ISSN: 2521-9022 Online ISSN: 2309-3447
Print
DOI: https://doi.org/10.17656/25219022
URL: http://jlps.univsul.edu.iq/

دراسات قانونية و سياسية

مجلة فصلية علمية محكمة يصدرها مركز الدراسات القانونية والسياسية
في كلية القانون / جامعة السليمانية - كوردستان العراق

Legal and Political Studies

دراسات قانونية وسياسية

مجلة فصلية علمية محكمة يصدرها مركز الدراسات القانونية والسياسية
في كلية القانون / جامعة السليمانية - كوردستان العراق

السنة السادسة، العدد (١١)
نيسان ٢٠١٨ م - ٢٧١٨ كـ

المشرف الفني: م.م. ئاواره ئازاد احمد
الاخراج الفني: هريم عثمان
طبع: مطبعة كارو - سليمانية

عنوان المراسلات:
إقليم كوردستان العراق / محافظة السليمانية – جامعة السليمانية/ كلية القانون
مركز الدراسات القانونية والسياسية
تلفون: ٠٠٩٦٤٧٤٨٠٨٣٤٤٦٢ - ٠٠٩٦٤٧٤٨٠٨٣٤٤٦١
البريد الالكتروني:jlps@univsul.edu.iq

دراسات قانونية وسياسية
مجلة علمية محكمة

استناداً الى كتاب رئاسة جامعة السليمانية/ مكتب رئيس الجامعة رقم (٩٨٢١/٢٩/٧)، المؤرخ في ٢٠١٣/٨/١٣، المستند على كتاب وزارة التعليم العالي والبحث العلمي لحكومة إقليم كوردستان العراق/ المديرية العامة للاشراف والضمان النوعي رقم (١٥٩٠٦/٤)، المؤرخ في ٢٠١٣/٨/٤ وافق مجلس الوزارة في جلسته رقم (١٤) بتأريخ ٢٠١٣/٧/١٦ على اصدار مجلة (دراسات قانونية وسياسية) في كلية القانون والسياسة بجامعة السليمانية.

واستناداً الى كتاب رئاسة جامعة السليمانية / مكتب رئيس الجامعة رقم (١٠١٠٧/٣/٧)، المؤرخ في ٢٠١٣/٨/٢٠، المستند على كتاب وزارة التعليم العالي والبحث العلمي/ حكومة اقليم كوردستان العراق/ المديرية العامة للاشراف والضمان النوعي المرقم (١٦٤٩٨/٤)، والمؤرخ في ٢٠١٣/٨/١٤، تم اعتماد مجلة (دراسات قانونية وسياسية) لأغراض الترقية العلمية.

شروط النشر في المجلة

- تنشر المجلة البحوث الرصينة التي لم يسبق نشرها من قبل، وذلك في مجالات القانون والسياسة.
- يشترط ألاّ يكون البحث مستلاً من رسالة الماجستير أو اطروحة الدكتوراه للباحث أو المشرف او جزءاً من كتاب سبق لهما نشره.
- تقبل البحوث المكتوبة باللغة العربية فقط، ويتحمل الباحث تقويمها من الناحية اللغوية.
- يتوجب أن يلتزم الباحث ببحثه بأصول البحث العلمي.
- يدفع الباحث مبلغ (٦٠) ألف دينار عراقي أجوراً لنشر بحثه وتقويمه علمياً.
- لا يزيد عدد صفحات البحث مع المصادر والهوامش والجداول على (٢٥) صفحة مطبوعة القياسية (A4)،
- يكون نوع الخط المعتمد في البحوث كافة (Simplified Arabic)، ويكون حجم الخط ١٦ للعناوين الرئيسة، و١٤ للمتن، و١٢ للهوامش، وبمسافة واحدة بين السطور.
- ترقم الصفحات في أعلى الصفحة من اليسار.
- تدرج الهوامش في كل صفحة على حدة، ويختتم البحث بقائمة بالمصادر المعتمدة.
- تعتمد (الفارزة) كفاصلة في الهوامش، ويكون تتابع مضمونها كالآتي: إسم المؤلف، عنوان المصدر، رقم الطبعة، دار النشر، مكان النشر، سنة النشر، رقم الصفحة، مع إعتماد الاختصارات بالنسبة للألقاب، ورقم الطبعة والمجلدات والاجزاء.
- يرفق الباحث ببحثه ثلاثة ملخصات باللغات (العربية والكوردية والانكليزية)، بما لا يزيد عن (١٠٠) كلمة لكل منها.
- تسلم البحوث الى سكرتارية تحرير المجلة بثلاث نسخ مطبوعة، ونسخة الكترونية على CD.
- لا تعاد البحوث، ولا أجور النشر، الى أصحابها في حالة عدم نشرها.
- تعد البحوث المنشورة في المجلة ملكاً لها، ولا تجوز إعادة نشرها الا بعد موافقة هيئة التحرير.

المحتويات

الدراسات القانونية

الدراسات السياسية

الدراسات القانونية

التعاون الدولي في مواجهةجريمة الإرهاب الإلكتروني

أ.د. حسين عبدعلي عيسى
كلية القانون/ جامعة السليمانية

م.م. هه لاله محمد تقي محمد أمين
كلية التربية الأساسية/جامعة السليمانية

المقدمة

مع التطورات التي لحقت بالبشرية تطورت الجريمة واتخذت أشكالاً عدة، وبالتالي ظهرت أنماط جديدة لها أطلقت عليها تسمية الجرائم المستحدثة، التي تتنوع ويتزايد عددها يوماً بعد يوم، وأصبحت صور هذه الجرائم، متعددة ومتجددة، ويمكن ظهور أنماط أخرى منها وفقاً للتطورات التكنولوجية بما فيها أنواع من الجرائم طال نسيانها ظهرت وإتخذت زيادات لا يستهان بها. وفي السياق نفسه تطورت العلاقات الدولية، وامتدت طموحات الدول للتعاون فيما بينها لمكافحة تلك الجرائم. وإزاء ظروف التطور الإجرامي والتطور التكنلوجي، ومع تزايد تلك الجرائم وتوسعها، أضحى من المتوجب الخروج عن الإطار التقليدي للنظرة التقليدية الى الجريمة من جهة، وإلى التعاون الدولي في مجال مكافحة الجريمة من جهة أخرى.

وعلى الرغم من أن الإرهاب الإلكتروني يختلف عن صور الإرهاب التقليدية، كما ويعد واحداً من التهديدات الكبيرة لأمن المجتمع الدولي، إلا أن التحليل القانوني لمواجهته الدولية يعتمد على الإطار القانوني لمواجهة الإرهاب والجرائم التكنولوجية عموماً، كما أن هذا الإطار القانوني وخاصة معظم الاتفاقيات ذات الصلة في مجال مكافحة الإرهاب، صيغت في وقت كان الإرهاب الإلكتروني فيه يعد مجرد خيال علمي. من هنا تطرح جملة تساؤلات، تشكل الموضوع الذي تجرى مناقشته في هذا البحث، منها : ما هو الأرهاب الألكتروني؟ وما هي خصائصه المميزة؟ وبماذا تنحصر خطورته؟ وما هي أنواعه؟ وكيف يواجه المجتمع الدولي الإرهاب الإلكتروني، حالياً، وفي المستقبل؟ وهل هناك إطار قانوني دولي لمواجهة هذا النوع المستحدث من الإرهاب؟ وما هي صور التعاون الدولي المعتمدة في مواجهة الارهاب الالكتروني؟ وكيف يمكن

تطويرها؟ هذه التساؤلات وغيرها تبين كذلك أهمية موضوع البحث، بوصفه أحد المواضيع الجديرة بإهتمام الباحثين والبحث فيه.

ويتمثل الهدف من هذا البحث في تقديم تصور عام عن مفهوم الإرهاب الإلكتروني وبيان أشكال التعاون الدولي وآلياته للتصدي لهذه الجريمة بأبعادها المختلفة وملاحقة مرتكبيها ومعاقبتهم، وكذلك مدى الحاجة إلى إطار قانوني دولي متماسك، لمواجهة الجريمة موضوع الدراسة من خلال التعاون الدولي على المستويين الدولي والإقليمي. وتحقيقاً لذلك نحدد نطاق البحث بدراسة التعاون الدولي في مواجهة الإرهاب الإلكتروني على المستويين الدولي والإقليمي، دون التطرق الى المواجهة الداخلية للدول في هذا المجال.

ولغرض دراسة موضوع البحث سيعتمد المنهج التحليلي لدراسة الإتفاقيات الدولية والإقليمية ذات الصلة بالإرهاب الإلكتروني، وذلك وفق خطة بحث مكونة من مبحثين، نخصص أولهما لبيان ماهية الإرهاب الإلكتروني، ونوضح في ثانيهما صور التعاون الدولي في مواجهة الإرهاب الإلكتروني.

المبحث الأول
ماهية الإرهاب الإلكتروني

لقد أتاحت التطورات التكنولوجية المعاصرة الكثير من الفرص لاستخدام التقنية الذكية في مختلف مناحي الحياة الاجتماعية، الا أن هذه التطورات ذاتها باتت أسلحة (عصرية) للتنظيمات الارهابية، فمن نتائجها أنها أدت الى ظهور أنواع جديدة من الاجرام المعاصر المرتبط بالارهاب من جهة والمعلوماتية من جهة ثانية، تطلق عليها اصطلاحاً تسمية (الإرهاب الإلكتروني)، وقد تعددت في السنوات الأخيرة أنواعه، وازدادت خطورته. ولتوضيح مفهوم الارهاب الالكتروني، وبيان خصائصه وأنواعه وخطورته، سنوزع هذا المبحث على مطلبين، نتناول بالبحث في المطلب الأول مفهوم الإرهاب الإلكتروني، ونخصص المطلب الثاني لبيان خطورة الإرهاب الإلكتروني وأنواعه.

المطلب الأول

مفهوم الإرهاب الإلكتروني

من أجل الوقوف عند مفهوم الإرهاب الإلكتروني، سوف نقسم هذا المطلب إلى فرعين، نبين في الفرع الأول تعريف الإرهاب الإلكتروني ، ومن ثم نتناول في الفرع الثاني خصائص الإرهاب الإلكتروني.

الفرع الأول

تعريف الإرهاب الإلكتروني

إن مصطلح (الإرهاب الإلكتروني) يتكون من عبارتي: (الالكتروني) و (الإرهاب)، وعبارة (الالكتروني) في مجال مكافحة الإرهاب تشير إلى الفضاء السيبراني. وهو مصطلح يضاف الى عدد من المصطلحات الأخرى بشأن القضايا في مجال الأمن السيبراني، بما في ذلك على سبيل المثال لا الحصر: الجرائم السيبرانية، والحرب السيبرانية، والتسلل السيبراني، وبالطبع الإرهاب السيبراني. والفضاء السيبراني، على عكس الإرهاب، وهو مصطلح متفق عليه عموماً [1].

وفي سياق تعريف الإرهاب الإلكتروني، لابد من تعريف الإرهاب، وعلى الرغم من ان تعريف الإرهاب بشكل عام مايزال حتى يومنا هذا مشكلة كبرى تواجه المجتمع الدولي، ومن أجل توضيح مفهوم الإرهاب الإلكتروني، ومحاولة تطبيق تعريف الإرهاب على الإرهاب الإلكتروني نقوم ببيا ن تعريف الإرهاب عموماً كما ورد في المادة الأولى الفقرة(٢) من الاتفاقية العربية لمكافحة الإرهاب الصادرة في القاهرة عام ١٩٩٨م بأنه" كل فعل من أفعال العنف او التهديد أياً كانت بواعثه وأغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس، أو ترويعهم بإيذائهم، أو تعريض حياتهم أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو اختلاسها أو الاستيلاء عليها

[1] Chuipka, A. (2016), The Strategies of Cyberterrorism-is cybertwrrorism an effective means to Achieving the Goals if Terrorists?, Affaires publiques et internationales - Mémoires / Public and International Affairs - Research Papers. p. 5-6., Retrieved from http://hdl.handle.net/10393/35695، last visite 27L12L2017.

أو تعريض أحد الموارد الوطنية للخطر"[١]. وبشكل عام يمكن القول بأن مصطلح "الإرهاب" المتمثل في الاستخدام غير المشروع للقوة أو العنف ضد الأشخاص، من أجل تخويف حكومة أو مواطنيها والتي قد تكون لتحقيق أهداف سياسية أو احتيالية، وبمساعدة التكنلوجيا تحول الإرهاب من الشكل التقليدي إلى الشكل السيبراني للإرهاب، المعروف باسم الإرهاب الإلكتروني[٢]، الذي يعد واحداً من أحدث أشكال الإرهاب[٣]. هذا وقد أطلقت على هذا النوع من الإرهاب مسميات عدة منها (الإرهاب التقني) الذي يعرف بأنه" العدوان أو التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الالكترونية والصادر من دول أو جماعات أو أفراد على الإنسان"، و(الإرهاب المعلوماتي) والمستخدم في وسائل الاتصالات الحديثة والانترنت لنشر المعلومات والأفكار التي تتنافى مع القيم والمبادئ التي يرتكز عليها المجتمع الدولي[٤].

لقد صاغ مصطلح "الإرهاب الإلكتروني "CyberTerrorism" في الثمانينات باري كولين (Barry Collin)، الذي أشار إلى اندماج العالم المادي والظاهري فيما يتعلق ببعض جوانب الإرهاب. وانتشر هذا المصطلح على نطاق واسع وبسرعة منذ إنشائه، من جانب القانونيين، والأكاديميين ووسائل الإعلام، باستخدامه للإشارة إلى حالات مختلفة وليس دائماً بطريقة دقيقة. على سبيل المثال، اعتبرت الهجمات على البنية التحتية لتكنلوجيا المعلومات والتسلط عبر الإنترنت (online bullying) إرهاباً عبر الإنترنت، في حين أن الأخيرة ربما ينبغي تعريفها بشكل صحيح على أنها جرائم الكترونية. والاختلاف عادة ما ينبع من حقيقة أن الأساليب التي

---

[١] الموضوع الذي نحن بصدده ليس الإرهاب بمفهومه التقليدي، وإنما الإرهاب الإلكتروني، وايرادنا لتعريف الارهاب التقليدي لم يكن إلا من باب توضيح مفهوم الإرهاب. انظر نص الاتفاقية على الموقع الإلكتروني (تأريخ الزيارة ٢٠١٨/٥/٢٦):

: http://www.madcour.com/LawsDocuments/LDOC-44-635278203054882024.pdf

[2] Samuel, K. O., (2014), cyber terrorism attack of the contemporary information technology age: issues, consequences and panacea, International Journal of Computer Science and Mobile Computing, 3(5), pg.1082 – 1090, 2320–088X, p. 1083.

[٣] د. محمد محمد الألفي، تشريعات الإرهاب الإلكتروني والافتراضي، الملتقى القضائي الأول (جرائم الإرهاب وأمن الدولة)، القاهرة، ٢٨-٢٠١٠/٦/٣٠، ص١٥-١٦.

[٤] د. حسن تركي عمير، وسلام جاسم عبدالله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى، ص٣٢٨.

يستخدمها مجرمو الإنترنت والإرهابيون السيبرانيون يمكن أن تكون هي نفسها، على الرغم من أن الأهداف قد تكون مختلفة[١].

ويعد مصطلح (الإرهاب الإلكتروني) مصطلحاً مثيراً للجدل وهناك حاجة إلى اتفاق بشأن تعريف مشترك له بين الدول، بيد أن المجتمع الدولي لم يتمكن حتى الآن من النجاح في وضع تعريف شامل مقبول عموماً "للإرهاب" نفسه[٢]. والإرهاب الإلكتروني عادة ما يكون مسألة تثار في إطار مناقشة الإرهاب[٣]. وقد تم بالفعل تحديد أكثر من مائة تعريف مختلف للإرهاب الإلكتروني[٤]. وتوفر الطبيعة المتعددة الوظائف للتكنلوجيات السيبرانية مجالاً لتعريف (الإرهاب الإلكتروني) بشكل ضيق وعلى نطاق واسع. فالدول التي تشعر بالقلق إزاء العواقب السياسية المحلية المترتبة على الوصول إلى الإنترنت تميل إلى تفضيل تعاريف واسعة النطاق للإرهاب الإلكتروني. وعلى العكس من ذلك، فإن شرعية العديد من الأنشطة السيبرانية تدعم تعريف الإرهاب الإلكتروني على نحو ضيق، فالهجمات الإرهابية التي ترتكب من خلال تكنلوجيا المعلومات والاتصالات، ونشر الدعايات الارهابية ودعوة الناس الى التطرف الديني من خلال وسائل التواصل الاجتماعي من قبل المنظمات الإرهابية، ومنها ما يسمى بتنظيم الدولة الإسلامية (داعش)[٥]، على سبيل المثال، هي أشكال من الإرهاب الإلكتروني يمكن أن تنطبق عليها هذه

---

(1) Riglietti, G. (2016), Defining the threat:what cyber terrorism means today and what it could mean tomorrow, The Business Continuity Institute Reading, United Kingdom، The Business and Management Review, 8 (3), supra note 1, at 2, p. 12.

(٢) Dogrul, M. , Aslan, A.,& Celik, E. (2011), Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.), CCD COE Publications, p. 29.

(٣) Akati-Udi, T. (2015), Combating the growing threat of cyber terrorism, Special Conference 2 on International Cooperation, Model United Nations International School of The Hague | XXV Annual Session p.7.

(٤) Brunst , P. W. (2010), Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet, Max Planck Institute for Foreign and International Criminal Law, Freiburg , Germany ,Springer Science, Business Media, P.51.

(٥) يعتبر تنظيم "الدولة الإسلامية" في العراق والشام- المعروف اختصاراً بـ "داعش" (ISIL)، تنظيماً مسلحاً يوصف بالإرهاب يهدف أعضاؤه-حسب اعتقادهم- إلى إعادة الخلافة الإسلامية وتطبيق الشريعة" من خلال الدولة التي تتشكل حديثاً. انظر د.سامر أبو رمان، داعش (تنظيم الدولة) في عيون الشعوب، ب. دار النشر ومكانها وتأريخه، ص١٠-١١.

التعاريف الضيقة والواسعة، حيث يمكن لدعايات تنظيم الدولة الإسلامية أن تروع المدنيين من خلال نشر الخوف من خلال أشرطة الفيديو الخاصة بالإعدام، والتحريض على العنف الإرهابي عن طريق تطرف الناس، واستلهام الدعم من خلال تصور الجهود لبناء دولة الخلافة[١].

وقد عرف مكتب التحقيقات الفدرالية (FBI) الإرهاب الإلكتروني، بأنه أي "هجوم متعمد بدوافع سياسية ضد المعلومات ونظم الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى العنف ضد الأهداف غير المقاتلة من قبل مجموعات دون وطنية أو عملاء سريين[٢]. وعرفه مكتب الأمن التابع لمنظمة حلف شمال الأطلسي- (الناتو) بأنه "هجوم سيبراني يستخدم أو يستغل شبكات الحاسوب أو الاتصالات لتسبب تدميراً أو تعطيلاً كافياً لتوليد الخوف أو تخويف المجتمع لتحقيق هدف أيديولوجي"[٣].

في حين طرحت وزارة الدفاع الأمريكية تعريفاً للإرهاب الإلكتروني بأنه" عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الإتصالات ينتج عنه عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الإرتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة"[٤]. كما قدم البروفيسور دوروثي دينينج (Dorothy Denning) تعريفاً مشابهاً للإرهاب الإلكتروني في العديد من المقالات والمقابلات، كما عرضه أمام لجنة خدمات القوات المسلحة في الكونغرس الأمريكي، إذ عرف الإرهاب الإلكتروني بأنه " يعني الهجمات غير المشروعة والتهديدات بالهجوم على أجهزة الكمبيوتر والشبكات، والمعلومات المخزنة فيها عند القيام به لتخويف أو إرغام حكومة أو شعبها على تعزيز الأهداف السياسية أو الاجتماعية. علاوة على ذلك، يجب أن يؤدي الهجوم إلى العنف ضد

---

(1)Fidler, D. P. (2016), Cyberspace, Terrorism and International Law, Journal of Conflict & Security Law, 21(3), Oxford University Press.pp 475-493, P. 478.

(2) Alford, L. C. L.(2017), The Department of Defense effort to countering the cyberterrorism threat:Is the threat real or hyperbole? (Master's Thesis), 21-04-2017, National Defense University Joint Forces Staff College Joint Advanced Warfighting School, p.14.

(3) NATO Advanced Research Workshop (ARW) on the topic "Responses to Cyber Terrorism".NATO Science for Peace and Security Series: Human and Societal Dynamics, (2008), Volume 34, Centre of Excellence - Defence Against Terrorism(Ed)(3rd ed., 164 pp).hardcover, IOS Press, Ankara, Turkey, p.7.

(٤) عادل عبدالصادق، الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩، ص١١٢.

الأشخاص أو الممتلكات، أو على الأقل يسبب ضرراً كافياً لتوليد الخوف"[١]. ووفقاً لهذا التعريف، فإن معظم الأنشطة الإرهابية المعاصرة لا تندرج ضمن هذه الفئة، وكان هذا الوصف قد يكون دقيقاً في أوائل العقد الأول من القرن الحادي والعشرين، فقد تطور مفهوم الإرهاب الإلكتروني على مر السنين. وعليه غيّر مكتب التحقيقات الفيدرالي (FBI) نفسه صياغة تعريفه للإرهاب الإلكتروني عدة مرات، واليوم يعتمد المكتب التعاريف التي تتبنى أنشطة أكبر من مجرد استهداف البنية التحتية لتكنلوجيا المعلومات. ومنها على سبيل المثال، تعريف مركز الدراسات الاستراتيجية والدولية، الذي يعرف الإرهاب الإلكتروني بأنه "تخويف المؤسسات المدنية من خلال استخدام التكنلوجيا العالية لتحقيق أهداف سياسية أو دينية أو أيديولوجية، أو أعمال تؤدي إلى تعطيل أو حذف بيانات أو معلومات البنية التحتية الحيوية"[٢].

وعرف بعض الفقهاء الإرهاب الإلكتروني بأنه"خرق للقانون يقدم عليه فرد من الأفراد، أو تنظيم جماعي، بهدف إثارة اضطراب خطير في النظام العام، عن طريق شبكة المعلومات العالمية الانترنت"[٣].

ويرى جانب من الفقهاء الإرهاب الإلكتروني بأنه "العدوان أو التخويف او التهديد مادياً ومعنوياً باستخدام الوسائل الإلكترونية الصادرة من الدول، أو الجماعات، أو الأفراد على الإنسان في دينه أو نفسه أو عقله أو ماله بغير حق بشتى صنوف وصور الإفساد في الأرض".[٤]

في حين عرفه آخرون بأنه" الاستخدام العدائي والعدواني للأنترنت، بهدف ترويع الحكومة والمدنيين، أو قسم منهم، في إطار السعي إلى تحقيق أهداف سياسية أو اجتماعية"[٥].

بينما يذهب البعض الآخر إلى تعريفه بأنه " الأعمال التي تمس حقوق الإنسان وحرياته الأساسية، أو تهدد هذه الحقوق والحريات بالضرر، بصرف النظر عن الدوافع والأهداف ومكان اقتراف العمل الإرهابي، أو موقف التشريعات الوطنية"[١].

---

[1] Dogrul and other, supra note 1 at 4, p.8.

[2] Riglietti, supra note 5 at 3, p. 13.

[٣] محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، مطبعة جامعة الملك فهد، الرياض، ١٤٢٣هـ ص١١.

[٤] د.محمد عوض الترتوري ود. اغادير عرفات جويحان، علم الإرهاب (الأسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب)، دار الحامد، عمان، ٢٠٠٦، ص٣٢٧.

[٥] د. ذياب البداينة، جرائم الحاسب الدولية، بحث مقدم إلى أكاديمية نايف للعلوم الأمنية، الرياض، ١٩٩٨، ص٢٢.

كما ذهب البعض الآخر في تعريفه إلى أنه" الاستخدام غير الأمثل للشبكة العالمية، بما يؤدي إلى ترويع المواطنين بشكل خطر، أو يسعى إلى زعزعة الأمن والاستقرار، أو تقويض المؤسسات السياسية، أو الدستورية، أو الاقتصادية، أو الاجتماعية، لإحدى الدول، أو المنظمات الدولية، عن طريق استعمال لغة التهديد والعدوان".[٢]

وعرفه آخرون بأنه:" العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد. فالإرهاب الإلكروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من اجل تخويف وترويع الآخرين، وإلحاق الضرر بهم، أو تهديدهم. [٣]

وبدورنا لسنا بصدد إيراد تعريف للإرهاب الإلكتروني، وذلك لأنه عندما يتعلق الأمر بتعريف الإرهاب الإلكتروني، فأن هناك مجالين أساسيين يتطلبان التوضيح، أحدهما، أن تعريف الإرهاب الإلكتروني يعد إمتداداً لتعريف الإرهاب التقليدي، على الرغم من الاختلاف بين النوعين من الإرهاب (التقليدي والإلكتروني) أما بسبب الوسيلة المستخدمة في ارتكاب الإرهاب الإلكتروني لتحقيق الغرض الإرهابي، أو لحداثة الإرهاب الإلكتروني وافتقاره الى التعريف التشريعي، بحيث لم تتصدَ له التشريعات إلا نادراً، هذا ما سنوضحه عند تناول التعاون التشريعي لمواجهته. فبهذا الوصف يعد الإرهاب الإلكتروني مرحلة تالية من تطور الإرهاب. وثانيهما، ومن التعريفات السابقة، نستطيع القول بأن الإرهاب الإلكتروني يظهر نتيجة للتقارب بين الإرهاب المادي وتطوير تكنلوجيا المعلومات والاتصالات، وهو استخدام التكنلوجيا والفضاء السيبراني لإطلاق هجوم على البنية التحتية القيمة التي يعتمد عليها وجود المنظمات والأمم تماماً.

وبالرجوع الى التعاريف المبينة أعلاه، من الممكن التوصل الى استنتاجات مهمة، ومنها:

---

[١] د. حسنين المحمدي بوادي، الإرهاب الإلكتروني بين التجريم والمكافحة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥، ص٢٧-٢٨.

[٢] محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، الرياض، ١٤٢٢، ص٢٢.

[٣] عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول (حماية أمن المعلومات والخصوصية في قانون الإنترنت)، القاهرة، ٢ - ٤ يونيو ٢٠٠٨. متاح على الموقع الإلكتروني (تاريخ الزيارة ٢٠١٧/١٢/٢٥) http://www.shaimaaatalla.com/vb/showthread.php?t=3937.

إنه لا يوجد حتى الآن تعريف دولي موحد للإرهاب بصفة عامة، والإرهابِ الإلكتروني بصفة خاصة، ويرجع ذلك إلى تنوع أشكاله ومظاهره، وتعدد أساليبه وأنماطه، واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله. فما يراه البعض عملاً إرهابياً، يراه الآخر عملاً مشروعاً، ولذلك ما يزال تعريف الإرهاب حتى يومنا هذا مشكلة كبرى تواجه الباحثين القانونيين والسياسيين.

كما وضحت التعاريف بأن "هناك تمييزاً واضحاً بين وجهين مختلفين لاستخدام الإرهابيين لتكنلوجيا المعلومات (أي الإرهاب الذي يمارس بواسطة تقنية المعلومات) واستخدام الإرهابيين للحواسيب كوسيط لأنشطتهم (أي الإرهاب الذي ينطوي على تكنلوجيا الحاسوب كسلاح أو هدف). إلا أنها لم تفرق بين نوع المعلومات، فيما إذا كانت المعلومات خاصة بالأفراد الشخصية المتمثلة بالبيانات وأرقام بطاقات الإئتمان، أو كانت المعلومات تعود إلى المؤسسات الحساسة في الدولة. وفيما يتعلق بالتمييز بين استخدام الإرهابيين لتكنلوجيا المعلومات والإرهاب، بما في ذلك تكنلوجيا الحواسيب كسلاح / هدف، فإن هذه الأخيرة فقط يمكن وصفها بأنها مكافحة للإرهاب الإلكتروني. في حين إن استخدام الإرهابيين للحواسيب كوسيط لأنشطتهم، سواء لأغراض الدعاية أو التواصل أو لأغراض أخرى، هو ببساطة ما يطلق عليه مصطلح الاستخدام.

كما ويتضح بأن الفقه لم يتفق على تعريف موحد للإرهاب الإلكتروني، ولذلك جاءت المفاهيم متباينة باختلاف زوايا النظر التي يأخذ بها كل باحث، وركزت غالبية الفقه على دراسة الظاهرة من خلال وجهة نظر علم الإجرام لبيان أسبابها وأشكالها المختلفة ونتائجها، حيث يركز كل تعريف من التعاريف السابقة على خاصية من خواصها، ويتخذه محوراً يُبنى عليه التعريف المختار. هذا من ناحية، كما ويلاحظ مما تقدم أن للفقه دوراً كبيراً في تعريف الإرهاب الإلكتري خاصة في ظل تأخر الإجماع الدولي على تعريفها. وهناك اتفاق بينهم على أن مصطلح (الإرهاب الالكتروني) يمكن أن يطلق على إحدى الصور المعاصرة للارهاب، الذي تقوم به التنظيمات الارهابية، والذي يستهدف تحقيق أهداف الارهاب التقليدي، وذلك باستخدام تكنلوجيا المعلومات، ويجب أن يكون للهجمات الإلكترونية مكون "إرهابي" لكي يطلق عليها مصطلح (الإرهاب الإلكتروني). وأن ترتكب الهجمات الإرهابية بحيث تؤدي إلى (الوفاة و / أو التدمير الواسع النطاق)، ويجب أن تكون لها دوافع سياسية. هذا يعني إن الأرهاب الالكتروني له بعد معنوي يرمي إلى التحريض على بث الكراهية الدينية وحرب الأفكار.

الفرع الثاني
خصائص الإرهاب الإلكتروني

إن الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي يختص بها دون سواه، وتحول دون اختلاطه بالإرهاب التقليدي، وعليه سنحاول حصر أهم خصائص الإرهاب الإلكتروني كما يأتي:

أولاً: سهولة ارتكابه: إن الإرهاب الإلكتروني لا يحتاج في ارتكابه إلى العنف المادي والقوة المادية، بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، لأن الحاسب الآلي في هذه الجرائم هو أداة ارتكابها، حيث أن بدونه لايمكن الدخول على شبكة الإنترنت، والتمكن من القيام بالفعل الذي يشكل إرهاباً.[١]

ثانياً: عالمية الجرائم الإرهابية: يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود[٢]. ومن خصائص الارهاب الالكتروني كذلك انتماء الإرهابيين الإلكترونيين الى جهات غير حكومية أو حكومية، فالجهات غير الحكومية موجودة كعناصر أو منظمات تعمل خارج نظام الدولة، على الرغم من أنها غالباً ما تعيش أو تقيم داخل حدود الدولة. وعلى النقيض من ذلك، فإن العناصر الإرهابية التي ترعاها الدولة من المحتمل أن تقيم داخل حدودها وتقتصر على دولة معينة وعادة ما تحصل على الموارد سراً وأحياناً علناً للقيام بأعمال إرهابية تهدف إلى التأثير على نتائج الأحداث على صعيد دولة ما أو على صعيد العالم [٣].

ثالثاً: تعدد أنواع وأشكال الإرهاب الإلكتروني الذي يستخدم من خلال التقنيات الحديثة[٤]، ومنها على سبيل المثال إنشاء المواقع الإرهابية على شبكة المعلومات العالمية لنشر الأفكار

---

[١] إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الألكتروني(دراسة مقارنة)، رسالة ماجستير، كلية الحقوق ، جامعة النهرين ، ٢٠١٢، ص ٣٨.

[٢] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة علمية مقدمة إلى الملتقى العلمي بعنوان "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، خلال الفترة من ٢-٢٠١٤/٩/٤، كلية العلوم الإستراتيجية، ص١١.

[٣] Alford, supra note 6, at 4, p2.

[٤] د. حسن تركي عمير، سلام جاسم عبدالله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مصدر سابق، ص٣٤٠.

الإرهابية، حيث وجد العديد من المواقع التي تعلم كيفية صناعة المتفجرات، واختراق البريد الإلكتروني، وطرق نشر الفايروسات[١].

رابعاً: صعوبة المقاضاة والإثبات في الإرهاب الالكروني: الإرهاب الإلكتروني يتسم بالغموض والضبابية، لدرجة يصعب معها التحري عنها والتحقيق فيها، والمقاضاة في نطاقها والذي ينطوي على الكثير من المشكلات والتحديات القانونية والأدارية، والتي تتعلق منذ البداية، من عملية ملاحقة الجناة، حتى ولو تحققت إمكانية الملاحقة، اصبحت الأدلة صعبة، وذلك لسهولة إتلافها أو لصعوبة الوصول إليها[٢]. فالجرائم التي تعتمد في موضوعها على التشفير، والأكواد السرية، والنبضات والأرقام يصعب أن تخلف وراءها آثاراً مرئية تكشف عنها أو يستدل من خلالها على الجناة، وهذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الالكترونية، تلقي بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية[٣]. أما بخصوص الإثبات، فقد تحظى قواعد الإجراءات الجنائية بشأن جرائم الكومبيوتر بأهمية خاصة باعتبار أن وسائل إثباتها قد تخرج عن القواعد العامة التقليدية في الإثبات، ومنذ نهاية السبعينات ومطلع الثمانينات كانت تثار في الإطار القانوني التساؤلات بشأن حجية مستخرجات الكومبيوتر، ومشكلات الإثبات بواسطة ما نمات الكومبيوتر، والبيانات المخزنة فيه أياً كانت صورة هذه البيانات، وقد شهدت أوروبا تحديداً نشاطاً محموماً في هذا الحقل، انطلق مع منتصف الثمانينات، وانصب على البحث في تطوير قواعد الإثبات، وأصول المحاكمات في المواد المدنية والتجارية لاستيعاب التوظيف المتنامي لأنظمة الكومبيوتر والاعتماد المتزايد عليها، وما ينشأ عن ذلك من كثرة اللجوء لسجلات الكومبيوتر، وملفات البيانات المخزّنة للاحتجاج بها، ليس فقط تلك المخزّنة في نظم المعلومات، بل سجلات وبيانات شبكات الاتصالات الخاصة، كبيانات شبكة سويفت وغيرها الخاصة بالعمل المصرفي، وبيانات أنظمة الشحن البحري الإلكترونية التي أخذت في الاتساع والنماء، وبيانات سجلات الشبكات الاتصالية المختلفة، لكن هذه البدايات ما لبثت أن أخذت منحّى مختلفاً تماماً مع دخول الانترنت في مطلع التسعينات الاستخدام التجاري الواسع،

---

[١] تغريد سامي إبراهيم الطائي، جرائم الإرهاب الالكتروني وآليات مكافحتها (دراسة تحليلية)، رسالة ماجستير، سكول القانون والسياسة، جامعة دهوك، ٢٠١٠، ص١٨.

[٢] د. يوسف حسن يوسف، الجرائم الدولية للأنترنت، ط١، المركز القومي للأصدارات القانونية، القاهرة، ٢٠١١، ص٢٨٥.

[٣] فهد سلطان محمد أحمد بن سليمان، مواجهة جرائم الإنترنت دراسة مقارنة، رسالة ماجستير ، كلية الحقوق، جامعة القاهرة، ٢٠٠٤، ص٣٧-٣٨.

إذ مع الاتجاه إلى ا لتشبيك أو بناء شبكات المعلومات على نحوٍ واسعٍ، والتحول من أنماط العمل الإلكتروني؛ أصبح الأمر أكثر من مجرد حجية مستخرجات نظم الكومبيوتر وشبكات الاتصال، بل أصبح من مسائل التعاقدات ووسائل إثباتها في بيئة الشبكات والنظم الإلكترونية[١].

خامساً: إن مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات[٢]. ولهذا يصنف الفقهاء هذه الجرائم ضمن جرائم اصحاب الياقات البيضاء، وعند إجراء التحقيق في هذه الجرائم أول ما يبحث ويتحرى عنه المحققون هو الخبراء في مجال إستخدام الحاسب الآلي؛ لأن معظم الإرهابيين الذين يمارسون أنشطتهم على الأنظمة المعلوماتية أو بواسطتها هم من الخبراء في هذا المجال[٣].على سبيل المثال تقوم الجماعات الإرهابية مثل تنظيم الدولة الإسلامية في العراق وسوريا بتجنيد أشخاص يتمتعون بمهارات إلكترونية متقدمة للعمل ضمن هيكل القيادة المركزية. وتسهل هذه التقنية التشغيلية ثلاثة إجراءات رئيسة هي: القيادة والتحكم وجها لوجه وتقييم المواهب الإلكترونية، وتبسيط عملية إتخاذ القرار[٤].

سادساً: الانتهاك الخطير بالنظام العام وزعزعة استقرار الدولة، وتعد هذه الخاصية عامة بالنسبة لصور الارهاب كافة، التقليدية والمستحدثة، فالهدف من الأعمال الارهابية هو ترويع المجتمع والمساس بهيبة الدولة ونظامها السياسي والاجتماعي، وفرض التنظيمات الارهابية مطالبها وشروطها على الدولة ومؤسساتها المختلفة وعلى أفراد المجتمع. وهذه الخاصية تعد أساساً لتمييز الارهاب عما يماثله من أنشطة الكترونية غير مشروعة، مثل الدخول غير المشروع الى المواقع الالكترونية لمؤسسات الدولة (القرصنة) أو اختراق مواقع البريد الالكتروني، أو ما شابه.[٥]

---

[١] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، مصدر سابق ص١٩-٢٠.

[٢] عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مصدر سابق.

[٣] عمرو عيسى الفقي، الجرائم المعلوماتية (جرائم الحاسب الآلي والانترنت في مصر والدول العربية)، المكتب الجامعي الحديث، الإسكندرية، ٢٠٠٦، ص٨٦ .

[٤] Alford, supra note 6 at 4, p2.

[٥] عبدالمجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الارهاب المعلوماتي، الدورة التدريبية الخاصة بمكافحة الجرائم الارهابية المعلوماتية، القنيطرة، المغرب، ٩-٢٠٠٦/٤/١٣، ص ٩-١١، متاح على الموقع الالكتروني (تأريخ الزيارة ٢٠١٨/٢/٦):https://repository.nauss.edu.sa/handle/123456789/57450

سابعاً: انه الإرهاب الوحيد الذي يمكن أن يرتكبه أكثر من شخص في وقت واحد دون التأثر بمكان العمليات الإرهابية، فقرصنة موقع ما من قبل شخص في العراق يمكن أن يتزامن مع عمل شخص آخر في اليابان مثلاً وآخر في بلد ثالث دون أي تأثير للمكان المستهدف[١].

ثامناً: ضمان استمرارية النشاط الارهابي، إذ أن استخدام النظم المعلوماتية كوسيلة مستحدثة في النشاط الارهابي يعد عاملاً في استمراريته، فالمواجهة مع الارهابي الالكتروني هي مواجهة غير مباشرة، كما هو الحال في العمليات الارهابية التقليدية، التي تنتهي عادة بمقتل أو انتحار الارهابيين، فالعمليات في ظل الارهاب الالكتروني تبقى مستمرة وذلك لخصائصه الأخرى المتمثلة في تشتت المواقع الالكترونية الارهابية في مختلف انحاء العالم، وصعوبة مكافحة الارهاب الالكتروني للمعوقات المتعلقة بالاهتداء الى الفاعلين وضمان أدلة الاثبات والتعاون بين الدول، وغير ذلك.[٢]

المطلب الثاني

خطورة الإرهاب الإلكتروني وأنواعه

نوزع هذا المطلب على فرعين ، نبين في الفرع الأول خطورة الإرهاب الإلكتروني ، ونوضح في الفرع الثاني أنواعه، وكما يأتي:

الفرع الأول

خطورة الإرهاب الإلكتروني

إن الإرهاب الإلكتروني يهدف إلى تحقيق جملة من الأهداف غير المشروعة ، التي من أبرزها:

١. نشر الخوف والرعب بين الأشخاص والدول والشعوب
٢. الإخلال بالنظام العام، والمن المعلوماتي، وزعزعة الطمأنينة.
٣. تعريض سلامة المجتمع وأمنه للخطر
٤. إلحاق الضرر بالبنى المعلوماتية الأساسة وتدميرها، ولإضرار بوسائل الاتصالات والتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة.

---

(١) د. حسن تركي عمير، وسلام جاسم عبدالله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مصدر سابق، ص٣٣٩.

(٢) عبدالمجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الارهاب المعلوماتي، الدورة التدريبية الخاصة بمكافحة الجرائم الارهابية المعلوماتية، مصدر سابق، ص٩-١١.

٥. الانتقام من الخصوم

٦. الدعاية والإعلان، وجذب الانتباه، وإثارة الرأي العام

٧. التعبئة وتجنيد إرهابيين جدد، إن استقدام عناصر جديدة داخل المنظمات الإرهابية، يحافظ على بقائها واستمرارها، وهم يستغلون تعاطف الآخرين من مستخدمي الانترنت مع قضاياهم، ويجتذبون هؤلاء بعبارات براقة وحماسية من خلال غرف الدردشة الإلكترونية[١].

٨. إعطاء التعليمات والتلقين الإلكتروني: يمتلئ الانترنت بكم هائل من المواقع التي تحتوي على كتيبات وإرشادات تشرح طرق صنع القنابل، والأسلحة الكيمياوية الفتاكة.

٩. الحصول على التمويل: يستعين الإرهابيون بيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، في التعرف على الأشخاص ذوي القلوب الرحيمة ومن ثم استجداؤهم لدفع تبرعات مالية لأشخاص اعتباريين، يمثلون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة البريد الإلكتروني بطريقة ماكرة لايشك فيها المتبرع بأنه يساعد إحدى المنظمات الإرهابية[٢].

وفي ظل هذه الأهداف المتعددة الخطيرة على الدولة والمجتمع والأفراد يشكل الإرهاب أحد أخطر الظواهر الإجرامية التي عرفتها المجتمعات الحديثة، وذلك لما تمثله من تهديد خطير للفكر والعقيدة والكيان السياسي للشعوب، وبإتساع مفهومه أصبح من أبرز التهديدات الأمنية، لما له من تأثيرات بعيدة المدى والخطورة على البشرية جمعاء[٣]. والإرهاب الإلكتروني باعتباره من أبرز صور الجرائم الإلكترونية (المعلوماتية)، أصبح هاجساً 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 أضراراً جسيمة على الأفراد والمنظمات والدول[٤]. ففي عالم ما

---

[١] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، مصدر سابق، ص١٢-١٤.

[٢] عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، مصدر سابق.

[٣] د. عبد المحسن محمد احمد بدوي، دور برامج الإعلام في تنمية الوعي الأمني ومكافحة الإرهاب(المعوقات والتحديات)، ورقة عمل مقدمة ضمن أعمال الدورة التدريبية (الإرهاب والإعلام) بكلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، الفترة (٢٤-٢٠٠٩/١/٢٨)، ص٣.

[٤] د. أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، مصدر سابق، ص١١.

بعد الحاد ي عشر من سبتمبر، غالباً ما ربط الصحفيون والمسؤولون الحكوميـون خطـر الإرهـاب الإلكتروني بـ (القاعدة) وغيرها من المنظمات الإرهابية للحصول على أقصى قدر من التأثير، فعـلى سبيل المثال، كتـب (Lenzner and Vardi): "قبـل أربعـة أعـوام كـان تنظـيم القاعـدة يتلقـون دروساً في الطيران. واليوم يكتسبون مهارة جديدة، هي قرصنة المواقع" [١].

وقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابيـة إذ قامـت بتوظيـف طاقتهـا للاستفادة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة. وأصبح من الممكـن اخـتراق الأنظمـة والشـبكات المعلوماتيـة، واسـتخدامها في المسـاس بالبنيـة التحتيـة المعلوماتيـة لمرافـق الـدول الحيويـة والمؤسسـات العامـة والشركات الاقتصـادية الكـبرى، وبـات الارهاب الالكتروني خطـر يهـدد البنـى التحتيـة للأنظمـة والشـبكات المعلوماتيـة في العـالم كلـه، ويكمن الخطر، من جهة، في سهولة استخدام هذا السـلاح الرقمـي، ومـن جهـة ثانيـة، في أضراره البالغة والشاملة، ومن جهة ثالثة، في بقاء مستخدمه بعمله الإرهـابي بعيـداً عـن أنظـار السـلطة والمجتمع.

إن خطورة الإرهاب الإلكتروني تزداد بشكل خاص في الدول المتقدمة إذ تدار بنيتها التحتيـة بالحواسيب الآلية والشـبكـ ات المعلوماتيـة، مـما يجعلهـا هـدفاً للارهـاب الالكـتروني، وبـدلاً مـن استخدام المتفجرات، كما هو جارٍ في الارهاب التقليدي، تستطيع الجماعات والمنظمات الإرهابيـة أن تستخدم الحواسيب الآلية لتدمير البنية المعلوماتية، وتحقيق آثار تفوق ما تحققه المتفجرات، حيث يمكن شن هجوم إرهابي الكتروني يؤدي الى إغلاق المواقع الحيوية وإلحـاق الشـلل بأنظمـة القيادة والسيطرة والاتصالات، أو قطع شـبكات الاتصـال بـين الوحـدات والقيـادات المركزيـة، أو تعطيل أنظمة الدفاع الجوي، أو إخـراج الصـواريخ عـن مسـارها، أو الـتحكم في خطـوط الملاحـة الجوية والبرية والبحرية، أو شل محطات إمداد الطاقة والماء، أو اختراق النظام المصرفي وإلحـاق الضرر بأعمال البنوك وأسواق المال العالمية [٢].

إن الإرهاب الإلكتروني هو اليوم أكثر أشكال التخريب الاجتماعـي والسـياسي شـيوعاً. فعـلى سـبيل المثـال، واجهـت إسـتونيا (Estonia) في أيـار / مـايو ٢٠٠٧ واحـدة مـن أكـبر الهجـمات

---

[١] Stohl, M. (2007), Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?, Crime Law Soc Change DOI 10.1007/s10611-007-9061-9, Business Media B.V., p. 2. &Springer Science

[٢] عبدالله بن عبدالعزيز بن فهد العجلان، الارهاب الالكتروني في عصر المعلومات، مصدر سابق.

السيبرانية التي شلت تماماً البنية التحتية لتكنلوجيا المعلومات الحكومية والمصرفين الاستونيين الرئيسيين[١].

وهكذا أصبح الفضاء الإلكتروني يستخدم سواء للقيام بعمل إرهابي أم المساعدة في القيام بعمل عسكري تقليدي، وهذا ما يعد انتهاكاً لمبدأ حظر استخدام القوة في العلاقات الدولية الوارد في المادة ٢ فقرة ٤ من ميثاق الأمم المتحدة والذي يتعامل مع التهديدات التقليدية ما يطرح ضرورة ملحة لإدماج التهديد الذي يمثله الإرهاب الإلكتروني ضمن تفسير هذه المادة باعتباره نوعاً من استخدام القوة في العلاقات الدو لية ويمثل تهديداً للسلم والأمن الدوليين[٢].

ووفقاً للبيانات المتعلقة بمؤشرات الإرهاب العالمي، فأن البلدان الأكثر تضرراً بالإرهاب كانت في السنوات الأخيرة: سوريا والعراق ونيجيريا وأفغانستان وباكستان. وكانت الجماعات الأكثر نشاطاً في المنطقة، من حيث الهجمات الإرهابية، هي تنظيم الدولة الإسلامية وبوكو حرام وطالبان ومقاتلو فولاني. ومن بين هذه المجموعات الأربع، يبدو أن طالبان وتنظيم الدولة الإسلامية هما الأكثر تقدماً من حيث استخدام شبكة الإنترنت[٣].

الفرع الثاني
أنواع الإرهـاب الإلكتروني

لقد تعددت أنواع الإرهاب الإلكتروني في المرحلة الراهنة وبالتالي إزادات خطورته وتعاظمت اضراره، ومن أجل التصدي له يكون من البديهي تحديد أنواعه، لوضع التدابير الكفيلة بمواجهة كل نوع على حدة ما يسهل عملية القضاء عليه، وارتباطاً بصعوبة الإحاطة بأنواعه كافة، رأينا ، في نطاق هذا الفرع ، توزيعها إلى مجموعتين ، المجموعة الأولى تضم جرائم الإرهاب الإلكتروني التي تمارس بواسطة النظام المعلوماتي، والمجموعة الثانية تشتمل على جرائم الإرهاب الإلكتروني الواقعة على النظام المعلوماتي، وسنبحث في كل منهما كما يأتي:

---

(1) Luca, G. (2017), Manifestations of contemporary terrorism: cyberterrorism-scientific review, research and science today, No. 1(13), p.23.

(٢) د.عادل عبدالصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩، ص٣٨١.

(3) Riglietti, supra note 5, at 3, p. 14.

أولاً: جرائم الإرهاب الإلكتروني التي تمارس بواسطة النظام المعلوماتي:

سنبحث بشيء من الإيجاز في جريمة انشاء المواقع الإلكترونية، وجريمة التهديد الإلكتروني، على اعتبار انهما جرائم الإرهاب الإلكتروني الأكثر شيوعاً، وكما يأتي:

(أ) جريمة انشاء المواقع الإلكترونية:

يعرف (الموقع) بأنه 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 WWW Browser ويقوم بحل رموز HTML وإصدار التعليمات لإظهار الصفحات المتكونة. ويقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل لتعليم 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، وطرق نشر الفيروسات وغير ذلك[1].

فإنشاء المواقع لتحقيق الأغراض غير المشروعة يعد في حكم جمعية أو هيئة أو مؤسسة، وإن كان هذا الإنشاء يقع في العالم الإفتراضي وليس الحقيقي، فالموقع الإفتراضي يتضمن العديد من الرسوم والتصاميم والأسماء والعلاقات المميزة لصاحب هذا الموقع كما يتضمن عنوان هذا الأخير الذي تتم مراسلته عليه[2]. وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً بالنسبة للإرهابيين، فإن إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات ، لخدمة أهدافهم وترويج أفكارهم الضالة أصبح سهلاً وممكناً، ولذا فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية، وهي بمثابة المقر الافتراضي لها. كما إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة، فإذا ظهر موقع

---

[1] رفد عيادة الهاشمي، الإرهاب الإلكتروني، ص١٠، متاح على الموقع الإلكتروني (تأريخ الزيارة ٢٠١٨/٥/٢٦): https://www.mizandz.com/2017/11/pdf.html

[2] د. عامر محمود الكسواني، التجارة عبر الحاسوب ماهيتها-اثباتها- وسائل حمايتها-القانون واجب التطبيق عليها في الأردن- مصر- دبي، دار الثقافة، عمان، ٢٠٠٩، ص١٤٩.

إرهابي فسرعان ما يغير نمطه الالكتروني غداً، ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف[١].

فالجماعات الإرهابية تدرك أهمية الانترنت من خلال ما يوفره من خدمات موثوق بها، وشروط مي سره، وهويات افتراضية. فـ (طالبان) على سبيل المثال، أخذت تدير موقعاً دعائياً لعملياتها العسكرية وتفجيراتها الانتحارية ضد القوات الأمريكية في أفغانستان، لأكثر من سنة، مع العلم بأن هذا الموقع الإلكتروني كان مملوكاً لشركة أمريكية في ولاية تكساس الأمريكية، وكانت تؤجر المواقع الإلكترونية بمبلغ ٧٠ دولاراً في الشهر، تدفع بواسطة بطاقة الإئتمان، وكانت تتعامل مع نحو ١٦ مليون حساب مستخدم[٢].

ومن الأمثلة على بعض المواقع الإلكترونية العربية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية، موقع (النداء) التابع لتنظيم (القاعدة)، الذي تم اكتشافه في عام ١٩٩٨، وهو الموقع الرسمي لتنظيم القاعدة بعد احداث الحادي عشر- من سبتمبر عام ٢٠٠١ ، ومن خلاله تصدر البيانات الإعلامية للقاعدة. كما أن التنظيم الإرهابي (داعش) لديه ٩٠ ألف صفحة باللغة العربية على موقع التواصل الاجتماعي و٤٠ أ لفاً بلغات أخرى، إضافة إلى موقعه الذ دشنه التنظيم بسبع لغات، وينشط هذا التنظيم والجماعات الإرهابية الأخرى في مواقع التواصل الاجتماعي لابتزاز الشباب عاطفياً ومادياً لضمهم إليه، أو تمويلهم[٣]. وفي عام ٢٠٠٣ نشر- (عبدالعزيز المقرن)، زعيم القاعدة في السعودية/جزيرة العرب، عدة مجلات رقمية، بما في ذلك (صوت الجهاد)، وفي عام ٢٠٠٥ نشر- (يوتيوب) على شبكة الإنترنت أكثر ٤٠٠٠ اتصال إلى الجماعات الإرهابية على شبكة الإنترنت[٤].

---

[١] محمد محمد الألفي، تشريعات مكافحة جرائم الإرهاب الإلكتروني" الأحكام الموضوعية والانماط"، ص٢٢. ورقة عمل متاحة على الموقع الإلكتروني:. http://www.jp.gov.eg/img/d2c88f10-171a-48d1-acbe-847ba5bf20de.pdf

[٢] الموقع الإلكتروني (تأريخ الزيارة ٢٠١٨/٥/٢٦):http://political-encyclopedia.org/dictionary

[٣] إيهاب شوقي، الإرهاب الإلكتروني وجرائمه، ٧ ديسمبر ٢٠١٥، متاح على الموقع الإلكتروني: http://www.anntv.tv/new/showsubject.aspx?id=121062

[٤] فراس رشيد، مكافحة تجنيد الإرهابيين عبر الإنترنت، ورقة عمل مقدمة الى "الحلقة العلمية في مكافحة الإرهاب جامعة نايف العربية للعلوم الأمنية، المملكة الأردنية الهاشمية، ٢٠١٢، ص٧.

(ب) جريمة التهديد الإلكتروني: المقصود بالتهديد: الوعيد بشر، وزرع الخوف في النفس وذلك بالضغط على إرا دة الإنسان وتخويفه من أن ضرراً ما سيلحقه أو سيلحق أشخاصاً أو أشياء له بها صلة. وقد يلجأ إرهابي الإرهاب الإلكتروني إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية، بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة التهديد، وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية. ولقد تعددت الأساليب الإرهابية في التهديد، فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية، في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية، ونحو ذلك[١].

ومن أمثلة التهديد الإلكتروني ما قام به شاب أمريكي يدعى (جاهابر جويل) البالغ ١٨ عاماً، حيث هدد كلاً من مدير شركة (مايكروسوفت) (ج) والمدير التنفيذي لشركة (M.P.I) بنسف شركتيهما إذا لم يتم دفع خمسة ملايين دولار، وقد قامت الشركة بتفتيش منزل المذكور بعد القبض عليه، وعثروا في حاسبه الآلي على ملفات رقمية عدة تحتوي على معلومات عن تصنيع القنابل تم إنزالها عبر الإنترنت[٢].

ثانياً : جرائم الإرهاب الإلكتروني الواقعة على النظام المعلوماتي

من أبرز الجرائم التي تضمها هذه المجموعة ما يأتي:

(أ) القصف الإلكتروني أو الإغراق بالرسائل: وهو أسلوب للهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، مايزيد الضغط على قدرتها على استقبال رسائل من المتعاملين معها، والذي يؤدي إلى وقف عملها[٣]. ويعرفه البعض الآخر بأنه إرسال كم هائل من الرسائل عبر البريد الإلكتروني لأجهزة الحاسب الآلي لمستخدم

---

[١] عبدالله بن عبدالعزيز بن فهد العجلان، الارهاب الالكتروني في عصر المعلومات، مصدر سابق.

[٢] د. هشام بشير،الإرهاب الإلكتروني في ظل ثورة المعلومات، مقال متاح على الموقع الإلكتروني (تأريخ الزيارة ٢٠١٨/٥/٢٥):

http://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-31&Itemid=294&option=com_content

[٣] د. هشام بشير،الإرهاب الإلكتروني في ظل ثورة المعلومات، مصدر سابق.

واحد أو للعديد من المستخدمين، والتي يراد تعطيلها وتوقفها عن العمل، ولا يشترط في تلك الرسائل أن تكون ذات محتوى معين، فقد تكون محملة بملفات كبيرة الحجم لمجرد التأثير على الجهاز نظراً لصغر المساحة المحددة للبريد الإلكتروني، والتي تصل لجهاز الحاسب الآلي مرة واحدة في وقت واحد تقريباً وتعمل على توقفه عن العمل على الفور، نظراً لما تسببه من ملئ منافذ الإتصال وكذلك قوائم الانتظار وبمجرد توقف تلك الأجهزة عن العمل تنقطع بالتالي الخدمة التي تؤديها[١]. وقد بدأت مثل هذه العملية عام ١٩٩٦ عندما أرسلت إحدى الشركات أعلانات عنها بالبريد الإلكتروني إلى الآلاف من مواقع الإنترنت، فتم تعطيل الشبكة فضلاً عن تكليف متلقي الرسائل ثمن مدة الإتصال اللازمة لإستقبالها مع ما يصاحبها من ملفات، وتجري حالياً محاولات من جانب نظم المعلومات لتطوير برامج تتعامل مع هذه الحالات بإستقبال جزء محدد من الرسائل عندما يحدث سيل مفاجئ منها حتى لا تنقطع الخدمة[٢].

(ب) تدمير أنظمة المعلومات: وهو محاولة اختراق شبكة المعلومات الخاصة بالأفراد أو الشركات العالمية بهدف تخريب نقطة الاتصال أو النظام عن طريق تخليق أنواع من الفيروسات الجديدة والتي تسبب كثيراً من الضرر لأجهزة الكمبيوتر والمعلومات التي تم تخزينها على هذه الأجهزة[٣].

(ت) التجسس الإلكتروني: التجسس هو التنصت وسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات، والتجسس على هذه المعلومات، أياً كان نوعها، يأخذ أبعاداً جديدة، فتعددت أهدافها من معلومات اقتصادية إلى معلومات سياسية وعسكرية وشخصية[٤]. ويقوم الارهابيون المبرمجون الذين يسمون بـ(الهاكرز أو قراصنة الحاسوب) باختراق المواقع أو الحواسيب الإلكترونية، باستخدام برامج للتجسس على الشبكات والأنظمة الإلكترونية، والاعتداء على البنية التحتية المعلوماتية للمؤسسات والخاصة على حد سواء، بما في ذلك البريد الإلكتروني،

---

[١] منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦، ص ٤٦-٤٧.

[٢] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، ٢٠٠٥، ص٥٨.

[٣] د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، مصدر سابق.

[٤] د. هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، المصدر السابق.

واشتراكات المستخدمين والأرقام السرية للبطاقات الإئتمانية، وما إلى ذلك[1]. والأمثلة على مثل هذه الجرائم كثيرة، ومنها على سبيل المثال لا الحصر: العمل على اختراق نظم السلامة الخاصة بالمصانع أو المستشفيات لإحداث اضرار بالناس، واختراق مواقع المنشآت الحيوية كمؤسسات الكهرباء او الغاز او البترول من أجل إلحاق الأذى بها.

بناء على ما سبق، يلاحظ بأن الإرهاب الإلكتروني من الجرائم التي توصف بأنها عابرة للحدود، وهي محل اهتمام التنظيمات الإرهابية المعاصرة، إذ بات مرتكبي الارهاب الإلكتروني يسخرون التكنلوجيا المعاصرة لتنفيذ أفعالهم الجنائية، نظراً لسهولة ارتكابها وقلة تكلفتها، وصعوبة اكتشاف مرتكبيها، خاصة إذا ما أخذنا في الحسبان سهولة إنشاء المواقع الإلكترونية واختراقها وانتشار برامج تدمير المواقع والنظم المعلوماتية وانتشار برامج التجسس و..الخ. لذلك فأن مواجهة هذه الجريمة بأنواعها المختلفة تستدعي تظافر الجهود الدولية وتعاون الدول في التصدي لها وردعها، لاسيما في ظل طبيعتها الدولية والعابرة للحدود.

المبحث الثاني

صور التعاون الدولي في مواجهة الإرهاب الإلكتروني

انقسمت الجهود الدولية في مكافحة الإرهاب الإلكتروني، إلى عدة أنماط: النمط الأول يتعلق بالعمل على إدخال تلك الجريمة ضمن الجرائم الإلكترونية والعمل على إصدار تشريعات وطنية تكافح تلك الظاهرة، أما النمط الثاني: فهو سعي عدد من الدول أو التكتلات الإقليمية إلى التعاون فيما بينها في مكافحة الإرهاب والجريمة عبر الإنترنت، أما النمط الثالث: فيتمثل في العمل على حث الأمم المتحدة على القيام بدور في المكافحة عن طريق فرض سيطرتها على إدارة الإنترنت وإقرار ثقافة عالمية للأمن الالكتروني[2] . ونظراً للطبيعة الواسعة لهذا الموضوع، سوف نسلط الضوء على ثلاثة صور رئيسة للتعاون الدولي لمواجهة هذا النوع المستحدث من الإرهاب ولتوضيح ذلك سيتم تقسيم هذا المبحث إلى مطلبين، نتناول بالبحث في المطلب الأول التعاون

---

[1] د. مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر، العدد الخامس، المجلد الأول، يناير-يونيو ٢٠١٥، ص١٣٥.

[2] د.عادل عبدالصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة، مصدر سابق، ص٣٢٩.

التشريعي والأمني الدولي في مواجهة الإرهاب الإلكتروني، وفي المطلب الثاني التعاون القضائي الدولي ومشكلة الاختصاص القضائي فيه.

المطلب الأول

التعاون التشريعي والأمني الدولي

من أجل تحديد مضمون التعاون التشريعي والأمني الدولي للتصدي للإرهاب الإلكتروني، سيجري تقسيم هذا المطلب الى فرعين، نبحث في الفرع الأول في التعاون التشريعي الدولي، وفي الفرع الثاني في التعاون الأمني الدولي، وكما يأتي:

الفرع الأول

التعاون التشريعي الدولي

إن التصدي للإرهاب الإلكتروني يجد إطاره القانوني ضمن طائفتين من تشريعات الدول، الأولى تشريعات الفضاء السيبراني وبشكل خاص تشريعات الجرائم الإلكترونية بقواعدها الموضوعية والإجرائية وتشريعات تنظيم الخدمات الإلكترونية والمعايير والمقاييس والسلامة المعلوماتية. والطائفة الثانية تشريعات مكافحة الارهاب (العادية) المناط بها تحديد المفاهيم وجهات الإشراف والاختصاص وإنفاذ القانون[1].

لقد سعت العديد من الدول المتقدمة من أجل اعتماد استراتيجية قومية فيما يخص تأمين الفضاء الإلكتروني، حيث قام عدد من الدول بسن قوانين وتشريعات وطنية في الوقت الذي إتجه البعض الآخر منها إلى تعزيز التعاون الدولي والإقليمي للحد من هذه الجريمة أو مكافحته، وتم تضمين خطر التعرض لهجمات الفضاء الإلكتروني من ضمن استراتيجيات الأمن القومي[2].

وعلى الرغم من أن العديد من الدول المتقدمة تدرك أهمية حماية أمن المعلومات الا أنها بدأت متأخرة في إعادة هيكلة أطرها التشريعية الخاصة بحماية الفضاء الإلكتروني بعد أحداث

---

[1] يونس محمد عرب، التدابير التشريعية لمواجهة أنشطة الإرهاب عبر الإنترنت، الندوة العلمية المعنونة (استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين)، القاهرة، ٢٥-٢٠١٠/١٠/٢٧، ص٢٨.

[2] خليل يوسف جندي ميراني، سياسة التجريم في ظل العولمة، أطروحة دكتوراه، كلية القانون والعلوم السياسية، جامعة دهوك، ٢٠١٧، ص٢٣٠.

١١ سبتمبر ٢٠٠١، وذلك لأن القوانين الوطنية لم تتواكب مع التطورات الحديثة، فهناك من الدول من اتجه إلى تحديث أطرها التشريعية بينما تمكنت دول أخرى من إصدار قوانين محددة[١] حول الجريمة الإلكترونية[٢]. وبحلول عام ٢٠٠٢، كان ستة عشر بلداً قد سنت تشريعات تتعلق بالإرهاب الإلكتروني والوصول غير المصرح به للحواسيب. ويلاحظ إن اللغة القانونية المستخدمة في هذه البلدان فيما يتعلق بالوصول غير المصرح به للحواسيب، لم تذكر أي إشارة للدوافع الخاصة اللازمة لتصنيف (الإرهاب الإلكتروني)[٣].

ونحاول فيما يأتي بيان أوجه التعاون الدولي التشريعي لمواجهة الإرهاب الإلكتروني، في إطار منظمة الأمم المتحدة، وبعض المنظمات الإقليمية.

أولاً: جهود منظمة الأمم المتحدة :

تعد منظمة الأمم المتحدة من أكثر المنظمات قدرة، والأكثر تأهيلاً على مجابهة الإرهاب الدولي ومكافحة أعمال العنف ذات الطابع الدولي، سواء كان على صعيد وضع المبادئ والسياسات أو على المستوى العملياتي والتنفيذي. وذلك لأن الأمم المتحدة هي منظمة عامة الاختصاص، تسعى طبقاً لميثاقها إلى حل المشاكل الدولية السياسية والمنية والاقتصادية والاجتماعية، ومن ثم فإن منع ومكافحة الارهاب يدخل في إطار ما تملك من اختصاصات[٤]. فمنذ عام ١٩٦٣ ، وضع المجتمع الدولي صكوكاً قانونية عالمية لمنع الأعمال الإرهابية تحت رعاية الأمم المتحدة ووكالاتها المتخصصة، ونتيجة للاهتمام الذي ركز على مكافحة الإرهاب عقب اتخاذ

---

[١] وقد اتجهت بعض الدول في الوقت الحاضر إلى سن تشريعات خاصة بمكافحة الجرائم الإلكترونية، للتفاصيل انظر: حسن بن أحمد الشهري، الإرهاب الإلكتروني-حرب الشبكات- المجلة العربية الدولية للمعلوماتية، المجلد الرابع، العدد الثامن، ٢٠١٥، ص١٩.

[٢] د.عادل عبدالصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة، مصدر سابق، ص٣٧٧.

[٣] Dolliver, D. S.& Seigfried-Spellar, K. C.(2017) Cyberterrorism 1 Legal, Forensic, and Criminological Aspects of Cyberterrorism,(6 edition),]e-book[.Wolters Kluwer Publishing House, Editors: Emil Pływaczewski. P.6-7.

[٤] د. عبدالعزيز مخيمر عبد الهادي، إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب(مع الإشارة إلى جهود الوكالات الدولية المتخصصة بهذا الخصوص)، ورقة علمية مقدمة الى ندوة القوانين العربية والدولية في مكافحة الارهاب جامة نايف العربية للعلوم الأمنية الرياض في ٥-٧ جمادي الثاني ١٤٣٤ هجرية، ص٧-٨.

مجلس الأمن للقرار ١٣٧٣ (٢٠٠١)[١]، الذي دعا فيه المجلس الدول الأعضاء لكي تصبح أطرافاً في الصكوك القانونية العالمية لمكافحة الإرهاب، زاد معدل التقيد بهذه الصكوك زيادة كبيرة. وحتى حزيران / يونيو ٢٠١١، كان ثلثا الدول الأعضاء قد صدق على عشر من الصكوك الـ ١٦ العالمية لمكافحة الإرهاب أو إنضم إليها[٢]. وعلى الرغم من صدور هذا العدد الكبير من الصكوك بشأن الإرهاب، الا أنه لا توجد حتى الآن معاهدة شاملة للأمم المتحدة تنطبق على قائمة شاملة بمظاهر الإرهاب[٣].

وقد صدرت عن الجمعية العامة قرارات عديدة تهدف إلى مكافحة الأعمال الإرهابية وتوضح مدى تزايد الاهتمام الدولي باستخدام تكنلوجيا الاتصالات والمعلومات استخداماً سليماً، ومنها: القراران ٦٣/٥٥ المؤرخان كانون الثاني / يناير ٢٠٠١ و ١٢١/٥٦، كانون الثاني / يناير ٢٠٠٢ بشأن مكافحة إساءة استخدام تكنلوجيا المعلومات لأغراض إجرامية اللذان يدعوان الدول الأعضاء إلى بذل جهود مشتركة لمكافحة الجريمة الإلكترونية؛ وتكييف التشريعات في هذا السياق، وقرار الجمعية العامة في الدورة ٢٨/٥٥ في ديسمبر ٢٠٠٠ والدورة ١٩/٥٦ في ديسمبر ٢٠٠١ بشأن ارساء الأساس القانوني لمكافحة استعمال تكنلوجيا الاتصالات والمعلومات في أعمال

---

[١] نص القرار على الموقع الإلكتروني (تاريخ الزيارة ٢٠١٨/١/٦):
https://undocs.org/ar/S/RES/1373(2001)

[٢] لقد أعدت واعتمدت ستة عشر صكاً قانونياً عالمياً(من بينها ١١ اتفاقية، وأربعة بروتوكولات، وتعديل واحد) تحت إشراف الأمم المتحدة والمنظمات الحكومية الدولية المتصلة به. وأغلبية هذه الصكوك سارية وتوفر إطاراً قانونياً لاتخاذ إجراءات متعددة الأطراف ضد الإرهاب ولتجريم أعمال إرهابية محددة، تشمل اختطاف الطائرات، وأخذ الرهائن، وتفجيرات القنابل الإرهابية، وتمويل الإرهاب، والإرهاب النووي، وتكملها قرارات صادرة عن الجمعية العامة (٤٩/٦٠ و٥٠/٢١٠ و٦٠/٢٨٨) وقرارات صادرة عن مجلس الأمن(١٢٦٧(١٩٩٩)، و١٣٧٣(٢٠٠١)، و١٥٤٠(٢٠٠٤)، و١٥٦٦(٢٠٠٤)، و١٦٢٤(٢٠٠٥)). انظر الموقع الرسمي للأمم المتحدة:
http://www.un.org/arabic/terrorism/strategy-implementation.shtml وللإطلاع على مجموعة الصكوك الدولية لمكافحة الإرهاب انظر الموقع الالكتروني (تأريخ الزيارة ٢٠١٨/١/٦):
https://www.un.org/counterterrorism/ctitf/ar/international-legal-instruments

[3] United Nations Counter-Terrorism Implementation Task Force Working Group Compendium، (2011),Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects, p. 18.

اجرامية[١]، وقرارا الجمعية العامة ٢٣٩/٥٧ و ١٩٩/٥٨ المؤرخان في ٢٠ و ٢٣ ديسمبر ٢٠٠٢ بشأن "إنشاء ثقافة عالمية للأمن السيبراني" و"حماية البنى التحتية للمعلومات الحرجة"[٢] اللذان يدعوان الدول الأعضاء إلى التعاون المستمر في مجال الأمن السيبراني، وتعزيز ثقافة الأمن الإلكتروني، وتوصيات ورشة العمل: "تدابير لمكافحة الكمبيوتر ذات الصلة بالجريمة "، التي عقدت في بانكوك في ٢٢ نيسان / أبريل ٢٠٠٥ كجزء من مؤتمر الأمم المتحدة الحادي عشر- لمنع الجريمة والعدالة الجنائية. كما تشمل قرارات مجلس الأمن الأخرى المتعلقة بالإرهاب الإلكتروني، القرار ١٦٢٤ (٢٠٠٥) ، الذي يتناول التحريض والتمجيد للأعمال الإرهابية، والقرار ١٩٦٣ (٢٠١٠) ، الذي "يعترف بأهمية التعاون بين الدول الأعضاء لمنع الإرهابيين من استغلال التكنلوجيا والاتصالات والموارد" [٣].

إضافة إلى ذلك، أعربت الدول أعضاء الأمم المتحدة في اجتماعات مختلفة عن قلقهم إزاء خطر الجريمة السيبرانية والإرهاب الإلكتروني، واقترحت برامج تدريبية بشأن مكافحة الإرهاب الإلكتروني للوكالات الوطنية لإنفاذ القانون[٤]. وفي عام ٢٠١٣ ، بدأ معهد الأمم المتحدة الأقاليمي لأبحاث الجريمة والعدالة، تنفيذ مشروع "جدول الأعمال البحثي الأوربي في مجال الجرائم الإلكترونية والإرهاب الإلكتروني"، الذي بدأ تنفيذه في عام ٢٠١٤ ، كما دُعي إلى أن يصبح عضواً في الفريق الاستشاري للمركز الأوربي للجرائم السيبرانية [٥].

---

[١] د. علاءالدين راشد، الأمم المتحدة والإرهاب قبل وبعد ١١ سبتمبر، دار النهضة العربية، القاهرة، ٢٠٠٥، ص٧٩ وما بعدها.

[٢] انظر نص القرارين على الموقع الإلكتروني (تاريخ الزيارة ٢٠١٨/١/٦):
http://www.un.org/ar/ga/71/resolutions.shtml

[٣] انظر نص القرارات الخاصة بمكافحة الإرهاب على الموقع الإلكتروني (تاريخ الزيارة ٢٠١٨/١/١٥):
http://www.un.org/ar/sc/ctc/resources/ressc.html

[4] Ozeren, S. (2005). Cyberterrorism and international cooperation: General overview of the available mechanisms to facilitate an overwhelming task, Responses to Cyber Terrorism, [E book], NATO Science for Peace and Security Series - E: Human and Societal Dynamics, 34, pages 34-88, IOS press, p. 81. Available from http://ebooks.iospress.nl/publication/24330 [Accessed 12 october 2017].

[٥] الأمم المتحدة، المجلس الاقتصادي والإجتماعي، لجنة منع الجريمة والعدالة الجنائية الدورة الثالثة والعشرون، فيينا، ١٢-١٦ آيار/مايو ٢٠١٤ البند ٥(هـ) من جدول الأعمال المؤقت، الوثيقة E/CN.15/2014/18 ، ص٦.

مما سبق يتضح، بأن هناك جهود مكثفة بذلتها منظمة الأمم المتحدة للتصدي للإرهاب الألكتروني، تمثلت في القرارات الدولية بهذا الخصوص، وإلزام الدول الأعضاء بها بالتعاون الدولي لتجسيدها ، فضلاً عن مجالات التعاون الدولي التي أشرفت عليها.

ثانياً: دور المنظمات الإقليمية :

سوف نحاول ان نوضح دور المنظمات الإقليمية في التصدي لظاهرة الإرهاب الإلكتروني وعلى النحو التالي:

(أ) مجلس أوربا:

تمثلت ذروة جهود مجلس أوربا المتعلقة بالجرائم الإلكترونية بإبرام إتفاقية مجلس أوربا بشأن الجرائم السيبرانية في علام ٢٠٠١، المعروفة باسم إتفاقية بودابست (ETS 185)[1]، التي دخلت حيز النفاذ في ١ تموز / يوليه ٢٠٠٤. وباتصديق على الإتفاقية أو الانضمام إليها، اتفقت الدول على أن تجرم قوانينها الداخلية السلوك الموصوف في قسم القانون الجنائي الموضوعي وتحدد الإجراءات والأدوات اللازمة للتحقيق في هذه الجرائم ومقاضاة مرتكبيها. وتستكمل إتفاقية بودابست ببروتوكول[2] يتعلق بكراهية الأجانب والعنصرية التي ترتكب عن طريق نظم الحاسوب (ETS No.189) [3]. وعلى الرغم من أن ٥٠ بلداً وقعت عليها وصدق عليها ٤٦ بلداً مشجعاً للتعاون الدولي، الا أن هناك العديد من البلدان التي لم تدرج في هذه الإتفاقية، وبالتالي فإن التعاون الدولي لم ينجز تماماً[4]. ولكي تكون المعاهدة أكثر فعالية في مكافحة الإرهاب

---

(1) See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185,[Accessed 12 october 2017].

(2) Additional Protocol to the Convention on Cybercrime، concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems(ETS No.189), Opening of the treaty; Strasbourg, 28/01/2003 ; 01/03/2006, Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=Z9kSyEKq

(3) Budapest Convention, Opening of the treaty(23/11/2001), Entry into Force(01/07/2004)، Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention.

(4) United Nations Counter-Terrorism Implementation Task Force Working Group Compendium، supra note 2, at 19, p. 22.

الإلكتروني، فأنه ينبغي أن تتعلق على وجه التحديد بالإرهاب الإلكتروني[١]. وبذلك حدد مجلس أوربا الإرهاب الإلكتروني واستخدام الإنترنت لأغراض إرهابية كمجالات تركيز ذات أولوية، إذ عمل المجلس على معالجة ذلك من خلال إتفاقية الجرائم السيبرانية (٢٠٠١) وإتفاقية مجلس أوربا بشأن منع الإرهاب (CETS No.196).[٢] ويقوم المجلس بدراسة الوضع في الدول الأعضاء لتقييم ما إذا كانت الصكوك الدولية القائمة كافية للاستجابة لهذا التهديد الناشئ، كما قام بوضع قاعدة بيانات عن الإرهاب الإلكتروني تتضمن المساهمات الوطنية لمواجهته.

وتضمنت إتفاقية مجلس أوربا لمنع الإرهاب الصادرة في عام ٢٠٠٥ عدة جرائم من قبيل الاستفزاز العام لارتكاب جريمة إرهابية وتجنيد الإرهابيين، ولكنها لا تتضمن، على سبيل المثال، أحكاماً تجرم الهجمات الارهابية المتصلة بالأنظمة الحاسوبية[٣]، وتهدف الإتفاقية إلى "زيادة فعالية النصوص الدولية القائمة بشأن مكافحة الإرهاب"، وعلى الرغم من أن الإرهاب يشمل الإرهاب الإلكتروني، فإن الإرهاب الإلكتروني لم يرد ذكره في الإتفاقية، وعدم وجود نص محدد لمواجهة الإرهاب الإلكتروني هو قضية تحتاج إلى تصحيح. ويمكن تطبيق إتفاقية مجلس أوربا بشأن الجرائم السيبرانية بالاقتران مع صكوك مكافحة الإرهاب، مثل إتفاقية مجلس أوربا بشأن منع الإرهاب، لتوفير أساس قانوني للتعاون ضد استخدام الإنترنت لأغراض إرهابية.

ودعا البروتوكول الإضافي لإتفاقية مجلس أوربا بشأن مكافحة الإرهاب[٤] (CETS No.217)، الذي عرض للتوقيع خلال اجتماع اللجنة الوزارية الأوربية في ٢٢ أكتوبر ٢٠١٥

---

(1) Ibid. at 8.

(2) The Council of Europe Convention on the Prevention of Terrorism, Explanatory Report CETS No.196, [hereafter European Convention] Opening of the treaty; Warsaw, 16/05/2005, Entry into Force; 01/06/2007. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196, [Accessed 12 october 2017].

(3) United Nations Counter-Terrorism Implementation Task Force Working Group Compendium، supra note 2, at 19, p. 22.

(4) Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism(CETS No.217), Opening of the treaty; Riga, 22/10/2015 , Entry into Force; 01/07/2017, Retrivate from

بعاصمة لاتفيا، إلى تجريم السفر لأغراض إرهابية، وكذلك تجريم تمويل وتسهيل وتنظيم هذه الرحلات. ويُجرّم البروتوكول الانتساب إلى المجموعات والتنظيمات الإرهابية والسفر لأغراض القتال والمشاركة في معسكرات تدريب وتجنيد وتنظيم سفر المقاتلين ودعمهم مادياً. ويهدف البروتوكول إلى تحقيق توافق في قوانين الدول الأعضاء في هذا الخصوص والتعاون والتنسيق بينها حيث جرى إعداده على خلفية التهديد الذي يمثله المقاتلون من مواطني أوربا العائدين إلى بلدانهم بعد مشاركتهم في القتال ضمن التنظيمات الإرهابية في سوريا والعراق ومن بينها تنظيم داعش. وبموجب البروتوكول ينبغي على الدول الأعضاء تبادل المعلومات الاستخباراتية وإنشاء مراكز اتصال تعمل على مدار الساعة من أجل تحقيق التعاون المنشود[١].

(ب) منظمة الدول الأمريكية:

أدرج الإرهاب على جداول أعمال منظمة الدول الأمريكية منذ الستينات، وتبنت المنظمة أول إتفاقية تتعلق بالإرهاب سنة ١٩٧١، عرفت بإتفاقية منع ومعاقبة الأعمال الإرهابية[٢]. كما اعتمدت في أعقاب هجمات ١١ أيلول / سبتمبر في نيويورك إتفاقية دولية ذات طابع إقليمي لمناهضة الإرهاب عام ٢٠٠٢[٣] ، ودخلت هذه الإتفاقية حيز النفاذ في عام ٢٠٠٣. كما أنشئت لجنة للدول الأمريكية لمكافحة الإرهاب (CICTE) والغرض الرئيس منها هو تعزيز وتطوير التعاون فيما بين الدول الأعضاء لمنع الإرهاب ومكافحته والقضاء عليه، وفقاً لمبادئ ميثاق منظمة الدول الأمريكية، وإتفاقية البلدان الأمريكية لمكافحة الإرهاب. وفي عام ٢٠٠٥، نظم مؤتمر بالتعاون مع مجلس أوربا وإسبانيا بعنوان "الجريمة الالكترونية: تحد عالمي، استجابة عالمية[٤]". ومن بين الاستنتاجات التي تم اعتمادها: تشجيع الدول على النظر في إمكانية أن

---

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217. [Accessed 12 october 2017].

[١] مقال منشور تحت عنوان، الاتحاد الأوربي يوقع على البروتوكول الإضافي لإتفاقية مكافحة الإرهاب يركز على كيفية التعامل مع مشكلة المقاتلين الأجانب في سوريا والعراق، ٢٣ أكتوبر ٢٠١٥ ، الشرق الأوسط، متاح على الصفحة الالكترونية (تاريخ الزيارة ٢٠١٧/١٢/٢٨): https://aawsat.com/home/article/

[٢] د. فيدا نجيب حمد، مكافحة الإرهاب قبل هجمات ١١ أيلول ٢٠٠١ وما بعدها، ط١٧، منشورات الحلبي الحقوقية، بيروت، ٢٠١٧، ص٢٥٦.

[3] See: http://www.oas.org/en/topics/terrorism.asp.[Accecced 12/25/2017].

[4] See: http://www.oas.org/juridico/english/cyber_meet.html. [Accecced 12/25/2017].

تصبح أطرافاً في إتفاقية مجلس أوربا بشأن الجريمة الالكترونية من أجل الاستفادة من القوانين والأدوات الفعالة والمتوافقة على الصعيد المحلي وباسم التعاون الدولي. وسلم بالحاجة إلى مواصلة التعاون وتقديم المساعدة التقنية وتنظيم أحداث مماثلة في مناطق عالمية أخرى. وقد أكد الاجتماع السادس لوزراء العدل في حزيران / يونيه ٢٠٠٦ هذا الالتزام. ولم تبدأ منظمة الدول الأمريكية، في اتخاذ الإجراءات لمواجهة الهجمات الإلكترونية الا في نيسان / أبريل ٢٠٠٤، إذ اعتمدت الاستراتيجية المتكاملة للبلدان الأمريكية لمكافحة التهديدات للأمن السيبراني[١].

لقد انتبه الغرب، منذ عقدين تقريباً، إلى قضية الإرهاب الإلكتروني ومخاطره، حيث قام الرئيس الأمريكي آنذاك بيل كلينتون في عام ١٩٩٦، بتشكيل هيئة منشآت البنية التحتية الحساسة. وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات، إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع للولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة[٢]. وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة بإنشاء هيئاتها ومراكزها الخاصة للتعامل مع احتمالات الإرهاب الإلكتروني، فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفاً من خبراء أمن المعلومات، وقوة ضاربة على مدى ٢٤ ساعة لمواجهة الإرهاب الإلكتروني، وقامت القوات الجوية الأمريكية باتخاذ خطوات مماثلة، ومثلها المباحث الفدرالية، كما تقوم قوات الأمن في أوربا باتخاذ إجراءات مماثلة. لكن من الواضح على ما يبدو أن هذه الإجراءات لم تكن كافية بدليل وقوع حادثة ١١ أيلول ٢٠٠١ الإرهابية بعد ذلك بسنوات قليلة. حيث وجد التحقيق في هجمات ١١ أيلول / سبتمبر أن الإرهابيين استخدموا البريد الإلكتروني لتنسيق هجماتهم[٣].

(ت) جامعة الدول العربية:

---

[1] Organization of American States, AG/RES. 2040 (XXXIV-0/04), at ch. IV, f 8 (June 8, 2004), available from http://www.oas.org/juridico/english/ga04/agres_2040.htm. [Accessed 12 october 2017].

[٢] د. بدر احمد، الإرهاب الإلكتروني أدواته وآثاره وأساليب الوقاية والعلاج، متاح على الصفحة الإلكترونية (تأريخ الزيارة ٢٠١٧/١/١٦): http://baathparty.sy/site/arabic/index.php?node=552&cat=15369

[٣] United Nations Counter-Terrorism Implementation Task Force Working Group Compendium، supra note 2, at 19, p.5.

فيما يتعلق بالتعاون العربي في مجال مكافحة الإرهاب عموماً، فقد جاء التعاون في إطار إدراك العديد من الدول العربية لأهمية مواجهة هذه الظاهرة بشكل جماعي وأن المواجهة الفردية لن تكون ذات أثر فعال. ويتخذ التعاون العربي في مجال مكافحة الإرهاب أكثر من مستوى وزراء الداخلية ووزراء العدل. ويعد مؤتمر الأمم المتحدة التاسع لمنع الجريمة الذي عقد بالقاهرة في إبريل عام ١٩٩٥ من أهم التجمعات الدولية التي شهدت تحركاً عربياً للتصدي لقضية الارهاب، فقد نجح هذا المؤتمر في تدويل الاهتمام بقضية الإرهاب وتكللت الجهود الرامية إلى عد الإرهاب أحد أنواع الجريمة المنظمة بالنجاح[١].

ونصت المادة الخامسة عشر- من الفصل الثاني المتعلق بالتجريم من الاتفاقية العربية لمكافحة جرائم التقنية الموقعة في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠ لتحديد الجرائم المتعلقة بالإرهاب ومرتكبيه بواسطة تقنية المعلومات التي عرفتها ذات الاتفاقية بأنها(أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها....) على الجرائم التالية: نشر- أفكار ومبادئ الجماعات الإرهابية والدعوة لها، تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر- طرق صناعة المتفجرات والتي تستخدم خاصة في العمليات الإرهابية، و..الخ[٢].

وفي إطار ما تشهده بلدان العالم المختلفة ومن بينها البلدان العربية، من احداث إرهابية مؤسفة، تقدمت مصر بمجموعة من المبادئ الاسترشادية المقترحة التي يمكن للدول العربية الاستناد إليها في صياغة ميثاق عربي لمكافحة الإرهاب الإلكتروني. تضمن مجموعة من المبادئ الاسترشادية المقترحة مرجعيتها من دراسة وتحليل الجهود الدولية المتمثلة في الإستراتيجيات الوطنية والأنشطة والاتفاقيات الإقليمية والدولية فيما يتعلق بالإرهاب الإلكتروني، والتي تأتي على رأسها إتفاقية بوادبست، المذكورة سابقا[٣].

---

[١] د. يوسف حسن يوسف، الجريمة المنظمة الدولية والإرهاب الدولي، ط١، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٠، ص٩٩.

[٢] نص الاتفاقية على الموقع الإلكتروني(تأريخ الزيارة ٢٠١٨/٥/٢٧)
http://haqqi.info/ar/haqqi/legislation/arab-convention-cyber Bcrimes

[٣] مبادئ استرشادية في مكافحة الإرهاب الإلكتروني، متاح على الموقع الإلكتروني:

وعلى صعيد أبرز جهود الدول العربية الأخيرة ، عقد في أبو ظبي في الفترة (١٦-٢٠١٧/٥/١٥) المؤتمر الدولي لتجريم الارهاب الالكتروني الذي أكد على أهمية ايجاد إطار تشريعي دولي شامل للارهاب الالكتروني، ووضع استراتيجية للتصدي له، وأصدر (أعلان أبو ظبي) الذي تضمن عدداً من التوصيات من أجل مواجهة الارهاب الالكتربي، وعلى رأسها: اعتماد إتفاقية دولية ملزمة تحظر الإرهاب الإلكتروني بكافة أشكاله بما في ذلك محاولات التجنيد والتحريض على الإرهاب والدعوة إليه والإشادة به وتمويله وعدم التبليغ عنه بالإضافة إلى الدعوة إلى العنف والكراهية والتمييز العرقي والديني والإساءة إلى الآخرين وإلى الأديان، وكذلك دعوة الدول الى وضع قانون خاص يتعلق بالجرائم الإلكترونية، وإنشاء هيئات وطنية للمعلوماتية والحريات والأمن الإلكتروني تتولى وضع سياسات واستراتيجيات في إطار سيادة القانون لرصد ومجابهة المحتوى الرقمي الذي ينطوي على مخاطر إرهابية.[1]

كما وتضمنت التوصية الخامسة من توصيات المؤتمر الثاني عشر- للمسؤولين عن مكافحة الإرهاب الذي عقد في تونس عام ٢٠٠٩ وتوصيات ورشة العمل التي عقدت بمقر الأمانة العامة لجامعة الدول العربية في القاهرة عام ٢٠٠٩ حول (تدابير استخدام الانترنت في الجرائم الإرهابية على الصعيد العربي) وتوصيات الاجتماع الثامن لفريق الخبراء العرب المعني بمكافحة الإرهاب الذي عقد في القاهرة عام ٢٠١٠ التأكيد على أهمية تقديم اقتراحات لمواجهة الإرهاب الالكتروني وقامت بعض الدول العربية بتقديم المقترحات في هذا الصدد، منها إنشاء أو تصميم برنامج على الحاسب يدعى (شرطة الإنترنت) وتكون مهامه تطهير الإنترنت بهدف حجب المواقع الإرهابية والمواقع الغريبة على المجتمع العربي، ومنع المستخدمين من الحصول على معلومات غير صحيحة وضارة من المواقع المعادية ويقوم بحذف وإيقاف أية رسالة واردة من مصادر معادية للقيم والتقاليد، وذلك على غرار (مركز حرب المعلومات)، الذي أسسته وكالة الاستخبارات المركزية للتعاطي مع جرائم الإرهاب الإلكتروني ويضم نحو ألف موظف ، وهو

http://www.lasportal.org/ar/councils/ministerialcouncil/Documents/CyberSecurity%20EG+Notes.pdfبلت

[1] المؤتمر الدولي لتجريم الارهاب الالكتروني، ١٥-١٦ /٢٠١٧/٥، أبو ظبي، ايلاف، العدد ٥٨١٤ في ٢٠١٧/٥/١٩، متاح على الصفحة الالكترونية (تأريخ الزيارة ٢٠١٨/٢/٤): http://elaph.com/Web/News/2017/5/1148632.html

يعمل على مدار الساعة مناوبة للرد على أي تطورات أو استفسارات، ومشروع (ايشلون) الذي أسس بالتعاون بين الدول الأوربية للتجسس على رسائل الانترنت والمكالمات الهاتفية في العالم، وغيرهما[١].

الفرع الثاني

التعاون الأمني الدولي

تمثل المعلومات مجالاً مهماً في مجال مكافحة جرائم الإرهاب، وخاصة بعد زيادة ارتكابها عبر الحدود الوطنية. ولهذا كان التعاون الشرطي الدولي بين الأجهزة الوطنية المسؤولة عن المحافظة على نظام الحماية أمراً لا غنى عنه لقمع الإجرام الدولي[٢]. وقد كان التعاون الشرطي الدولي محلاً للعديد من الاتفاقيات الدولية، ومنها الإتفاقية التي عقدتها المنظمة الدولية للشرطة الجنائية (OPC-Interpol)، هذا بجانب اتفاقيات أخرى إقليمية للتعاون الشرطي الدولي منها معاهدة البينالكس Benalxum، واتفاقيات تشنجن سنة ١٩٨٥ وإتفاقية لتطبيقها سنة ١٩٩٠ والتي أُدمجت في نطاق الاتحاد الأوربي سنة ١٩٩٩، والإتفاقية التي أنشأت الإيروبول سنة ١٩٩٥، ومعاهدتا ماسترخت وأمستردام[٣].

ويلعب الأنتربول دوراً رائداً فيما يتعلق بتحقيق أهداف التعاون الشرطي الدولي على صعيد العالم، ويتركز نشاط الانتربول حالياً على ستة مجالات للجريمة: الفساد، ملاحقة الفارين من وجه العدالة، المخدرات والجريمة المنظمة، السلامة العامة والإرهاب، والاتجار بالبشر والإجرام المالي المرتكب بواسطة التكنولوجيا المتقدمة[٤]. ويلعب الإنتربول دوراً نشطاً وخلاقاً في

---

[١] فراس الرشيد، مكافحة تجنيد الإرهابيين عبر الإنترنت، مصدر سابق، ص١٤-١٦.

[٢] د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، ط٢، مركز الأهرام للترجمة والنشر،مؤسسة الأهرام، مصر، ٢٠٠٨، ص٤٢٠.

[٣] د. أحمد فتحي سرور، المواجهة القانونية للإرهاب، المصدر السابق، ص٤٢١.

[4] Sandler, T., Arce, D. G., Enders, W.(2011) An Evaluation of Interpol's CooperativeBased Counterterrorism Linkages, The Journal of Law & Economics, 54(1), pp. 79 -110, The University of Chicago Press for The Booth School of Business, p.79.

استغلال التكنولوجيات الجديدة التي تتيح تبادل البيانات الدولية على نطاق واسع بشأن الإرهاب بشكل عام وفي عدد من المشاكل المتعلقة بالجريمة[١].

وقد حظي الدور الحيوي الذي يضطلع به الإنتربول بصفته مركزاً عالمياً للبيانات المتصلة بالإرهاب باعتراف دولي، فالقرار ٢١٧٨ الصادر عن مجلس الأمن التابع للأمم المتحدة عام ٢٠١٥ أوكل إلى الإنتربول ولاية واضحة تتمثل في العمل كمركز عالمي لتبادل المعلومات الشرطية الرامية إلى مكافحة التهديد الإرهابي[٢]. وانضم الإنتربول في عام ٢٠١٦ الى التحالف العالمي لمكافحة تنظيم الدولة الإسلامية. وأضاف الإنتربول إلى التحالف الذي يضم ٧٣ بلداً ومنظمة دولية عنصراً حاسماً من عناصر العمل الشرطي الدولي، إذ يعمل بمثابة قناة لتبادل المعلومات بين مناطق النزاع والشرطة في جميع أنحاء العالم[٣].

وتشكل (السلامة العامة والارهاب) جانبين رئيسين من نشاطات الانتربول في هذا المجال كونه يسهم في إسناد التحقيق الميداني في سياق مشروع الدمج Fusion والنشاطات الوقائية المنفذة بشكل أساسي في إطار الشراكة مع منظمات أخرى[٤]. كما يضطلع الإنتربول بدور كبير في مواجهة وردع الهجمات الإرهابية عبر الوطنية التي تبدأ في بلد واحد وتنتهي في بلد آخر ، إذ أنشأ الإنتربول في تشرين الأول / أكتوبر ٢٠٠١ (الإدارة الفرعية للسلامة العامة والإرهاب) ، بعد أحداث ١١ سبتمبر ٢٠٠١ في الولايات المتحدة[٥]. كما أنشأ (مركز العمليات والتنسيق)، للرد على طلبات البلدان الأعضاء أثناء الأزمات وتنسيق تقديم المساعدة الخاصة باللغات الرسمية الأربع (الإنكليزي ة والفرنسية والإسبانية والعربية) للإنتربول. ويسهل المركز أيضاً تبادل المعلومات الاستخبارية ونقل جميع إشعارات الإنتربول[٦].

---

(1) Jacobs J. B., Blitsa D(2008) Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy.L.A. Int'l & Comp. L. Rev. 125. p.127. Available from http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1631&context=ilr [Accessed 25 December 2017].

(٢) تقرير الإنتربول السنوي لعام ٢٠١٥، ص٣٤.

(٣) تقرير الإنتربول السنوي لعام ٢٠١٤، ص١٣.

(٤) تقرير الإنتربول السنوي لعام ٢٠٠٤، ص١٢.

(٥) Sandler and other , supra note 3, at 25, P. 80.

(٦) Ibid, at 84.

وتعمل الأمانة العامة لمنظمة الإنتربول على تحديث أدوات ونظم عملها باستمرار، ومن مظاهر ذلك اعتمادها منظومتين متطورتين هما: منظومة اتصالات (١/٧-٢٤)، ومنظومة (MIND وFIND)[١]. وتعزز منظومة (٧/٢٤-١) نظام الانتربول السابق وترفع من قدرته على التعاون السريع والفعال لمكافحة الإرهاب وكافة أشكال الجرائم الدولية الخطرة[٢]. أما منظومة (MIND وFIND) فتمكِّن موظفي الشرطة في خط المواجهة من الاتصال مباشرة بمنظومات الإنتربول[٣] . وتتزايد قيمة (النشرة الحمراء)، التي تكتسب القيمة القانونية لمذكرة التوقيف الاحتياطي".[٤]

وعلى غرار منظمة الانتربول أنشأ المجلس الأوربي في لوكسمبورج عام ١٩٩١ شرطة أوروبية هي اليوروبول (Europol) لتكون همزة وصل بين أجهزة الشرطة الوطنية في دول المنظمة وملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت. والى جانب ذلك، صممت وكالات خصيصاً لتيسير هذا التنسيق، بين كل من اليوروبول، ووحدة التعاون القضائي Eurojust، التي أنشأتها الإتفاقية، الموقعة في ٢٦ تموز / يوليه ١٩٩٥، وهي وحدة التعاون القضائي لتحقيق التعاون القضائي الجنائي على مستوى الاتحاد الأوربي [٥].

وفي إطار استراتيجية الأمن الداخلي للاتحاد الأوربي، تضطلع اليوروجست، بدور نشط ومهم بصفة خاصة، في دعم وتعزيز والتنسيق والتعاون بين سلطات التحقيق والادعاء الوطنية. وهي جهة فاعلة رئيسية ومركز خبرة قضائية لأنشطة مكافحة الجريمة المنظمة والجريمة العابرة للحدود والإرهاب داخل الاتحاد.

---

[١] د. شعبان أبو عجيلة عصار، و د. أبو المعاي محمد عيسى، الرصد المبكر لخطر الجريمة، مجلة العلوم القانونية والشرعية، العدد السادس، جامعة الزاوية، ص ٣٢١.

[٢] حيمر عبدالكريم، منظمة الإنتربول، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر- بسكرة، ٢٠١٤، ص٣٠. متاح على الموقع الإلكتروني (تاريخ الزيارة ٢٠١٧/١٢/٢٣):
http://dspace.univ-biskra.dz:8080/jspui/bitstream/123456789/4232/1/126-%.pdf

[٣] See https://www.interpol.int/ar

[٤] د. شعبان أبو عجيلة عصار، و د. أبو المعاي محمد عيسى، الرصد المبكر لخطر الجريمة، مصدر سابق، ص ٣٣٣-٣٣٤.

[5] Bodin, S., Echilley, M. & Quinard-Thibault, O.(2015) , International cooperation in the face of cyber-terrorism : current responses and future issues, Themis competition Semi-Final A – International Cooperation in Criminal Matters, p.12.

وقد تطور التعاون في أوربا ضد الاستخدام الإرهابي للإنترنت كثيراً ، إذ تم إنشاء فرق تحقيق مشتركة، وهي آلية أنشأها المجلس الأوربي وفق القرار ٢٠٠٢/٤٦٥ / JHA.13، كما اعتمد المجلس توصية في عام ٢٠٠٢ بإنشاء فرق مخصصة متعددة الجنسيات للقيام بذلك وجمع وتبادل المعلومات عن الإرهاب. ويجوز لليوروبول واليوروجست أن يشاركا معاً في إنشاء هذه الفرق بناء على طلب دولة عضو، ويمكن أيضاً إنشاء مثل هذه الفرق مع دولة ثالثة على أساس قضائي مثل البروتوكول الإضافي الثاني لعام ٢٠٠١ الملحق بالإتفاقية الأوربية بشأن المساعدة المتبادلة في المسائل الجنائية بمجلس أوربا أو اتفاق عام ٢٠٠٩ بشأن تبادل المساعدة القانونية بين الاتحاد الأوربي والولايات المتحدة.[1]

المطلب الثاني

التعاون القضائي الدولي ومشكلة الاختصاص فيه

إن الخطوة المنطقية الأخرى للتصدي للإرهاب هي محاولة ردع الإرهابيين الإلكترونيين، وذلك عن طريق تدويل الإجراءات القضائية، هذا ما سنوضحه في هذا المطلب، الذي نوزعه على فرعين، نكرس الفرع الأول لبيان التعاون القضائي الدولي في مواجهة الارهاب الالكتروني، ونبحث في الفرع الثاني في مشكلة الاختصاص القضائي في هذه الجريمة.

الفرع الأول

التعاون القضائي الدولي

لا يعد التشريع الأداة الوحيدة للتعاون بين الدول في مكافحة الإجرام إذ يمكن للسلطة القضائية أن تقوم بدور مهم للغاية في هذا الصدد. والتعاون القضائي ينبع من الضرورة ذاتها التي ينبع منها التعاون التشريعي. ومادامت سيادة الدول لا تتجاوز حدودها فأنه يمتنع عليها القيام بأي عمل قضائي وإجراء عدلي في الأراضي الخاضعة لسيادة دولة أخرى غيرها. ولذا يتوجب

[1] Ibid, at 13.

عليها -إذا اقتضت الحاجة -أن تطلب العون من الدولة التي ينبغي إجراء العمل القضائي المطلوب فوق أراضيها[١].

ويقصد بالتعاون القضائي، تعاون السلطات القضائية في مختلف الدول لمكافحة الجريمة، ويهدف هذا التعاون إلى التقريب في الإجراءات الجنائية من حيث إجراءات التحقيق والمحاكمة إلى حين صدور الحكم على المتهم وضمان عدم إفلاته من العقاب نتيجة لارتكابه جريمته في عدة دول، والتنسيق بين السلطات القضائية في هذا الشأن يجري للإتفاق على معايير موحدة[٢].

إن منع الهجمات الإرهابية والحماية منها والتصدي لها – كما تقدم ذكره- هي من محاور سياسة مكافحة الإرهاب، وينطبق الشيء نفسه على الاستخدام الإرهابي المحتمل لتكنلوجيات المعلومات والاتصالات لمهاجمة البنية التحتية أو المرافق أو الخدمات التي تتيح إمكانية استخدام الإنترنت[٣]. لكن نظراً لعدم وجود قانون دولي شامل، وعدم وجود هيئة فوق وطنية قادرة على التحقيق في الجرائم عبر الوطنية، فأن هذا يتطلب تعاون السلطات في البلدان المعنية. كما أن تنقل المجرمين، وأثر الجريمة يجعلا من الضروري لإنفاذ القانون تعاون السلطات القضائية ومساعدة الدولة التي تولت الاختصاص. وبسبب الاختلافات في القانون الوطني والصكوك المحدودة، يعتبر التعاون الدولي أحد التحديات الرئيسة التي تواجه عولمة الجريمة ويتصل ذلك بالأشكال التقليدية للجرائم عبر الوطنية والجريمة السيبرانية. ويتمثل أحد المطالب الرئيسة للمحققين في التحقيقات عبر الوطنية في أهمية وجود رد فعل فوري من جانب نظرائهم في البلد الذي يوجد فيه مرتكب الجريمة. وفيما يتعلق بهذه المسألة، فإن الصكوك التقليدية للتعاون القضائي الدولي في مسائل القانون الجنائي كثيراً ما لا تفي بالمتطلبات من حيث سرعة التحقيقات في جرائم الإنترنت[٤].

---

[١] د. محمد فاضل، التعاون الدولي في مكافحة الجريمة/ ط٧، منشورات جامعة دمشق، دمشق، ١٩٩٧، ص٥١.

[٢] فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر١ ،٢٠١٣، ص١٣٣-١٣٤.

[٣] Fidler, supra note 5 at 4, P. 478.

[٤] Gercke, M.(2012), understanding cybercrime: phenomena, challenges and legal response , Telecommunication Development Sector, ITU publication, Switzerland , P. 267.

وعليه يعد التعاون القضائي حاجة ملحة في مكافحة الجرائم ومن بينها الإرهـاب الإلكـتروني ويأخذ هذا التعاون عدة أشكال، مثل تبادل الخبرات والمعلومات القضائية والمساعدة التقنيـة أو الإنابة القضائية أو مصادرة الأموال الناتجة من الجريمة المنظمة، أو تسـليم المجـرمين الهـاربين او الإعتراف بالأحكام الجنائية أو نقل الإجراءات الجنائيـة، وغـير ذلـك مـن صـور التعـاون القضـائي. وفيما يتعلق بالتحقيقات في الجرائم الإلكترونية والإرهاب الإلكتروني، فإن الآليات الرسمية الأكـثر صلة بدعم التعاون الدولي هي المسـاعدة القانونيـة المتبادلـة وتسـليم المجـرمين، وهنـاك آليـات أخرى مثل نقل السجناء، ونقل الإجراءات في المسـائل الجنائيـة، ومصـادرة العائـدات الإجراميـة ، واسترداد الأصول، والتي هي أقل أهمية في الممارسة العملية[١].

ومن ذلك، يقوم التعاون في الاتحاد الأوربي على أساس الاعتراف المتبادل بأهميته وضرورتـه، وهو يستند الى أمر الاعتقال الأوربي الذي أقر في عام ٢٠٠٢، و مذكرة الأدلة الأوربية التي أنشئت في عام ٢٠٠٨. وهذه الأدوات تجعل التعـاون أسـهل بـين الـدول الأعضـاء في الاتحـاد الأوربي مـن خلال استبعاد متطلبات التجـريم المـزدوج في قائمـة الجـرائم، بمـا في ذلـك الإرهـاب، والحـد مـن الدوافع لعدم التنفيذ. وعلاوة على ذلك، فإن إجراءات استخدامها بسيطة وتضطلع بها السـلطات القضائية مباشرة. ومع ذلك، غالباً ما كان الحكم الأوربي على الأدلة غير مجد لأنه يتطلـب اليقـين بشأن وجود الأدلة المطلوبة. ونتيجة لذلك، تم إنشاء صك جديد عام ٢٠١٤، وهـو أمـر التحقيـق الأوربي، الذي يغطي جميع اجراءات التحقيق تقريباً[٢].

وتلعب هذه الصكوك دوراً فاعلاً في مكافحة استخدام الإنترنت لأغراض إرهابية لأنها تسمح بالتعاون الدولي السريع[٣]. وإلى جانب ذلك، وعلى الرغم من التسـليم بأهميـة أسـاليب التعـاون القضائي السابق ذكرها، إلا أن استقراء الواقع يطالعنا بخضوعها لكثير من الشـروط والاسـتثناءات التي تضعف من فعاليتها،[٤] ومن بينهـا مسـألة الاختصـاص القضـائي، التـي سنناقشـها في المحـور التالي.

---

[١] Ibid, at 39.

[٢] Gercke, M., supra note 3 at 28, p. 39-40.

[٣] Bodin and other, supra note 1, at 27, p12.

[٤] د. محمود شريف بسيوني، الجريمة المنظمة عبر الوطنية، ماهيتها ووسائل مكافحتها دولياً وعربياً، ط١، دار الشروق، القاهرة، ٢٠٠٤، ص١٩٢.

الفرع الثاني

الإختصاص القضائي في الارهاب الالكتروني

إن القانون الدولي ينص على عدة أشكال من الولاية القضائية، إذ ينص على تطبيق القوانين على أساس جنسية الضحية (الشخصية السلبية) أو المعتدي (الشخصية النشطة)، أو على أساس الجريمة التي تحدث في إقليم الدولة أو التي تؤثر عليها، أو التي تبدأ في إقليم الدولة رغم استكمالها في مكان آخر، والولاية القضائية العالمية، استناداً إلى الخطورة القصوى للجريمة بموجب القانون الدولي، والولاية الوقائية، على أساس تهديد أمن وسلامة الدولة. ومن بين تلك الاختصاصات الإقليمية، تعد الولاية القضائية العالمية ذات أهمية خاصة لردع الإرهاب الإلكتروني. حيث من الصعب للغاية تطبيق الولاية القضائية الإقليمية على الإرهاب الإلكتروني، نظراً لطبيعة الإنترنت وخصائص الإرهاب الإلكتروني. أما الولاية القضائية العالمية فمن السهل أكثر تطبيقها، ويرجع ذلك جزئياً إلى أنها تتشارك مع الإرهاب الإلكتروني في تجاهل الحدود الوطنية، ما يجعل الولاية القضائية العالمية خياراً أكثر جدوى للردع[١]. وهذا يجعل الإختصاص القضائي العالمي ، مقارنة بالاختصاص القضائي الإقليمي هو الأفضل، في التصدي بالإرهاب الإكتروني. وهذا ما سنحاول بيانه كما يأتي:

أولاً: الاختصاص القضائي الإقليمي:

يصف البروفيسور روستيالا (Raustiala)[٢] ، الإقليمية بأنها توفر "المبادئ الأساسية لتطوير القانون الدولي الحديث". بيد أنه نظراً لطبيعة الإنترنت وخصائص الإرهاب الإلكتروني، فإن

---

[١] Gable, K. A. (2012) Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent , vanderbilt journal of transnational law,1(34), p.99. Available from SSRN: https://ssrn.com/abstract=1452803 or http://dx.doi.org/10.2139/ssrn.1452803. [Accessed at 28 Dec. 2017].

[٢] Raustiala, K.(2009) does the constitution follow the flag? the evolution of territoriality in american law . Available from https://global.oup.com/academic/product/does-the-constitution-follow-the-flag-9780195304596?cc=us&lang=en& [Accessed at 28 December 2017].

استخدام الولاية الإقليمية هو في أحسن الأحوال مسألة معقدة للغاية وفي أسوأ الأحوال غير ممكنة. وذلك، لأسباب عديدة، على رأسها: إنه لا يوجد إقليم في الفضاء السيبراني عندما يتعلق الأمر بالإرهاب الإلكتروني. ويرى البروفيسور (روستيالا) بأنه "يمكن تحديد نطاق الانترنت بشكل متزايد"، وأن يُخضع لسيطرة الدول ذات السيادة. وعلى الرغم من أن ذلك قد ينطبق على بعض مجالات القانون، لكنه لا ينطبق على الإرهاب الإلكتروني لعدد من الأسباب، إذ لا توجد حالياً قوانين وطنية تنطبق مباشرة على الإرهاب الإلكتروني. وعلاوة على ذلك، أن الفضاء الإلكتروني قد يخضع لسيطرة الدولة بمعنى أنه يمكن تعيين أسماء النطاقات أو تصفية المحتوى، الا أنه لا يمكن لأي دولة أن تتحكم في مكافحة الإرهاب من منظور تكنولوجي. كما أن مرتكبي الإرهاب الإلكتروني يعملون دون حدود، ويرفضون صراحة الإلتزام بأية تعليمات تكون قد أقامتها الدولة للمواطنين الملتزمين بالقانون. ونتيجة لذلك، فإن مفهوم (تحديد نطاق الإنترنت) لا يتناسب مع الإرهاب الإلكتروني.[١]

وهناك صعوبة ثانية في تحديد ما إذا كانت الدول الأخرى قد تكون لها مصلحة في تأكيد مقبولية الاختصاص. فعلى الرغم من إمكانية تطبيق مبدأ الاختصاص الإقليمي من الناحية النظرية، فإن مقبولية هذا المذهب بموجب القانون الدولي مثيرة للجدل في كثير من الدول. وبما أن الإرهاب الإلكتروني يجب إدانته على نطاق واسع لكي يكون لهذه الإدانة والمقاضاة أثر رادع، فإن أساس الولاية القضائية غير مقبول على نطاق واسع في المجتمع الدولي. وعلاوة على ذلك، أنه على الرغم من أن آثار مبدأ الإقليمية، "أكثر تشدداً" ، وقد يكون منطقياً للإجراءات المدنية، فأنه لا ينطبق على الإرهاب الإلكتروني. كما إن أهداف الهجمات الإلكترونية ليست دائماً سهلة التحديد.[٢]

إن هذه الصعوبات تجعل من غير العملي محاولة الأخذ بالولاية الإقليمية (الاختصاص القضائي الاقليمي) وتطرح أفضلية الأخذ بالاختصاص القضائي العالمي.

ثانياً: الاختصاص القضائي العالمي[٣]:

---

[١] Gable, supra note 4, at 29, P.100-101.

[٢] Ibid, at 104.

[٣] الواقع أن مبدأ الاختصاص العالمي ليس جديداً فثمة اتفاقيات دولية تسمح بتطبيق هذا المبدأ دون النظر إلى جنسية مرتكبيها أو جنسية الضحايا، ودون التقيد بمبدأ الإقليمية. ومن بين هذه الاتفاقيات نذكر

إن العدد المتزايد من الأنشطة الإرهابية الإلكترونية يسلط الضوء على الصعوبات التي تواجه ها الدول ، كما ذكرنا سابقاً، من حيث تحديد مرتكبي جرائم الإرهاب الإلكتروني ومحاكمتهم في العصر الرقمي[١]. وعليه، من بين الطرق الكثيرة لتحقيق الولاية القضائية بموجب القانون الدولي، فيما يتعلق بالإرهاب الإلكتروني، قد تكون الولاية القضائية العالمية هي الأكثر تط رفاً، وإن لم تكن على الأرجح الأكثر إثارة للجدل. وبعيداً عن مصادر الاختصاص الأكثر تقليدية، تمنح الولاية القضائية العالمية "لأي دولة سلطة محاكمة المجرمين الدوليين المزعومين، حتى عندما لا يكون لدى الدولة الملاحقة أي صلة على الإطلاق بالجريمة ". وعلى الرغم من وجود اختصاص قضائي عالمي منذ عدة قرون، إلا أنه يبدو الآن أنه " يخرج من تلقاء نفسه كوسيلة منهجية لتعزيز المساءلة القانونية "[٢].

وبسبب الانتشار الواسع للولاية القضائية العالمية والصعوبات العملية المتأصلة التي يسببها الإرهابيون العاملون في الفضاء السيبراني، فإن الولاية القضائية العالمية هي أكثر الطرق فعالية لردع الإرهاب الإلكتروني، وتوفير المساءلة، وتعزيز السلم والعدالة الدوليين. ويرى الباحثون إن الحجج الداعية إلى توسيع نطاق الولاية القضائية العالمية لتشمل الإرهاب الإلكتروني كثيرة ومتباينة ومنها: أولاً: يمكن القول بأنه يوجد أساس في قانون المعاهدات أو القانون الدولي العرفي لتوسيع نطاق الولاية القضائية العالمية على مكافحة الإرهاب الإلكتروني. ثانياً: إن بشاعة الجريمة تتساوى مع الإرهاب التقليدي والإبادة الجماعية والجرائم المرتكبة ضد الإنسانية. وقد خضعت هذه الجرائم للولاية القضائية العالمية ليس لأنها كانت مماثلة للقرصنة، ولكن بسبب الطبيعة

الاتفاقيات الدولية المرتبطة بالأعمال الإرهابية، حيث يوجد العديد من الاتفاقيات في مجال حماية المجتمع الدولي من الأعمال الإرهابية، الواقعة على أمن الطيران المدني والملاحة البحرية، وكذلك المتعلقة بتجريم تمويل الإرهاب والهجمات الإرهابية بالقنابل. ومن بين الاتفاقيات الإقليمية نذكر على سبيل المثال الإتفاقية الأوربية لملاحقة مجرمي العمليات الإرهابية لعام ١٩٧١. انظر د. طارق سرور، الاختصاص الجنائي العالمي، ط١، دار النهضة العربية، القاهرة، ٢٠٠٦، ص١٣١-١٥٢.

(1) Prasad, K.(2012), cyberterrorism: addressing the challenges for establishing an international legal framework, Research Online -Edith Cowan University, Western Australia Perth, Australian Counter Terrorism Conference, p. 9. Available from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act. [Acceced at 28 December 2017].

(2)Gable,supra note ,4 at 29 , P.104

الجسيمة للجرائم. وعلاوة على ذلك، يمكن إجراء تشبيه للقرصنة، لا على أساس ما إذا كانت القرصنة محظورة أو لم تكن محظورة بسبب بشاعتها، بل تستند إلى تعريف القرصنة على أنها، جريمة ترتكب بصو رة عشوائية أو غير عشوائية ضد مواطني دول مختلفة في أعالي البحار. وأخيراً، فإن المسائل الأخرى المختلفة التي أثيرت في سياق الإرهاب التقليدي، من قبيل صعوبة تعريف الإرهاب وإمكانية عدم تطبيق الولاية القضائية العالمية، ليست مدعاة للقلق فيما يتعلق بالإرهاب الإلكتروني[١].

ويؤكد لوكاسيك[٢] على أنه من أجل تحقيق استجابة عالمية ناجحة للتصدي للجريمة الإلكترونية عبر الوطنية ومكافحة الإرهاب الإلكتروني، ينبغي توفير العناصر التالية قائمة: أولاً: المصطلحات الشائعة بين الأطراف المعنية في الحادث لتشمل تحديد طريقة عمل الدخيل، وتفاصيل الهجوم التقني، وتحديد الأهداف. ثانياً: معرفة المهارات التقنية لجميع الأطراف المشاركة في حل الحادث. ثالثاً: الاتفاقات القائمة بشأن كيفية التعامل مع حوادث مختلفة[٣].

وفي ضوء ما تقدم نرى إن الاختصاص القضائي العالمي يشكل اليوم أساساً مناسباً للتصدي للار هاب عموماً، والارهاب الالكتروني خصوصاً، ويشكل صورة مثلى للتعاون بين الدول على صعيد التعاون القضائي فيما بينها.

---

[١] Ibid, at 105.

[٢] Lukasik, S. J. (2001), Current and future technical capabilities. In A. D. Sofaer, & S. E. Goodman (Eds), the transnational dimension of cybercrime and terrorism (pp. 125-184). Stanford, CA: Hoover Institution Press Publication.

[٣] Ozeren, S.(2005), Global response to cyberterrorism and cybercrime: a matrix for international cooperation and vulnerability assessment(Doctoral dissertation, The university of north texas، p.49. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.4323&rep=rep1&type=pdf.

الخاتمة

من خلال بحثنا في التعاون الدولي في مواجهة الارهاب الالكتروني توصلنا الى عدد من الاستنتاجات والتوصيات، التي نلخص أبرزها كما يأتي:

أولاً: الاستنتاجات:

١) مصطلح (الارهاب الالكتروني) يمكن أن يطلق على إحدى الصور المستحدثة للارهاب، الذي تقوم به التنظيمات الارهابية، والذي يستهدف تحقيق أهداف الارهاب التقليدي، وذلك باستخدام تكنلوجيا المعلومات.

٢) يتميز الإرهاب الإلكتروني بكونه من الجرائم غير العنفية، التي ترتكب من خلال حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، كما أنه جريمة إرهابية متعدية الحدود، وغير خاضعة لنطاق إقليمي محدود، ومن الصعب إكتشافها وإثباتها، نظراً لسرعة إخفاء الدليل الرقمي، وسهولة إتلاف، كما يكون مرتكبها عادة من ذوي الاختصاص في مجال تقنية المعلومات، هذا إضافة الى خطورتها البالغة وأضرارها الكبيرة.

٣) بالنظر لخطورة الارهاب الالكتروني وأضراره البالغة فأن مواجهته تتطلب وضع استراتيجية خاصة للتعاون بين الدول في ظل مراعاة عدد من المعايير التي تعتمد في مواجهة أنماط الارهاب الالكتروني المختلفة.

٤) تتوزع الجهود الدولية في مكافحة الإرهاب الإلكتروني، إلى ثلاثة أنماط هي تجريمه في التشريعات الوطنية، والتعاون فيما بينها في مواجهته، وتفعيل دور منظمة الأمم المتحدة في ذلك. وتتمثل أبرز أوجه التعاون فيما بينها في التعاون التشريعي الدولي والتعاون الأمني الدولي والتعاون القضائي الدولي.

٥) يتحقق التعاون التشريعي الدولي في مواجهة الإرهاب الإلكتروني من خلال التعاون فيما بينها في اصدار طائفتين من التشريعات: الأولى تشريعات الجرائم الإلكترونية بقواعدها الموضوعية والإجرائية وتشريعات تنظيم الخدمات الإلكترونية والسلامة المعلوماتية. والطائفة الثانية تشريعات مكافحة الارهاب.

٦) لقد وضع المجتمع الدولي صكوكاً قانونية عالمية لمكافحة الإرهاب تحت رعاية الأمم المتحدة ووكالاتها المتخصصة، الا أنه لا توجد حتى الآن إتفاقية شاملة للأمم المتحدة بشأن الإرهاب عامة أو الارهاب الالكتروني خاصة.

٧) يجري التعاون الدولي التشريعي لمكافحة الجرائم الإلكترونية، وبضمنها الارهاب الالكتروني، وخاصة على صعيد مجلس أوربا والاتحاد الأوربي ومنظمة الدول الأمريكية وجامعة الدول العربية، وغيرها، من خلال ابرام الاتفاقيات الدولية وتشكيل المؤسسات الشرطية والأمنية المتخصصة لمواجهتها.

٨) يلعب (الأنتربول) ومكتب الشرطة الاوربية (اليوروبول) ووحدة التعاون القضائي (اليوروجست) وفرق التحقيق المشتركة دوراً كبيراً في تجسيد أهداف التعاون الأمني الدولي على صعيد مكافحة الارهاب الالكتروني في العالم.

٩) يلعب التعاون القضائي الدولي دوراً بارزاً في مكافحة الجرائم ومن بينها الإرهاب الإلكتروني ويتخذ هذا التعاون عدة أشكال، مثل تبادل الخبرات والمعلومات القضائية والمساعدة التقنية أو الإنابة القضائية أو مصادرة الأموال الناتجة من الجريمة المنظمة، أو تسليم المجرمين الهاربين او الإعتراف بالأحكام الجنائية أو نقل الإجراءات الجنائية، أو غير ذلك.

١٠) تعد الولاية القضائية العالمية ذات أهمية خاصة لردع الإرهاب الإلكتروني. حيث من الصعب للغاية تطبيق الولاية القضائية الإقليمية على الإرهاب الإلكتروني، نظراً لطبيعة الإنترنت وخصائص الإرهاب الإلكتروني العابر للحدود الوطنية لذلك يعد الإختصاص القضائي الإقليمي غير ملائم لمواجهة الإرهاب الإكتروني.

ثانياً: التوصيات:

١) نوصي بتعزيز الاطار القانوني والتشريعي عبر اصدار إتفاقية دولية خاصة بمكافحة الارهاب الالكتروني، مع النص كذلك على تجريمه في التشريعات الوطنية.

٢) نوصي بإرساء قواعد تعاون فاعل وحقيقي في مواجهة الارهاب الالكتروني على المستوى الدولي.

٣) نوصي بالعمل على تبادل المعلومات بين الاجهزة الأمنية المعنية بمواجهة الارهاب الالكتروني، وإنشاء خلايا عمل مشتركة تعمل على رصد تهديدات الارهاب الالكتروني وتبادل المعلومات بشأنها.

٤) نوصي بالعمل على لفت إنتباه مستخدمي الانترنيت الى خطورة الارهاب الإلكتروني من خلال مختلف ورش العمل التعريفية والإعلامية وضرورة الانخراط في مواجهته.

قائمة المصادر

أولاً: باللغة العربية:

أ-الكتب:

١) أحمد فتحي سرور، المواجهة القانونية للإرهاب، الطبعة الثانية، مركز الأهرام للترجمة والنشر-مؤسسة الأهرام، مصر ، ٢٠٠٨.

٢) حسنين المحمدي بوادي، الإرهاب الإلكتروني بين التجريم والمكافحة، دار الفكر الجامعي، الأسكندرية، ٢٠٠٥.

٣) د. طارق سرور، الاختصاص الجنائي العالمي، ط١، دار النهضة العربية، القاهرة، ٢٠٠٦.

٤) عادل عبدالصادق، الإرهاب الإلكتروني، القوة في العلاقات الدولية. نمط جديد وتحديات مختلفة ، مركز الاهرام للدراسات السياسة والاستراتيجية، القاهرة،٢٠٠٩ .

٥) عامر محمود الكسواني، التجارة عبر الحاسوب ماهيتها- اثباتها- وسائل حمايتها- القانون الواجب التطبيق عليها في الأردن - مصر - دبي، دار الثقافة، عمان، ٢٠٠٩.

٦) علاء الدين راشد، الأمم المتحدة والإرهاب قبل وبعد ١١ سبتمبر، دار النهضة العربية، القاهرة، ٢٠٠٥.

٧) علي جميل حرب، نظام تسلم واسترداد المطلوبين، تسليم المجرمين في القانونين الدولي والوطني، الموسوعة الجزائية الدولية، الجزء الثالث، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠١٥.

٨) عمرو عيسى- الفقي، الجرائم المعلوماتية (جرائم الحاسب الآلي والانترنت في مصر والدول العربية) ، المكتب الجامعي الحديث، الإسكندرية ، ٢٠٠٦.

٩) فيدا نجيب حمد، مكافحة الإرهاب قبل هجمات ١١ أيلول ٢٠٠١ وما بعدها، ط١، منشورات الحلبي الحقوقية ، بيروت ، ٢٠١٧ .

١٠) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية ، ٢٠٠٥.

١١) محمد عبدالله منشاوي، جرائم الانترنت من منظور شرعي وقانوني، مطبعة جامعة الملك فهد ، الرياض، ١٤٢٣ هـ.

١٢) محمد عوض الترتوري واغادير عرفات جويحان، علم الإرهاب (الأسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب)، دار الحامد عمان ، ٢٠٠٦.

١٣) محمد فاضل ، التعاون الدولي في مكافحة الجريمة، ط ٧، منشورات جامعة دمشق، دمشق ، ١٩٩٧.

١٤) محمود شريف بسيوني ، الجريمة المنظمة عبر الوطنية، ماهيتها ووسائل مكافحتها دولياً وعربياً ، ط١، دار الشروق ، القاهرة ، ٢٠٠٤ .

١٥) منير محمد الجنبيهي وممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي، الاسكندرية ، ٢٠٠٦.

١٦) يوسف حسن يوسف، الجرائم الدولية للأنترنت ، ط١، المركز القومي للأصدارات القانونية ، القاهرة ، ٢٠١١

ب: الرسائل الجامعية:

١٧) فهد سلطان محمد أحمد بن سليمان، مواجهة جرائم الإنترنت دراسة مقارنة، رسالة ماجستير، كلية الحقوق ، جامعة القاهرة ، ٢٠٠٤.

١٨) إسراء طارق جواد كاظم الجابري، جريمة الإرهاب الألكتروني ، (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة النهرين، العراق، ٢٠١٢.

١٩) تغريد سامي إبراهيم الطائي، جرائم الإرهاب الإلكتروني و آليات مكافحتها (دراسة تحليلية)، رسالة ماجستير، كلية العلوم الإنسانية، جامعة دهوك، ٢٠١٠.

٢٠) حيمر عبدالكريم ، منظمة الإنتربول، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة ،٢٠١٤ .

٢١) خليل يوسف جندي ميراني، سياسة التجريم في ظل العولمة، أطروحة دكتوراه، كلية القانون والعلوم السياسية، جامعة دهوك، ٢٠١٧.

٢٢) فنور حاسين، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة، رسالة ماجستير، كلية الحقوق بن عكنون، جامعة الجزائر ١، ٢٠١٣.

٢٣) ت: البحوث :

٢٤) أيسر- محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته ، بحث مقدم إلى الملتقى العلمي المعنون (الجرائم

المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية)، المملكة الأردنية الهاشمية، كلية العلوم الإستراتيجية ، ٢-٢٠١٤/٩/٤.

٢٥) حسن بن أحمد الشهري، الإرهاب الإلكتروني – حرب الشبكات - ، المجلة العربية الدولية للمعلوماتية ، المجلد الرابع ، العدد الثامن ، ٢٠١٥.

٢٦) حسن تركي عمير، وسلام جاسم عبدالله، الإرهاب الالكتروني ومخاطره في العص الراهن، مجلة العلوم القانونية والسياسية، عدد خاص، كلية القانون والعلوم السياسية، جامعة ديالى.

٢٧) ذياب البداينة ، جرائم الحاسب الدولية، بحث مقدم إلى أكاديمية نايف للعلوم الأمنية، الرياض ، ١٩٩٨.

٢٨) شعبان أبو عجيلة عصار، و أبو المعاي محمد عيسى، الرصد المبكر لخطر الجريمة، مجلة العلوم القانونية والشرعية، العدد السادس، جامعة الزاوية.

٢٩) عبد المحسن محمد احمد بدوي، دور برامج الإعلام في تنمية الوعي الأمني ومكافحة الإرهاب (المعوقات و التحديات)، ورقة عمل مقدمة ضمن اعمال الدورة التدريبية (الإرهاب والإعلام) بكلية التدريب، جامعة نايف العربية للعلوم الأمنية، الرياض، الفترة (٢٤-٢٠٠٩/١/٢٨).

٣٠) عبد العزيز مخيمر عبد الهادي، إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (مع الإشارة إلى جهود الوكالات الدولية المتخصصة بهذا الخصوص)، ورقة علمية مقدمة الى ندوة القوانين العربية والدولية في مكافحة الارهاب جامعة نايف العربية للعلوم الأمنية الرياض في ٥-٧ جمادي الثاني ١٤٣٤ هجرية.

٣١) فراس رشيد، مكافحة تجنيد الإرهابيين عبر الإنترنت، ورقة عمل مقدمة الى "الحلقة العلمية في مكافحة الإرهاب جامعة نايف العربية للعلوم الأمنية، المملكة الأردنية الهاشمية، ٢٠١٢م.

٣٢) مايا حسن ملا خاطر، الإطار القانوني لجريمة الإرهاب الإلكتروني، مجلة جامعة الناصر ، العدد الخامس، المجلد الأول ، يناير - يونيو ٢٠١٥.

٣٣) محمد أمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المجلة العربية للدراسات الأمنية والتدريب، الرياض ،١٤٢٢ هـ.

٣٤) محمد محمد الألفي، تشريعات الإرهاب الإلكتروني والافتراضي، بحث مقدم إلى الملتقى القضائي الأول (جرائم الإرهاب وأمن الدولة)، القاهرة، ٢٨-٢٠١٠/٦/٣٠.

٣٥) يونس محمد عرب، التدابير التشريعية لمواجهة أنشطة الإرهاب عبر الإنترنت، الندوة العلمية المعنونة (استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين)، القاهرة، ٢٥-٢٠١٠/١٠/٢٧.

ث: التقارير:

٣٦) الأمم المتحدة ، المجلس الاقتصادي و الإجتماعي، لجنة منع الجريمة والعدالة الجنائية الدورة الثالثة والعشرون، فيينا، ١٢-١٦ آيار/مايو ٢٠١٤ البند ٥(هـ) من جدول الأعمال المؤقت، الوثيقة E/CN.15/2014/18

٣٧) تقرير الإنتربول السنوي ، ٢٠٠٤.

٣٨) تقرير الإنتربول السنوي ، ٢٠١٥.

ثانياً: باللغة الإنكليزية:

أ: الكتب:

39) Dolliver, D. S.& Seigfried-Spellar, K. C.(2017) CYBERTERRORISM 1 Legal, Forensic, and Criminological Aspects of Cyberterrorism,(6 edition), [e-book].Wolters Kluwer Publishing House, Editors: Emil Pływaczewski.

ب: الرسائل الجامعية:

40) Alford, L. C. L. ، (2017). The Department of Defense effort to countering the cyberterrorism threat:Is the threat real or hyperbole? (Master's Thesis), 21-04-2017, National Defense University Joint Forces Staff College Joint Advanced Warfighting School.

41) Özeren, S.(2005). Global response to cyberterrorism and cybercrime: a matrix for international cooperation and vulnerability assessment(Doctoral dissertation, The university of north texas) .

ت: البحوث و التقارير:

42) Akati-Udi, T. (2015). Combating the growing threat of cyber terrorism، Special Conference 2 on International Cooperation, Model United Nations International School of The Hague | XXV Annual Session.

43) Bodin, S., Echilley, M. & Quinard-Thibault, O.(2015) , International cooperation in the face of cyber-terrorism : current responses and future issues, Themis competition Semi-Final A – International Cooperation in Criminal Matters.

44) Brunst , P. W. (2010). Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet, Max Planck Institute for Foreign and International Criminal Law , Freiburg , German,Springer Science,Business Media.

45) Chuipka , A. (2016). The Strategies of Cyberterrorism-is cybertwrrorism an effective means to Achieving the Goals if Terrorists?, Affaires publiques et internationales - Mémoires // Public and International Affairs .

46) Dogrul, M. , Aslan, A. & Celik, E.,(2011), Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.), CCD COE Publications.

47) Fidler, D. P.,(2016), Cyberspace, Terrorism and International Law, Journal of Conflict & Security Law, 21(3), Oxford University Press.

48) Gable, K. A. (2012) Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent, vanderbilt journal of transnational law,1(34).

49) Gercke, M.(2012), understanding cybercrime: phenomena, challenges and legal response, Telecommunication Development Sector, ITU publication, Switzerland.

50) Luca, G. (2017), Manifestations of contemporary terrorism: cyberterrorism-scientific review, research and science today, No. 1(13).

51) Nato Advanced Research Workshop (ARW) on the topic "Responses to Cyber Terrorism".NATO Science for Peace and Security Series: Human and Societal Dynamics، (2008), Volume 34, Centre of Excellence - Defence Against Terrorism(Ed) (3rd ed., 164 pp).hardcover، IOS Press, Ankara, Turkey.

52) Riglietti, G. (2016). Defining the threat: what cyber terrorism means today and what it could mean tomorrow، The Business Continuity Institute Reading, United Kingdom, The Business and Management Review, 8 (3).

53) Samuel, K. O., (2014), cyber terrorism attack of the contemporary information technology age: issues, consequences and panacea، International Journal of Computer Science and Mobile Computing, 3(5), pg.1082 – 1090, 2320–088X.

54) Sandler, T., Arce, D. G., Enders, W.(2011) An Evaluation of Interpol's CooperativeBased Counterterrorism Linkages, The Journal of Law & Economics, 54(1), pp. 79 -110, The University of Chicago Press for The Booth School of Business.

55) Stohl, M. , (2007), Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?, Crime Law Soc Change DOI 10.1007/s10611-007-9061-9, Springer Science & Business Media B.V.

56) United Nations Counter-Terrorism Implementation Task Force Working Group Compendium, (2011),Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects.

ثالثاً: الإتفاقيات والمواثيق الدولية:

٥٧) إتفاقية منظمة الدول الامريكية لمناهضة الإرهاب لسنة ٢٠٠٢.

٥٨) إتفاقية بودابست للجرائم السيبرانية لسنة ٢٠٠١.

٥٩) ميثاق منظمة الأمم المتحدة لسنة ١٩٤٥.

60) Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism(CETS No.217).

61) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems(ETS No.189).

رابعاً: المصادر الإلكترونية:

٦٢) رفد عيادة الهاشمي، الإرهاب الإلكتروني ، كتاب الإلكتروني ، متاح على الموقع الإلكتروني:

٦٣) سامر أبو رمان ، داعش (تنظيم الدولة) في عيون الشعوب، مركز بيان للبحوث و الدراسات، ب.ت. تأريخ النشر كتاب الإلكتروني، متاح على الموقع الإلكتروني:
http://albayan.co.uk/Fileslib/adadimages/malfat%20pdf/daesh.pdf
http://elaph.com/Web/News/2017/5/1148632.htm

٦٤) مبادئ استرشادية في مكافحة الإرهاب الإلكتروني، متاح على الموقع الإلكتروني:

٦٥) http://www.lasportal.org/ar/councils/ministerialcouncil/Documents/CyberSecurity%20EG+Notes.pdf

٦٦) بدر احمد، الإرهاب الإلكتروني أدواته وآثاره وأساليب الوقاية والعلاج، ١٦-١-٢٠١٧، بحث منشور متاح على الموقع الإلكتروني:
http://baathparty.sy/site/arabic/index.php?node=552&cat=15369

٦٧) عبدالله بن عبدالعزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول (حماية أمن المعلومات و الخصوصية في قانون الإنترنت)، القاهرة ، ٢ - ٤ يونيو ٢٠٠٨:
.http://www.shaimaaatalla.com/vb/showthread.php?t=3937

٦٨) عادل عبد الصادق، الأمم المتحدة و دعم الاستخدام السلمي للفضاء الإلكتروني، ٢٠١٥، بحث منشور، متاح على الموقع الإلكتروني:

http://accronline.com/article_detail.aspx?id=22762

٦٩) عبد المجيد الحلاوي، أهمية التعاون العربي و الدولي في مكافحة جرائم الارهاب المعلوماتي، الدورة التدريبية الخاصة بمكافحة الجرائم الارهابية المعلوماتية ، القنيطرة، المغرب، ٩-٢٠٠٦/٤/١٣، ص ٩-١١، متاح على الموقع الالكتروني: .https://repository.nauss.edu.sa/handle/123456789/57450

٧٠)الاتحاد الأوربي يوقع على البروتوكول الإضافي لإتفاقية مكافحة الإرهاب يركز على كيفية التعامل مع مشكلة المقاتلين الأجانب في سوريا والعراق، ٢٣ أكتوبر ٢٠١٥ ، الشرق الأوسط، متاح على الموقع الالكتروني:

https://aawsat.com/home/article/

٧١)هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، مقال متاح على الموقع الإلكتروني (تأريخ الزيارة ٢٠١٨/٥/٢٥):

http://araa.sa/index.php?view=article&id=244:2014-06-13-16-21-، 31&Itemid=294&option=com_content

٧٢)مقال منشور تحت عنوان، الاتحاد الأوربي يوقع على البروتوكول الإضافي لإتفاقية مكافحة الإرهاب يركز على كيفية التعامل مع مشكلة المقاتلين الأجانب في سوريا و العراق، ٢٣ أكتوبر ٢٠١٥ ، الشرق الأوسط، متاح على الصفحة الالكترونية (تاريخ الزيارة ٢٠١٧/١٢/٢٨): https://aawsat.com/home/article

٧٣) عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدم إلى المؤتمر الدولي الأول حول (حماية أمن المعلومات و الخصوصية في قانون الإنترنت)، القاهرة، ٢ - ٤ يونيو ٢٠٠٨. متاح على الموقع الإلكتروني (تأريخ الزيارة ٢٠١٧/١٢/٢٥):

http://www.shaimaaatalla.com/vb/showthread.php?t=3937.

٧٤)عبد المجيد الحلاوي، أهمية التعاون العربي والدولي في مكافحة جرائم الارهاب المعلوماتي، الدورة التدريبية الخاصة بمكافحة الجرائم الارهابية المعلوماتية ، القنيطرة ، المغرب، ٩-٢٠٠٦/٤/١٣.، ص ٩-١١، متاح على الموقع الالكتروني (تأريخ الزيارة ٢٠١٨/٢/٦):

https://repository.nauss.edu.sa/handle/123456789/57450

٧٥)مؤتمر بعنوان (الجريمة الالكترونية : تحد عالمي، استجابة عالمي)، نظم بالتعاون مع مجلس أوربا و إسبانيا، عام ٢٠٠٥، متاح على الموقع الإلكتروني:

http://www.oas.org/juridico/english/cyber_meet.html.

٧٦)إيهاب شوقي، الإرهاب الإلكتروني وجرائمه، ٧ ديسمبر ٢٠١٥، مقال منشور على الموقع الإلكتروني:

http://www.anntv.tv/new/showsubject.aspx?id=121062

٧٧) المؤتمر الدولي لتجريم الارهاب الالكتروني، ١٥-١٦ /٢٠١٧/٥، أبو ظبي، ايلاف، العدد ٥٨١٤ في ٢٠١٧/٥/١٩، متاح على الموقع الالكتروني :

https://www.mizandz.com/2017/11/pdf.html

78)Conway,M.& Bytes, R. ,(2002)Cyberterrorism and Terrorists "Use" of the internet, firsy Monday, peer-reviewed journal on the internet, 7(11-4) .Available from http://firstmonday.org/article/view/1001/922#author.

http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1631&context=ilr

Jacobs J. B., Blitsa D(2008) Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy.L.A. Int'l & Comp. L. Rev. 125. Available from

Organization of American States, AG/RES. 2040 (XXXIV-0/04), at ch. IV, f 8 (June 8, 2004), available from http://www.oas.org/juridico/english/ga04/agres_2040.htm.

Ozeren, S. (2005). Cyberterrorism and international cooperation: General overview of the available mechanisms to facilitate an overwhelming task, Responses to Cyber Terrorism, [E book], NATO Science for Peace and Security Series - E: Human and Societal Dynamics, 34, pages 34-88, IOS press, p. 81. Available from http://ebooks.iospress.nl/publication/24330 [Accessed 12 october 2017].

79)Prasad, K.(2012), cyberterrorism: addressing the challenges for establishing an international legal framework, Research Online -Edith Cowan

University, Western Australia Perth, Australian Counter Terrorism Conferenc. Available from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act.

Raustiala, K.(2009) does the constitution follow the flag? the evolution of territoriality in american law . Available from https://global.oup.com/academic/product/does-the-constitution-follow-the-flag-9780195304596?cc=us&lang=en&.

80)The Council of Europe Convention on the Prevention of Terrorism, Explanatory Report CETS No.196. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

الملخص

في عصر تزايد النشاط الإرهابي عبر الإنترنـت، أصبح الخـوف مـن الإرهـاب الإلكـتروني قائمـاً كونه جريمة حديثة ترتكب بواسطة تكنلوجيا الحاسوب، وذات طبيعة عـابرة للحـدود الوطنيـة. ونظراً لغياب إطار قانوني دولي شامل يتناول على وجه التحديـد مكافحـة هـذا التهديـد العـالمي، تواجه السـلطات والحكومـات في جميـع أنحـاء العـالم تحـديات بالغـة في العثـور عـلى المجـرمين ومحاكمتهم. لذلك كان لابـد للـدول والمـنظمات الدوليـة والإقليميـة أن تتخـذ خطـوات قانونيـة وتكنلوجية لمكافحة هذا التهديد العالمي، وهذا يتطلب التعاون الدولي الفعال، ومن هنـا يحـاول هذا البحث أن يوضح أوجه التعاون الدولي في هذا المجال وكيفيـة تطـويره. وعليـه تـم تقسـيم البحث إلى مبحثـين، يتنـاول المبحـث الأول ماهيـة الإرهـاب الإلكـتروني وخُصـص المبحـث الثـاني للبحث في صور التعاون الدولي في مواجهته.

پوخته

لەم سەردەمەدا زیـادبوونی چـالاکیی تیـرۆر لە ریـگەی ئەنترنیـتەوە، بـوەتە هـۆی ترسی رودانی تیرۆری ئەلیکترۆنی. وەك تاوانکیی نوێ وبەهۆی بەکارهێنانی تەکنەلۆجیـای کۆمبیـوتەرەوە ئەنجـام دەدرێـت، سـنوری نیشـتمانی دەبەزێنێـت. بە لەبەرچـاو گرتنـی نەبـوونی چوارچێـوەیەکی نیـودەوڵەتی گشـتگیر کە بەشـێوەیەکی دیـاریکراو کـار بـۆ قەلاچۆکردنی ئەم هەرەشـە جیهـانییە بکـات، دەسـەڵات و حکومەتەکـان لە سەرتاسـەری جیهـان ئاڵەنگـارییەکی زۆریـان رووبەرووبێـتەوە بـۆ دۆزینـەوەی تاوانبـاران و دادگـایی کردنیان. دەبوو کە وولاّتان وریکخراوە نێودەوڵەتی و هەرێمییەکان هەنگـاوی یاسـایی و تەکنەلۆژی بگرنەبەر بۆ قەلاچۆکردنی ئەم هەرەشە جیهانییە. هەربۆیە ئەم لایەنە پێویستی بە هاریکارییەکی چالاکی نێودەوڵەتی دەکات. لێرەدا ئەم تـوێژینەوەیە هەوڵـدەدا جۆرەکـانی هاریکاری نێودەوڵەتی وچـۆنیەتی بەرەوپێشـچوونی لەوبـوارەدا روون بکـاتەوە، هەربـۆیە ئەم توێژینەوەیە کراوە بەدوو بەشەوە؛ یەکەمیان خستنەرووی چەمکـی تیـرۆری ئیلکترۆنـی ، وبەشی دووەمیش تـایبەتکراوە بە شـێوازەکانی هاریکـاری نێـودەوڵەتی بەرەنگـاربونەوەی تیرۆری ئەلکترۆنی.

Abstract

In an age of increasing terrorist activity، the fear of cyber terrorism has come to exist. Cyber terrorism is a modern crime which primary designates the use of computer technology to commit which is transnational in charactor .

Effort to combat cybercrime is often hindered due to the existence of a large gap in legislative framework compatibility across international borders. The cross national nature of most cybercrime have imposed a series of challenges upon governments around the world in profiling the cybercriminal and prosecuting offenders. Thus، there is an urgent need for an effective international effort to combat cybercrime offences. In addition، there are a bilatearal efforts for international and regional institutions in deterring and combating cybercrime offences. Adopting relevant legislative and technology steps will enable to create a unified web of enforcement against cyberterrorist global threat.This reaserch presentas an outline of the effectiveness of international coperations to combat cyberterrorism and how to develop it. Morever، this paper divided into two parts. Part one discusses the concepts of cyber terrorism. Part two examines the forms of international cooperation in the confrontation it.