرت قانون مكافحة التزوير والتزييف عام 1981، وسنت عام 2006 قانون الإرهاب الذي يُجرّم في الجزء الأول منه قيام شخص بنشر أقوال يقصد بها التشجيع المباشر أو غير المباشر لأفراد الجمهور على أن يقوموا بالتحضير لأعمال إرهابية أو التحريض عليها [30].

27- سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص: 65.

28- رافد عيادة الهاشمي، الإرهاب الإلكتروني، مكان الطبع بلا، سنة الطبع بلا، ص: 32.

29- خالد علي سليمان بني أحمد، الضوابط الشرعية المتعلقة بالعمل المحوسب مقارنًا بالقانون، المجلة الأردنية في الدراسات الإسلامية، العدد(1)، جامعة آل البيت، الأردن، 2008، ص: 19.

30- استخدام الإنترنت في أغراض إرهابية، منشورات مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فينا، 2013، ص: 29.

ولم تكن الدول العربية بمنأى عن ذلك فقد اتخذت تدابير للمعالجة، ولاسيما دول الخليج العربي التي طورت اهتمامها بالأمن الإلكتروني أكثر من الدول العربية الأخرى، وتعد الإمارات الأكثر بروزاً في مجال الدفاع الإلكتروني على مستوى الخليج، فقد طورت قدراتها الدفاعية الإلكترونية منذ وقت طويل، وكانت من أوائل الدول التي قامت بذلك، وفي عام 2012 أصدرت الإمارات قانوناً خاصاً بمكافحة الجريمة الإلكترونية، وفي عام 2014 أعلنت الإمارات أنها ستضاعف ميزانيتها للأمن القومي إلى (10 مليار) دولار في السنوات العشر القادمة، وإن أغلب هذه الزيادة ستوجه للأمن الإلكتروني[31].

وقد أصدرت المملكة العربية السعودية قانوناً خاصّاً بمكافحة الجرائم المعلوماتية والحد من وقوعها والمساعدة في تحقيق الأمن المعلوماتي، وحماية المصالح العامة والاقتصاد الوطني، وفي قطر صدر قانون العقوبات الجديد رقم (11/2004) متضمناً نصوصاً خاصةً بالجرائم الإلكترونية، واهتمت سلطنة عمان هي الأخرى بتعديل قانونها الجزائي فأصدرت المرسوم رقم (72/2001) الذي أضاف نصوصاً جديدة خاصّة بالجرائم المعلوماتية[32].

وعلى الرغم من أن دول الخليج تعد الأبرز في الشرق الأوسط في الاهتمام بالجوانب الدفاعية للأمن الإلكتروني، إلا أن الأبعاد الهجومية تغيب عنها تماماً فلم تطور قدرات هجومية أو إجراء تدريبات على الحروب الإلكترونية، ولم توجّه الاهتمام إلى شن هجمات إلكترونية ضد دول أو فواعل أخرى كما تفعل القوى العظمى، إذ قامت الولايات المتحدة الأمريكية في عام 2000 بتطوير برنامج سمي (كارنيفور) أو الملتهم وظيفته التجسس على جميع أنواع الاتصالات التي تتم عبر الإنترنت[33].

31- نوران شفيق، مصدر سبق ذكره، ص: 82-81.

32- مايا حسن ملا خاطر، مصدر سبق ذكره، ص: 141.

33- سعد عطوة الزنط، مصدر سبق ذكره، ص: 20.

وجدير بالذكر أن العراق لم يشرع قانوناً للمعلوماتية، وما زال القضاء مقيداً بمبدأ الشرعية (لا جريمة ولا عقوبة إلا بنص)، وعلى الرغم من وجود مشروع قانون الجرائم المعلوماتية لعام 2011 بيد أنه لم يقر حتى الآن[34].

الخاتمة

نخلص مما سبق أن الإرهاب الإلكتروني يمتاز باستغلال التقدم التكنولوجي –بما فيه تكنولوجيا الاتصالات والمعلومات والشبكة العنكبوتية– من قبل الجماعات والمنظمات الإرهابية بدوافع سياسية، واقتصادية، واجتماعية من أجل تخطيط إفعالهم الإرهابية التخريبية وأعدادها وتنظيمها، مع ما يترتب على ذلك من أضرار بالغة في جميع المجالات التي تصل إلى حد تقويض سلطة الدولة وتهديد أمنها القومي وإلحاق الأذى باقتصادها الوطني واستثماراتها الأجنبية؛ ويرجع السبب في استخدام الإرهابيين لوسائل تقنية المعلومات كالحاسوب والشبكات المعلوماتية لعدة لعتبارات أهمها أن هذه الوسائل تستخدم لتسهيل ارتكاب الجرائم الإرهابية وربما تعد عاملاً مشجعاً على ارتكابها، فضلاً عن السرعة التي تمتاز بها هذه الوسائل في التنفيذ وتذليلها للمعوقات والصعاب، وإنها تساعد الإرهابيين على إخفاء آثار جرائمهم.

الاستنتاجات

1) يرتبط الإرهاب الإلكتروني بالتطورات التي تحدث في مجتمع المعلومات، فهو يزداد خطورة كلما ازداد التقدم في المجال المعلوماتي، فالاكتشاف والتطور والبناء الذي يجعل من المعلومة مادته الأساسية، يقابله الهدم والدمار الذي يمارسه الإرهاب باستخدام سلاح المعلومة نفسه.

2) الإرهاب الإلكتروني غير محصور بزمان ومكان معينين؛ لذلك يتطلّب من الحكومات متابعته باستمرار.

34– ضرغام جابر عطوش آل مواش، مصدر سبق ذكره، ص: 13.

3) عدم وجود تشريعات قانونية صريحة تحدّ من الجريمة الإلكترونية في أغلب الدول، إذ لم يشر الدستور العراقي وأغلب دساتير العالم إلى ذلك.

4) تتعدد استخدامات الإرهابيين للوسائل التكنولوجية كالإنترنت والأجهزة الذكية وغيرها؛ لأهداف الترويج لمعتقداتها، وتوجيه رسائل التهديد وجمع المعلومات، واختراق الحسابات، وغير ذلك؛ مما يساعد في تنفيذ أعمالهم الارهابية.

5) إذا كانت المعلومات هي أدوات القوة الناعمة يمكن القول إن الإرهاب الإلكتروني هو سلاح الدمار لهذه القوة الناعمة والخطر المستقبلي؛ نظرا للتطور المتسارع في مجال الإنترنت، واتساع مجال الأهداف التي يمكن مهاجمتها عبر وسائل الاتصالات وتقنية المعلومات.

المصادر:

1. أحمدي بو جليطة بو علي، الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي: دراسة للتجربتين السعودية والقطرية، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد (16)، جامعة حسيبة بن بو علي الشلف، الجزائر، 2016.

2. أسامة أبو أرشد، الموقف الأمريكي من الأزمة الخليجية، مجلة سياسات عربية، العدد (27)، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2017.

3. استخدام الإنترنت في أغراض إرهابية، منشورات مكتب الأمم المتحدة المعني بالمخدرات والجريمة، فينا، 2013.

4. أليهاندرو كاسترو أسين، إمبراطورية الإرهاب، ترجمة وفيقة ابراهيم، ط1، شركة المطبوعات للتوزيع والنشر، بيروت، 2012.

5. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة علمية مقدمة إلى الملتقى العلمي (الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية)، كلية العلوم الاستيراتيجية، عمان، 2014.

6. بوحادة سارة، أثر الإرهاب الإلكتروني على أمن واستقرار الدول، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، 2016.

7. حسن تركي عمير، جاسم عبد الله، الإرهاب الإلكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسة، عدد خاص، جامعة ديالى، 2013.

8. خالد علي سليمان بني أحمد، الضوابط الشرعية المتعلقة بالعمل المحوسب مقارناً بالقانون،

المجلة الأردنية في الدراسات الإسلامية، العدد(1)، جامعة آل البيت، الأردن، 2008.

9. رافد عيادة الهاشمي، الإرهاب الإلكتروني، مكان الطبع بلا، سنة الطبع بلا.

10. زين العابدين عواد كاظم الكردي، جرائم الإرهاب الإلكتروني (دراسة مقارنة)، ط1، منشورات الحلبي الحقوقية، بيروت، 2018.

11. سامر مؤيد عبد اللطيف، الإرهاب الإلكتروني وسبل مواجهته، مجلة جامعة كربلاء العلمية، العدد(3)، جامعة كربلاء، 2016.

12. سعد عطوة الزنط، الإرهاب الإلكتروني وإعادة صياغة استيراتيجيات الأمن القومي، ورقة علمية مقدمة إلى (مؤتمر الجرائم المستحدثة–كيفية إثباتها ومواجهتها)، المركز القومي للبحوث الاجتماعية والجنائية، مصر، 2010.

13. ضرغام جابر عطوش ال مواش، جريمة التجسس المعلوماتي (دراسة مقارنة)، ط1، المركز الطولي للدراسات والبحوث العلمية، مصر، 2017.

14. عبادة الحارث خليل قمر، فن الاختزال بين الحقيقة والخيال، جامعة الحسين بن طلال، الأردن، 2015.

15. عبد الصمد سعدون عبد الله، ليلى عاشور حاجم، ظاهرة الإرهاب في عصر المعلوماتية الرقمية: مبررات الحدث وسبل المواجهة، مجلة قضايا سياسية، العدد (1)، جامعة النهرين، 2012.

16. علي بن محمد بن سالم العدوي، مكافحة التجسس الإلكتروني في القانون العماني مقارنة بالشريعة الإسلامية والقانون الجنائي الدولي، ورقة علمية مقدمة إلى المؤتمر الدولي الأول (العلوم الشرعية تحديات الواقع وافاق المستقبل، كلية العلوم الشرعية، سلطنة عمان، 2018.

17. علي جاسم محمد التميمي، الإرهاب الإلكتروني وأثره على المجتمع، المجلة السياسية والدولية، العددان (34-33)، الجامعة المستنصرية، 2016.

18. علي عبد المحسن البغدادي، الإرهاب دراسة في المنهج المعرفي تفكيك البنية المعرفية للإرهاب بوصفها محتوى لكل مظاهر المشكلة، المجلة السياسية والدولية، العددان (36-35)، الجامعة المستنصرية، 2017.

19. مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، العدد (5)، جامعة الناصر، اليمن، 2015.

20. ممدوح الشيخ، التجسس التكنولوجي: سرقة الأسرار الاقتصادية والتقنية، مكتبة بيروت، سلطنة عمان، 2007.

21. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، ط 1، المكتب العربي للمعارف، القاهرة، 2016.

22. نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدولة»، مجلة مركز بابل للدراسات الإنسانية، العدد (2)، جامعة بابل، 2018.

23. هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، ط1، دار الكتب العلمية، بيروت، 2005.

24. عبد الرحمن البكري، داعش ومستقبل العالم بين الوضع السياسي والحديث النبوي الشريف، دار الغرباء للنشر، ألمانيا، 2014.