Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 14- Issue 1- June 2024 المجلد ١٤- العدد ١ – حزيران ٢٠٢٤

The role of international law in confronting the threat of electronic terrorism crimes

[1] Assist. Lecturer. Haneen Faiq Hussein
[1] Al-Mustansiriya University - College of Political Sciences
1: Email: haneenfaeq1205@uomustansiriyah.edu.iq
2: Email:

Abstract:

The crime of cyber terrorism is the greatest concern among many countries, especially since the crime of cyber terrorism has become an unknown danger that threatens the entire international community, due to its capabilities for extreme destruction across borders, as it represents a danger to countries that rely primarily on information technology to manage their administrative, security and economic interests. In light of the difficulty of combating cybercrimes, there must be international cooperation to strengthen international efforts, at the security, technical and judicial levels, between countries to protect their security and the safety of their individuals from the danger of misuse of information technology, which called for countries to sign several agreements to confront the danger of this crime. The first of these agreements was the International Convention to Combat Cybercrime, which was signed by thirty countries in the capital, Budapest, in 2001, and the Arab Convention to Combat Information Technology Crimes in 2010, which came to unify criminal policy at the Arab regional level to confront the threat of cybercrime, most notably the crime of cyberterrorism.

.

DOI
10.37651/aujlps.2024.146715.1188

Submitted: 24/3/2024
Accepted: 10/4/2024
Published: 1/06/2024

Keywords:
The crime of electronic terrorism
International efforts
terrorism.

دور القانون الدولي في مواجهة خطر جرائم الارهاب الالكتروني

[١] م.م حنين فائق حسين
[١] الجامعة المستنصرية _كلية العلوم السياسية

الملخص:

تعد جريمة الإرهاب الإلكتروني مصدر القلق الأكبر لدى العديد من الدول، لاسيما ان جريمة الارهاب الالكتروني اضحت تشكل خطراً مجهولاً يهدد المجتمع الدولي كافة، نظرا لقدراتها على التدمير الشديد العابر للحدود، كونها تمثل خطراً على الدول التي تعتمد على تقنية المعلومات بالدرجة الأولى في إدارة مصالحها الإدارية والأمنية والاقتصادية، وفي ظل صعوبة مكافحة جرائم الفضاء الإلكتروني، لا بد ان يكون هناك تعاون دولي لتعزيز الجهود الدولية، على المستوى الأمني والتقني والقضائي بين الدول لحماية امنها وسلامة افرادها من خطر اساءة استخدام تقنية المعلومات، الأمر الذي دعا إلى توقيع الدول على اتفاقيات عدة لمواجهة خطر هذه الجريمة، وكان من أول هذه اتفاقيات الاتفاقية الدولية لمكافحة الإجرام المعلوماتي التي وقعتها ثلاثين دولة في العاصمة بودابست لسنة ٢٠٠١، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠، والتي جاءت لتوحيد السياسة الجنائية على المستوى الاقليمي العربي لمواجهة خطر الجرائم الكترونية وفي مقدمتها جريمة الارهاب الالكتروني.

الكلمات المفتاحية:

جريمة الارهاب الالكتروني، الجهود الدولية، الارهاب، أمن المعلومات.

المقدمة

تنصب دراستنا على موضوع مهم من الموضوعات التي تهم القانون الدولي، ومن أبرزها موضوع (الإرهاب)، إذا أصبح حديث الساعة لدى الشعوب والأمم على اختلاف مستوياتهم، وإزاء تنامي قدرات التنظيمات الإرهابية في العالم واتساع جرائمها بشكل عام بعد التطور الذي شهده العالم في المجال التكنولوجي، والذي يعد اليوم من ضرورات الحياة اليومية لدى الأفراد للتواصل فيما بينهم وتبادل الأفكار وتحويل العديد من الأموال والبحث عن المعلومات... إلخ من المميزات التي حققها هذا التطور، إلا أنه أدى بدوره إلى ظهور العديد من الجرائم الإلكترونية العابرة للحدود، والتي لا يمكن لأي دولة منفردة القضاء عليها أو الحد من انتشارها، إلا عن طريق تعزيز الجهود الدولية والإقليمية في المجال الأمني والتقني والقضائي.

ويشكل "الإرهاب الإلكتروني" من الجرائم التي تشكل تهديدا حقيقيا للأمن والاستقرار في المجتمع الدولي أجمع، بسبب توظيف الجماعات الإرهابية لتقنية المعلومات في تنفيذ مخططاتها الإرهابية وعلى وجه الخصوص شبكة الإنترنيت، لتصبح أقوى في الوسائل وأوسع في المدى في نشر أفكارها الإرهابية، وتمويل أعمالها، التحريض على القتل والتخريب وتجنيد الارهابين، وما يترتب على هذه الجرائم من الوحشية ودرجة الأجرام في العصر الحاضر، من خلال سعي هذه المنظمات الارهابية لاختراق النظم المعلوماتية للأجهزة الامنية التابعة للدول، والتي تؤدي الى الحاق اضرار بسمعة الدولة ومعنويات مواطنيها لما يسببه ذلك من حدوث خسائر في الارواح والمؤسسات المادية، طالما ان هدف هذه الجماعات هو نشر الخوف والذعر بين المواطنين الابرياء.

ولم يسبق أن انشغل العالم في شتى بقاع الأرض بأمر أو قضية كما انشغل بالإرهاب الإلكتروني، مما تتطلب تضافر الجهود الدولية لغرض مواجهة الإرهاب الإلكتروني، لذلك وضعت في صدده المنظمات الدولية العالمية والإقليمية قرارات واستراتيجيات وبذلت العديد من الدول الجهود لتكون على مستوى من هذا التهديد الإرهابي.

أولاً: أهمية البحث:

يكمن الهدف من هذه الدراسة أو غرضها في معالجتها لجريمة جديدة وهي جريمة الارهاب الالكتروني والتي تعد من المواضيع الحديثة التي تلعب دور القانون الدولي، أذ كل ما تحتاجه هذه المجموعات هو بعض المعلومات لتتمكن من اختراق المواقع الإلكترونية الخاصة بالدولة، لذلك؛ يهدف هذا البحث إلى التعرف على دور المجتمع الدولي من منظمات ودول في مكافحة الارهاب الالكتروني، ومدى تأثيره على الأمن القومي، والإجراءات التي يجب اتخاذها في مواجهة الهجمات الإرهابية من خلال تفعيل الدور الدولي لمواجهة هذه الظاهرة الخطيرة.

ثانياً: مشكلة البحث:

تنطلق مشكلة البحث من إشكالية مفادها أن "الإرهاب الإلكتروني" أحدث تغيرا في شكل الصراعات الدولية، إذ نقل علاقات القوى بين الوحدات الدولية والصراعات العالمية إلى مرحلة متقدمة ومختلفة عما كانت عليه في السابق، إذ أصبحت العديد من دول العالم وأجهزتها الأمنية في مواجهة أشكال عديدة من جرائم الإرهاب الإلكتروني، والتي تمثل تهديدا مباشرا على الأمن الدولي وتأثر سلب على العديد من جوانب الحياة الاقتصادية والأمنية والعسكرية، بشكل يوجب حتمية التدخل الدولي الحازم لمواجهة مثل هذه الجرائم، لذا؛ يدور في البحث عدة تساؤلات قانونية منها، هل تستطيع الدول ايجاد تدابير قانونية ملائمة لمواجهة الارهاب

الالكتروني؟ ام ان الارهاب الالكتروني يجد له مداخل مناسبة ينفذ منها وينفذ عملياته التخريبية دون ان يكون للتدابير اية فاعلية ذات جدوى ومدى تأثير جريمة الارهاب الالكتروني على الامن الدولي؟ وما هي التدابير الدولية والاقليمية لمواجهة الارهاب الالكتروني في المجتمع الدولي؟

ثالثاً: منهجية البحث:

اتبعنا في دراستنا المنهجين المقارن والتحليلي، الذي يقوم على تحليل ظاهرة الجرائم الإلكترونية، وشرح النصوص القانونية المتعلقة بالإرهاب الإلكتروني، من خلال طرح النصوص القانونية والاتفاقية التي أشارت إلى ظاهرة الإرهاب الإلكتروني.

ووفقاً لما تقدم قسم موضوع البحث الى مبحثين نتناول في **المبحث الأول**: ظاهرة الإرهاب الالكتروني في النظام الدولي، والذي قسم الى مطلبين اولهما: التعريف بمفهوم الإرهاب الالكتروني والثاني: دوافع الإرهاب الإلكتروني، اما في **المبحث الثاني** تناولنا: الجهود الدولية لمكافحة جرائم الإرهاب الإلكتروني من خلال مطلبين الأول وضح: جهود المنظمات الدولية في مواجهه للإرهاب الالكتروني و الثاني: الجهود الإقليمية والعربية لمكافحة جرائم الإرهاب الإلكتروني

I. المبحث الأول

ظاهره الإرهاب الالكتروني في النظام الدولي

ترتب على التوسع في استخدام شبكات الإنترنيت وتكنولوجيا المعلومات في شتى مجالات الحياة إلى تنوع في أشكال التهديدات الناجمة عن هذا الإرهاب بشكل يمثل تهديدا يواجه التنظيم الدولي المعاصر، ولا شك في أن ظهور الهجمات الإلكترونية وتغير نمط النزاع المسلح وأشخاصه ووسائله، قد أثار التساؤلات حول الطبيعة القانونية للهجمات الإرهابية ومدى خضوعها للقانون الدولي، اذ تعد جريمة الارهاب الالكتروني ظاهرة من ظواهر العنف في المجتمع الدولي، ورغم خطورتها المتنامية كان هناك صعوبة في وضع تعريف محدد لها، لا سيما ان الإرهاب الإلكتروني يشكل في العديد من القوانين الوطنية والدولية جريمة تستحق العقاب عليها، مما يتطلب جهودا دولية بين حكومات الدول لتعزيز الأمان الرقمي ومواجهة التهديدات السيبرانية، وهو ما يستلزم في بداية الأمر في وضع تعريف محدد للإرهاب الإلكتروني.

I.أ. المطلب الأول

التعريف بمفهوم الإرهاب الالكتروني

أصبحت ظاهرة الإرهاب الإلكتروني الدولي محور اهتمام المنظمات الدولية والدول والأفراد على حد سواء[١]، إذ تعد من القضايا الجدلية على المستوى الدولي، لعدم وجود تعريف محدد للإرهاب الإلكتروني بشكل عام، بل حتى الآن لم يصل المجتمع الدولي لتعريف جامع مانع متفق علية، السبب في ذلك يعود إلى تنوع أشكاله ومظاهرة وتعدد في الأساليب المستخدمة، واختلاف وجهات النظر الدولية نتيجة حداثته، وافتقار الإرهاب التقليدي للتعريف دقيق، يمكن الاستناد إليه عند وضع تعريف للإرهاب الإلكتروني[٢].

بدأ استخدام مصطلح الارهاب الالكتروني في الثمانيات القرن الماضي، إذ استخدمه الخبير البريطاني (باري كولين)، المصطلح لأول مرة في عام ١٩٩٨، اذ قام بتطوير هذا المصطلح وبدا بتسليط الضوء على التهديدات الامنية الناشئة من عمليات الهجوم عبر شبكات الانترنيت، فعرفه بأنه: "الهجوم الإلكتروني، والذي يكون غرضه تهديد الحكومات أو العدوان عليها، سعيا منها لتحقيق أهدافها السياسية، الدينية أو أيدلوجية، ويجب أن يكون الهجوم مدمرا مكافئ للأفعال الإرهابية المادية والتخريبية"[٣].

ويعرف بعض الفقهاء الإرهاب الإلكتروني بأنه: "ارتباط أعمال الإرهاب بالتطورات الحديثة التي صاحبها ظهور الحواسيب الإلكترونية والإنترنيت، إذ لم يعد الإرهاب مقتصرا على جوانبه التقليدية كالتفجير والتفخيخ والقتل والإتلاف، بل أصبح من الأعمال التي تتم عن طريق أجهزة الحاسوب وشبكة الإنترنيت، حيث بات الإرهابي يجلس في قارة من الكرة الأرضية خلف حاسوب وبلمسه زر واحدة تمكنه من ارتكاب عمل إرهابي ينفذ في قارة أخرى"[٤]، وعرف أيضا بأنها: "استخدام الوسائل الكترونية صادرة عن دوله ما أو الجماعات، من خلال استخدام الفضاء الإلكتروني، أو بهدف ارتكاب أفعال مادية أو معنوية،

(١) محمد نعيم، *موسوعة القانون الدولي العام، قانون مكافحة الارهاب الدولي*، (بيروت: منشورات زين الحقوقية، ٢٠١٢)، ص٣٧.

(٢) عادل يوسف عبد النبي، "الجريمة المعلوماتية وازمة الشرعية الجزائية"، *بحث منشور في مجلة مركز الدراسات الكوفة*، (٢٠٠٨): ص ١١٢.

(٣) عادل عبد الصادق، *الارهاب الالكتروني، القوة في العلاقات الدولية نمط جديد وتحديات مختلفة*، (القاهرة: مركز الدراسات السياسية والاستراتيجية، ٢٠٠٩)، ص١٠٩.

(٤) نبأ نزار الربيعي، "مخاطر الارهاب الالكتروني وسبل مكافحتة"، مقال منشور على شبكة الانترنيت عبر الرابط الاتي: http://law.uobablyoun.eduliq، 2017.

أو التخويف أو التهديد، أو قد يكون هدف لهذا العدوان على نحو يؤثر على استخداماته السلمية"[١].

أما منظمة الأمم المتحدة فقد عرفت الإرهاب الإلكتروني في عام ٢٠١٢ بأنه: "استخدام الإنترنيت لنشر أعمال إرهابية"[٢] وعرفته وكالة الامن السيبراني على أنه: "كل عمل إجرامي يتم التحضير له باستخدام أجهزة الحواسيب، وشبكات الاتصال، والتي ينتج عنها تدمير أو تعطيل في الخدمات، بهدف نشر الخوف وزرع الشك لدى السكان، للتأثير على الحكومات والسكان في الدولة، لخدمة الجماعات السياسية أو اجتماعية أو أيدلوجية"[٣]

وعليه فأن اغلب التعريفات المتعلقة بالإرهاب الالكتروني تنطلق من تعريف الارهاب التقليدي اذ لا يختلف كلاهما الا من حيث الطريقة او الوسيلة التي يلجأ اليها الجاني لتحقيق العمل الارهابي، وعليه فأننا نعرف الارهاب الالكتروني بانه: (كل سلوك اجرامي ارادي يرتكبه فرد او مجموعة افراد باستخدام الوسائل الالكترونية وتضمن انتهاكا لاحد مبادى القانون الدولي، سواء اكان هذا السلوك باسم او ايعاز او بدعم وتشجيع ام برضا من دولة ما، او احدى المنظمات او الهيئات الرسمية، او ارتكبت بشكل اعتداء او تهديد المصلحة محمية دولية عبر الوسائل الالكترونية)، اذ يتضح لنا من خلال التعريف مدى الارتباط الوثيق للإرهاب الالكتروني بالتطور التكنولوجي، اذ بات هذا التقدم التكنولوجي يلعب دورا مهما في كافة جوانب الحياة، فضلا عن حجم المخاطر التي يمكن ان يسببها، اذ تزداد خطورة الارهاب الالكتروني، وفي الدول المتقدمة، تتم إدارة البنية التحتية لها عن طريق أجهزة الكمبيوتر وشبكات المعلومات، مما يجعلها اهدافا سهله للهجمات، ولا تحتاج هذه الجماعات الى استخدام المتفجرات، بل فقط عن طريق النقر على لوحة المفاتيح لتدمير البنية التحتية المعلوماتية لدولة ما ومهاجمتها، مما يسبب اثارا مدمره، فالإرهاب الالكتروني يعد خطرا قائما ومحدقا، نظرا لتنوع وسائله وتوسع نطاقه، فانه يجعل من الممكن مهاجمه الدول عبر وسائل الاتصالات وتكنولوجيا المعلومات، في اجواء توفر درجة كبيرة من السلامة والامان للإرهابيين.

وفي الآونة الأخيرة أصبح الإرهاب الإلكتروني يشكل تهديد للأمن والسلم الدوليين، فضلا عن الآثار الضارة على العلاقات الدولية، ويحدث ذلك في حال الشك بدوله ما بقيامها

---

(١) عادل عبد الصادق، *الارهاب الالكتروني نمط جديد وتحديات مختلفة*، (مصر: مركز العربي لأبحاث الفضاء الالكتروني، ٢٠١٣)، ص٢.

(٢) علي مطر، "الارهاب الالكتروني في القانون الدولي: نوع جديد لم يتم التعامل معه بعد"، مقال صحفي، https://www.inbaa.com/%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8 2013،.

(٣) ريهام عبد الرحمن، "اثر الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية، دراسة حالة تنظيم داعش"، بحث منشور على شبكة الانترنيت عبر الرابط الاتي: ٢٠١٦ https://democraticac.de/?p=34528

بتجنيد ارهابين عبر الوسائل الإلكترونية، وتحريض الإرهابيين من خلال هذه الوسائل للاستهداف دوله أخرى، مما سيؤدي إلى آثار سلبية بينها وبين الدول المتضررة من الإرهاب الإلكتروني، قد تصل أحيانا إلى مرحلة مقاطعة تلك الدولة. من الأمثلة على ذلك ما فعلته عصابات داعش والقاعدة، من خلال استخدامهم للوسائل التكنولوجية لقيامها بأعمالها الإرهابية، والتي أدت إلى توتر العلاقات الدولية وتهديد الأمن الدولي.

وما قام به موقع" ويكيلكس "والذي يعرف" بصراع الإلكتروني ذو طبيعة ناعمة "وهي جرائم لا تحتاج عنفا ولا سفك للدماء إذ تعرف بطبيعتها الهادئة، وكل ما تحتاج إليه هذه الجرائم هو القدرة على التعامل مع الحاسوب على مستوى عال من التقنية لارتكاب الأفعال غير المشروعة(١)، وأدى هذا الصراع الإلكتروني في الحصول على المعلومات والأسرار واستخدامها عبر المنصات الإعلامية وتسريبها، والذي يكون ذا تأثير على طبيعة العلاقات الدولية، فإن هذا الصراع سيشكل تهديدا للسلام العالمي، لكونه حرب إلكترونيات بين الدول، يتسبب في إضرار بالأمن والسلم الدولي(٢)، فضلا عن تأثير هكذا نوع من الجرائم على العلاقات الدبلوماسية الدولية، كونها تتم من خلال جمع المعلومات والتجسس، وتسهيل الأنشطة السرية في العلاقات الدولية، لدرجة أن هذه الجرائم تحدث من دولة إلى دولة أخرى، وتعريضها للخطر نتيجة حدوث عمل إرهابي على إقليمها وتأثيره على مصالح دولة أخرى كوقوعه على أعضاء السلك الدبلوماسي أو على رعايا عدة دول أو على وسائل نقل أجنبية، من الأمثلة التطبيقية على ذلك ما حدث في سنة ٢٠١٥ عندما أفاد مكتب الإدارة الشخصية التابع للحكومة الأمريكية أن قراصنة تمكنوا من سرقة ما يقارب أربعة ملايين من بيانات الموظفين الفدراليين،" وقد تم اتهام حكومة الصين بالوقوف خلف هذه العملية التي تعد الفاجعة الأكبر في البلاد، إذ تمكنها هذه العملية من تجنيد جواسيس نظرا لأهمية المعلومات المسروقة والتي تمكنها من الوصول إلى أسرار أمن الدولة الأمريكية(٣).

وبناء على ما تقدم فإن الإرهاب الإلكتروني له عدة آثار، منها ما يؤثر على مجرى العلاقات الدولية من خلال تجنيد الإرهاب عبر شبكات الإنترنيت وتحريضهم ضد الدول الأخرى، وكذلك في تأثيره على المجال السياسي إذ إنه يهدد الوحدة الدولية بالتفكك والنيل من سمعه الدولة وهيبتها، فضلا عن الجانب الأمني والذي يفضي إلى عدم الشعور بالأمن والطمأنينة جراء هذه الجريمة، وعن تأثيرها في الجانب الاقتصادي للدول نتيجة للشل الذي

(١) خليل يوسف جندي،" المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني(دراسة مقارنة)"، *بحث منشور في مجلة القانون للعلوم السياسية، جامعة كركوك*، (٢٠١٨): ص٩٣.
(٢) حمدان رمضان محمد، "الارهاب الدولي وتداعياته على الامن والسلم العالمي دراسة تحليلية من منظور اجتماعي"، *بحث منشور في مجلة ابحاث التربية الاساسية جامعة الموصل*، (٢٠١١): ص٢٨٢-٢٨٣.
(٣) محمود رجب فتح الله، *الوسيط في الجرائم المعلوماتية*، (الإسكندرية: دار الجامعة الجديدة، ٢٠١٩)، ص٥١٩.

يصيب عجلة الإنتاج إلى غير ذلك من الآثار في مختلف المجالات، إذ إن كل هذه الأفعال الناجمة عن جريمة الإرهاب الإلكتروني تؤثر وتهدد أمن المجتمع الدولي ككل.

I.ب. المطلب الثاني

دوافع الإرهاب الالكتروني

تتعدد دوافع الإرهاب الإلكتروني وتختلف في درجة أهميتها، فهنالك اتجاهات سياسية وظروف اقتصادية وأحوال الاجتماعية وكذلك الاختلاف الديني والعقائدي التي تؤدي وتشجع هكذا عمليات إرهابية، تكون هي الدافع وراء ظاهرة الإرهاب بشكل عام، كما أن هناك عوامل كثيرة تجعل من ظاهرة الإرهاب الإلكتروني موضوعا مناسبا وسهلا للجماعات الإرهابية والتنظيمات المسلحة، وتتنوع هذه الدوافع وتختلف باختلاف الأطراف المتورطة، ويمكننا إيجاز هذه الدوافع فيما يأتي:

أولا: الدوافع الشخصية للإرهاب الالكتروني:

ان افتقار الإنسان لدوره في الأسرة والمجتمع وفشله في الحياة، وكذلك الإخفاقات العلمية أو العملية أو النواحي الوظيفية، أو التجارب العاطفية، تجعله يشعر بالفشل في الحياة، كل هذا يؤدي إلى اكتساب بعض الصفات غير مرغوب فيها، بما في ذلك عدم إحساسه بالانتماء والولاء لوطنه، فعلى سبيل المثال الشاب الذي فقد معنى الحياة في مختلف دول العالم، بسبب الظلم وعدم المساواة والفقر وانعدام الحياة الكريمة وغيرها من الأسباب، من الممكن أن ينحرف بسهولة ويقع في عالم الجريمة والإرهاب.

نتيجة لذلك، فان التفكك الاسري والاجتماعي والطفولة المضطربة والانطوء على النفس، الذي يعيشها الفرد، كل ذلك يولد لديه العدوان والانحراف والارهاب، مما يؤدي به إلى الجنوح وعدم الشعور بالانتماء والولاء للوطن، فضلا عن أن الشخص يكون غير مؤهل فيبحث عما يؤهله، كحب الظهور والشهرة[١]، وانعدام التربية، وغياب لغة التفاهم والحوار بين افراد المجتمع، كل ذلك من شانه ان يؤدي الى تفشي ظاهرة الارهاب.

ثانيا: الدوافع الدينية والفكرية للإرهاب الالكتروني:

وتتمثل في الفراغ الفكري، والفهم الخاطئ لمبادئ الدين الحنيف وآدابه وسلوكه، وسوء التفسير والجهل بمقاصد الشريعة الإسلامية، حيث تقوم الجماعات الارهابية بشن

(١) زين العابدين عواد كاظم الكردي، *جرائم الإرهاب المعلوماتي، دراسة مقارنة* ، ط ١ ، (بيروت: منشورات الحلبي الحقوقية، ٢٠١٨)، ص ١٠٣ – ١٠٩.

هجماتها الالكترونية لتعزيز افكارها الدينية والايدولوجية، واعتماد الشباب على بعضهم البعض دون الرجوع إلى العلماء والانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة.

فالتطرف الفكري او الديني هما الجذور الايدلوجية، التي أدت الى زيادة الإرهاب، كما ساهمت أو ساعدت في ظهور سياسات غير عادلة وقسرية، فالتطرف الديني خطير للغاية في أي مجال، وخاصة في الجهل الفكري، فالتعصب الديني يدفع فئة معينة الى استعمالها للعنف من اجل فرض مبادئها المتطرفة على المجتمع[١].

ثالثا: الدوافع السياسية للإرهاب الالكتروني :

قد يكون السبب من وراء الهجمات الإلكترونية دوافع سياسية تهدف إلى التأثير على القرارات السياسية، أو من أجل تحقيق غايات سياسية من ورائها، انعدام العدالة الاجتماعية، والتوزيع غير العادل للثروات الوطنية، كما أن التفاوت في توزيع الخدمات والمرافق العامة، واختلاس الأموال العامة، وانعدام التنمية المستدامة، وإهمال شؤون الرعايا، ومعاناة بعض المجتمعات والشعوب الدولية التي تعاني من الظلم والاضطهاد والسيطرة الاستعمارية، وعدم السيطرة على ثقة الناس وصدقهم وتسهيل حياتهم وشؤونهم الإنسانية.

فضلا عن الظلم والاضطهاد والاستعمار التي تعاني منها بعض المجتمعات والشعوب الدولية، أن الاستعمار، والانتهاكات الصارخة للحقوق والحرمات، وسرقه الأموال والمقدرات، وانتهاك القوانين والمواثيق الدولية، تدفع هذه الشعوب نحو التطرف، إضافة إلى السياسات المجحفة، التي تنتهجها بعض الدول تجاه مواطنيها وشعوبها، والقمع السياسي للمواطنين، وتهميش دورهم وتغييبهم عن المشاركة السياسية، وانتهاك الحقوق، وعدم استيفاء متطلبات التوازن الاجتماعي، وعدم تفعيل أدوارهم في المؤسسات، كما أن العديد من الدول العربية والإسلامية، لم تقف عند حد تهميش هذه الجماعات الإسلامية، وإنما تصدت لها ووقفت في وجهها، وجمدت نشاطاتهم وعطاءهم.

حتى في الدول المتقدمة التي تدعي الديمقراطية وحرية التعبير عن الرأي[٢]، ادى كل ذلك إلى نشوء ردود الفعل والمنظمات السرية ضد الدول، الأمر الذي من شأنه أن يدفع القوميات المضطهدة التي لا تستطيع تحقيق مطالبها إلى نشوء نزعة إرهابية لديهم، في سبيل أن تستحصل على جزء من المكاسب التي تطمح في الوصول إليها. كما يؤدي غياب الدور الذي تلعبه الأحزاب السياسية، وانشغالاتها في صراعاتها على السلطة، وتعاون بعضها

(١) مصطفى سعد حمد مخلف، "جريمة الارهاب عبر الوسائل الالكترونية"، (اطروحة دكتورا، جامعة الشرق الاوسط، الاردن، ٢٠١٧)، ص ٢٠-٢٣

(٢) اسراء طارق جواد كاظم، "جريمة الإرهاب الالكتروني دراسة مقارنة"، (رسالة ماجستير تقدمت بها الى كلية الحقوق جامعة النهرين،٢٠١٢)، ص٣٤

وتحالفهم مع بعض المؤسسات، التي تدعم الإرهاب لتحقق غاياتها وأهدافها للوصول للسلطة أو توليها الرئاسة.

رابعا: الدوافع التكنولوجية للإرهاب الالكتروني:

يشن الإرهاب هجماته في بعض الأحيان من خلال استغلال الثغرات الأمنية، أن بنية شبكة المعلومات في هذه الدول ضعيفة ومعرضه للتسلل وتدميرها للبناء التحتية لدولة ما وتخريبها، من قبل التنظيمات الإرهابية، وذلك نتيجة لكون شبكات المعلومات في هذه الدول تتسم بكونها مفتوحة، وليس لها أي قيود أو حواجز أمنية، واحتواء شبكات المعلومات على العديد من الفجوات، والتي من شأنها أن تسهل الدخول لها[١]، علاوة على ذلك، فإن استخدام تقنيات التشويش في الخدمات الرقمية الوطنية أمر غير مرغوب فيه، والتخريب بقصد الإضرار بالخدمات الإلكترونية وإلحاق الأذى بها[٢].

وان صعوبة إثبات الجرائم السيبرانية، والتي لا يعلم بوقوعها أصلا خاصة في مجالات جرائم القرصنة، كل ذلك يساهم في مساعدة الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته، فصعوبة الإثبات تعد من أقوى دوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني لأنها تعطي المجرم أملا في الإفلات من العقوبة، فضلا عن عدم وجود اتفاقيات دولية وتشريعات وطنية بشأن الإرهاب الإلكتروني الدولي، مما أدى إلى ظهور انتشار وتوسع هذه الظاهرة بشكل متزايد، أو انتشارها في دول العالم، وأن عدم وجود سلطة مركزية موحدة للسيطرة على ما يتم عرضه على الشبكة، والتحكم في مدخلاته ومخرجاته، يعد سبب مهم في انتشار ظاهرة الإرهاب الإلكتروني.

فان اي شخص يمكنه الدخول ووضع أي شيء يريده على الشبكة، ويعتبر هذا هو السبب الرئيس للانتشار الإرهاب الإلكتروني، والطريقة المثالية والخيار الأسهل للمنظمات والجماعات الإرهابية[٣]، لذلك لا بد من فهم هذه الدوافع وتدريب الجهات الأمنية في الدولة، كل ذلك من شأنه أن يساعد في تطوير استراتيجيات فعالة للدفاع عن الأمن السيبراني ومواجهة تهديدات الإرهاب الإلكتروني

وعليه فإن دوافع الإرهاب الإلكتروني ليست نتيجة لعامل واحد بل هي محصلة لجملة من العوامل الداخلية والخارجية والمشتركة، والبيئية، وظروف الزمان والمكان، لذلك لا بد من نشر ثقافة التسامح، ونبذ التطرف والإرهاب والفرقة والاختلاف، وهي مسؤولية تقع على كاهل الدولة والمجامع الدولي ككل للحد من هذه الظاهرة لذلك لابد أن يكون هناك تنظيم وقوانين رادعة لمثل هكذا نوع من الجرائم، ونتيجة لما تقدم فان الإرهاب الإلكتروني يستخدم

---

(١) عبدالله بن عبد العزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات"، *بحث مقدم الى المؤتمر الدولي الأول حول حماية أمن المعلومات وخصوصيته في قانون الإنترنت، المنعقد بالقاهرة*، في المدة من ٢-٤ يونيو، (٢٠٠٨): ص ٤.

(٢) مصطفى يوسف كافي، وآخرون، *الإعلام والإرهاب الإلكتروني*، ط ١ ، (الأردن: دار الإعصار العلمي للنشر والتوزيع، ٢٠١٥)، ص ١٥١.

(٣) حوراء رشيد مهدي الياسري، "الإرهاب الإلكتروني وطرق مواجهته ٢٠١٧ "، مقالة منشورة على شبكة الإنترنت عبر الرابط الآتي: https://m.annabaa.org/arabic/informatics/11123 آخر زيارة للموقع ٢/١٠/٢٠٢٣

تكنولوجيا المعلومات وشبكة الإنترنيت لتنفيذ الهجمات الإرهابية من خلال اختراق أنظمة الحواسيب الآلية التابعة للدول، ونشر الأخبار الزائفة والتلاعب بالمعلومات من أجل تحقيق أهدافها الإرهابية، وعليه لابد أن يكون هناك تعاون بين حكومات الدول والمنظمات الدولية لمواجهة خطر الإرهاب الإلكتروني، وتعاون العديد من الدول فيما بينها من أجل وضع تشريعات وآليات لمواجهة الإرهاب الإلكتروني، من خلال تنسيق الجهود على الصعيد الوطني والدولي لمكافحة الأشخاص والجماعات المشتركة في هكذا أنشطة.

II. المبحث الثاني

الجهود الدولية لمكافحة جرائم الارهاب الالكتروني

بعد التطور التكنولوجي الهائل أصبح العالم كالقرية الصغيرة، بسبب التقنيات المتطورة ووسائل الاتصال الحديثة، والعلاقات المتنوعة والمصالح المتبادلة بين الشعوب، الأمر إلى يقضي ظهور التعاون الدولي في كافة المجالات، ومن أهم صور التعاون الدولي هو التعاون في المجال الأمني بين دول العالم عامة والدول العربية خاصة، لأن هذا التعاون أصبح أمرا حتمي كونه السبيل الوحيد لتغلب على المعوقات والعقبات التي تواجه الدول في محاولاتها لتصد للإرهاب، لا سيما بعد زيادة الإحصائيات المروعة والمخاطر الناجمة عن الإرهاب الإلكتروني، إذ باتت تشكل تهديدا للمجتمع الدولي.

وبما أن جريمة الإرهاب الإلكتروني ذات طابع دولي عابرة للحدود، إذ لا تقف عن حدود دولة معينة، كان إلزام على المجتمع الدولي والإقليمي الالتفات إلى التكاتف وتوحيد جهودها لمكافحة هكذا نوع من الجرائم الدولية، وهذا ما سعت إليه منظمة الأمم المتحدة حيث عقدت العديد من المؤتمرات لمكافحة جرائم الإرهاب الإلكتروني وأصدرت بشأنها العديد من التوصيات، كما عقدت عدة اتفاقيات دولية منها عالمية وأخرى إقليمية لمواجهة خطر الإرهاب الإلكتروني.

وعليه سنتناول في هذا المبحث الجهود الدولية والإقليمية في مكافحتها للإرهاب الإلكتروني من خلال مطلبين

II.أ. المطلب الأول

جهود المنظمات الدولية في مواجهه الإرهاب الالكتروني

يتسابق اشخاص القانون الدولي و الداخلي من دول ومنظمات دولية، وشركات ومنظمات مجتمع مدني وجمعيات وحتى افراد لدعم جهود مكافحة الارهاب بكافة اشكاله وصوره ومنها الارهاب الالكتروني، اذ تنصهر في مواجهة هذه العقبة، كافة التوجهات السياسية والفلسفات الاقتصادية. فمنذ نشأة الدولة الحديثة كانت ولا تزال الحاجة الى الأمن، تتطلب تعاون دولي اممي كوني من اجل اشباعها وذلك بفعل التهديدات الارهابية التي

تجاوزت الحدود وتخطت الحدود الجغرافية المكانية لكل دولة لتصل الى مستوى العالمية ،فالإرهاب الالكتروني وما يتركه من تهديد على جميع انحاء العالم شجع الدول على زيادة بل مضاعفة جهودها في مجال محاربة الارهاب باستخدام التقنيات الحديثة، اذ تشهد الفترة الحالية جهودا دولية متزايدة لمواجهه خطر الارهاب الالكتروني، اذ يعد الارهاب ظاهرة دائمة التغير، ونتيجة لذلك، فأن الوسائل التي تعتمد عليها هذه التنظيمات تتغير باستمرار، لمواكبة مع التطورات التكنولوجية لتحقيق اهدافها الارهابية، فقد قامت الجماعات الارهابية على اختلاف اشكالها وانماطها الفكرية الاستفادة من المزايا الالكترونية لتحقيق ودعم اهدافها الاجرامية، وتحولت الى مجتمع افتراضي غير محدد الابعاد، كان لذلك الدور الكبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات، منذ عام ١٩٩٩، اذ تتمتع جميع هذه التنظيمات الارهابية بحضور كبير على شبكة الانترنيت، وبعد عام ٢٠٠١ كان هناك اكثر من (٥٠٠٠) موقع الالكتروني وغرف دردشة تابعة لهذه الجماعات، استخدمتها في التأثير على الرأي العام من خلال معاركها الفكرية، واستخدامها ايضا للقيام بأعمالها الارهابية عن طريق جمع المعلومات والتنسيق والتنظيم، بهدف زعزعة الامن ونشر الخوف والرعب[١]، وتهديد وابتزاز كل من الاشخاص والسلطات العامة والمنظمات الدولية، وعليه ادركت الدول والمنظمات اهمية التعاون الدولي فيما بينها بغاية وضع حد لهذه الجماعات الارهابية، فعمدت الى عقد اتفاقيات لتسهيل مهمة التحقيق في جرائم الارهاب الالكتروني.

وعلى راس الجهود الدولية الدور الملحوظ للمنظمة الامم المتحدة والتي بذلت جهدا لا يستهان به في مجال مكافحة الارهاب الالكتروني، حيث اتخذت العديد من الاجراءات لتعزيز الامان العالمي ومكافحة هكذا نوع من التهديدات الارهابية، اذ اكدت على وجوب تعزيز العمل المشترك بين اعضاء المنظمة من اجل التعاون للحد من انتشارها(٢)، وتمثل هذا الجهد من خلال المؤتمرات التي عقدها لمنع الجريمة ومعاملة المجرمين[٣]، بدء من المؤتمر السابع في سنة ١٩٨٥ حتى المؤتمر الثاني عشر عام ٢٠١٠، بالإضافة الى المؤتمر الخامس عشر للرابطة الدولية لقانون الجنائي، والذي اقام بإشراف منظمة الامم المتحدة عام ١٩٩٤، ففي المؤتمر السابع المنعقد في ميلانو كلفت فيها لجنة الخبراء بدارسة مشكلة حماية انظمة المعالجة الالية والهجمات على الحاسوب الالي واعداد تقرير عنها، يعرض على الدورة الثامنة والتي عقدت في هافانا سنة ١٩٩٠، والتي تم فيها عرض العديد من التوصيات، بما في ذلك التأكيد على فوائد واهمية التطور الالكترونية لمواجهة الجرائم الالكترونية، كما شدد ايضا على الحاجة لتحديث القوانين التي تعالج هذه الجرائم، وتدريب القضاة والمسؤولين في كيفية

(١) صباح كزيرة، امال كزير، "الارهاب الالكتروني وانعكاساته على الامن الاجتماعي، دراسة تحليله"، *مجلة التراث*، (٢٠١٨): ص٣١٦.

(٢) علي جبار الحسيناوي، *جرائم الحاسوب والانترنيت*، (الأردن: دار اليازوري العلمية للنشر والتوزيع، ٢٠٠٩)، ص١٤١.

(٣)علي يوسف الشكري، *المنظمات الدولية*، (عمان: دار الصفاء للنشر والتوزيع، ٢٠١٢)، ص٩٧-٩٨.

التحقيق والمحاكمة في هكذا نوع من الجرائم، وفي سنة ١٩٩٥ انعقد مؤتمر الامم المتحدة في القاهرة والذي اوصى بوجوب حماية الانسان نظرا لتزايد المخاطر التكنولوجية، وضرورة التنسيق والتعاون بين اعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة، أما مؤتمر بودابست سنة ٢٠٠٠، فاعتبر جرائم الحواسيب الالكترونية بمثابة نموذج من الجرائم المستحدثة، والتي اوجب فيها التشدد لوضع حد لهكذا نوع من الجرائم(١).

ونبه مجلس الأمن أيضا في قراره ذي العدد ١٩٦٣ لسنة ٢٠١٠ "أن الإرهابيين يستخدمون التكنولوجيا الجديدة للمعلومات والاتصالات بشكل متزايد للتجنيد من خلال شبكات الإنترنيت، فضلا عن التحريض على دعم الأعمال الإرهابية"، على اعتبارها أنماطا جديدة في استخدام الإرهابيين لبيانات شبكة المعلومات الدولية، وكان القرار ذو العدد (٢٢٥٥) في شباط لسنة٢٠١٥ أكثر شمولا، بشأن طرق استخدام الإرهابيين للإنترنت في الأنشطة الإرهابية، بما في ذلك "الإعراب عن القلق بشأن الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات من قبل الإرهابيين، ولا سيما شبكة الإنترنت لتنفيذ عمالها الإرهابية والتحريض على الإرهاب أو تجنيد أو تمويل مرتكبي هذه الجرائم"

كما أقرت المنظمة في مؤتمرها المنعقد في سلفادور المؤتمر الثاني عشر، لمنع الجريمة والعدالة الجنائية لعام ٢٠١٠، بعنوان "الاستراتيجيات الشاملة لمواجهة التحديات العالمية"، لتنظيم منع الجريمة والعدالة الجنائية وتطورهما في عالم متغير، وتضمن المؤتمر ثمانية بنود، من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة جرائم الإرهاب الالكتروني (٢).

وعلى الرغم من ذلك لم ينص ميثاق المنظمة بشكل صريح على اعتبار استخدام الإنترنيت، كأداة إرهابية من ضمن ما يعد ب" الارهاب الالكتروني "، إلا أن الميثاق اتفق بتجريم استخدامها باعتبارها انتهاكا لما جاء فيه بشأن" التهديد أو استخدام العنف ضد سلامة الأقاليم أو الاستقلال السياسي لدولة "، فضلا عن ذلك أنه جاء لمواجهة النزاعات المسلحة، باعتبار إن استخدام الإنترنيت في حرب المعلومات تقع ضمن إطار العدوان، إذ إن الإرهاب من النوع الذي لا يتفق مع سيادة الدول، لما فيه من تهدد للعلاقات الدولية باستعمال القوة، أو

(١) محمود احمد القرعان، *الجرائم الالكترونية*، (الأردن: دار وائل للنشر والتوزيع، ٢٠١٧)، ص١٥٦.
(٢) مجمع البحوث والدراسات الاكاديمية السلطان قابوس لعلوم الشرطة، *الجريمة الالكترونية*، (عمان: ٢٠١٦)، ص١٧٠.

استخدامه ضد سلامة أراضيها أو استقلالها السياسي، بشكل الذي لا يتفق مع مقاصد وأهداف منظمة الأمم المتحدة[١].

أما المنظمات العالمية المتخصصة كمنظمة الاتحاد الدولي للاتصالات ومن ضمن مساعيها الأكثر شمولا عند عقدها القمة العالمية لمحاربة الجرائم الإرهابية، في تونس سنة٢٠٠٥[٢]، والمؤتمر الدولي حول الأمن الإلكتروني الدولي بالتعاون مع مكتب الاتحاد الدولي للاتصالات في قطر سنة ٢٠٠٨[٣]، أما منظمة التعاون الاقتصادي والتنمية ففي سنة (١٩٨٣)، بادرت هذه المنظمة إلى عقد اجتماع في باريس كرس لبحث جرائم الإرهاب الإلكتروني الدولي[٤]، وأصدرت قرارها المتعلق بالجرائم المتعلقة بالحاسوب وتحليل السياسات الجنائية، والذي تضمن القوانين الجنائية النافذة، والتوصيات الخاصة التي نادت بها الدول الأعضاء، باستعراض الحدود الأدنى لإساءة استعمال الحواسيب الآلية، والتي يلزم على المجتمع الدولي أن يتولى تجريمها بوضع عقوبات صارمة لها[٥]، أما فيما يتعلق بالمنظمة العالمية للملكية الفكرية فقد أبرمت في سنة (١٩٩٦)، اتفاقية مع منظمة التجارة العالمية، تتعلق بالتعاون المشترك فيما بينها في مجال الملكية الفكرية، خاصة فيما يتعلق بتطبيق نصوص التي جاءت بها اتفاقية "تريبس"[٦]، وفي مجملها تهدف هذه الاتفاقية في تعزيز الدور الذي تقوم به الدول المتقدمة، وتحقيق الإنصاف للدول النامية في موضوع الملكية الفكرية، إذ عملت لتطال عجله التقنيات الحديثة في الدول العالم الثالث لا سيما بعض الدول العربية، لتعزيز سيطرتها لمفهوم الربح على المؤلفات الفكرية والأدبية، وتجنب اعتماد مفهوم التوزيع العادل عند نشر هذه التقنيات، وإخضاعها للحصار التكنولوجي عليها، يتبين لنا من كل ذلك أن هذه المنظمات جميعا عملت من خلال المؤتمرات الدولية والتعاون الدولي الذي ينص على

---

(١) سامر عبد اللطيف، نوري رشيد الشافعي، "دور المنظمات الدولية في مكافحة الارهاب الرقمي، جامعة كربلاء، ٢٠١٦"، بحث منشور عبر الرابط الاتي: ، https://search.emarefa.net/ar/detail/BIM-938322-%D8%AF%D9%88%D8%B1-%D8%A7%D9%84%D9%85%D اخر زيارة للموقع في٩-١٩٢٠٢٣، ١٠:٥٠ am .

(٢) محمد سعادي، *أثر التكنولوجيا المستحدثة على القانون الدولي العام*، (مصر: دار الجامعة الجديد، ٢٠١٤)، ص٢٣٨.

(٣) الاعلان الختامي للمؤتمر متاح عبر شبكة الانترنيت عبر الرابط الاتي: https://www.ituarabic.org/%DB%B2%DB%B0%DB%B0%DB%B8/cllp/doha-declaration.pdf اخر موعد لزيارة الموقع ٢٠٢٣_٩_٢٣، ٢:٠٠ pm .

(٤) غازي عبد الرحمن، "الحماية القانونية من الجرائم المعلوماتية"، (اطروحة دكتورا، كلية الحقوق، الجامعة الاسلامية، لبنان، ٢٠٠٤)، ص١٨١.

(٥) يونس عرب، *جرائم الكمبيوتر والإنترنت*، (بيروت: اتحاد المصارف العربية، ٢٠٠٢)، ص٣٢٢

(٦) منظمة عالمية مقرها مدينة جنيف في سويسرا، مهمتها الأساسية ضمان انسياب التجارة بأكبر قدر من السلاسة واليسر والحرية، وهي المنظمة العالمية الوحيدة المختصة بالقوانين الدولية المعنية بالتجارة ما بين الدول، إذ تضم منظمة التجارة العالمية ١٦٤، دولةً عضواً إضافةً إلى ٢٠ دولة مراقبة.

توفير الحماية وتطوير بنية المعلومات، وتعزيز قدراتها في مجال أمن المعلومات، وكل ذلك لمكافحة الإرهاب الإلكتروني الدولي الذي يخلفه محاولات إساءة استخدام هذه التقنيات من قبل بعض الجهات الإرهابية الدولية.

أما على مستوى الاتفاقيات الدولية فقد صدرت في سنة ٢٠٠٠ الاتفاقية العالمية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (٥٥/٦٣) عن الجمعية العامة لمنظمة الأمم المتحدة، وإن سببا من عقد هذه الاتفاقية تزايد الجرائم المرتكبة عبر الإنترنت وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقدها، تؤكد هذه الاتفاقية على أهمية الجهود التي تقوم بها الهيئات المعنية، لمنع ومكافحة استخدام استعمال تكنولوجيا المعلومات بطريقة غير مشروعة، والإجراءات التي تهدف إلى الحد من هذا النوع من الانتهاكات، كما هو مبين في المادة (١) من هذه الاتفاقية[١]، كما تدعو المادة (٢) إلى أن تأخذ الهيئات المعنية بعين الاعتبار من التدابير المشار إليها في المادة (١)، في جهودها لمكافحة استخدام تكنولوجيا المعلومات بشكل إجرامي، وتقرر المادة (٣) أن تبقى مسألة إساءة استخدام تكنولوجيا المعلومات بشكل غير مشروع، على جدول أعمال دورتها السادسة والخمسين تحت البند المسمى "إيقاف الجريمة والعدل الجنائي"[٢].

وحرصا على حماية مصالح المواطنين وحقوقهم، وفي عام ٢٠٠١، تعاونت اللجنة الأوروبية ولجنة الخبراء في مجال الجرائم التقنية لإنشاء مشروع اتفاقية جرائم الكمبيوتر، خضعت الاتفاقية المقترحة للمناقشات مستفيضة وتبادل للآراء منذ المسودة الأولية وحتى النسخة النهائية، والتي تمت الموافقة عليها في نهاية المطاف في بودابست بتاريخ ٢٠٠١نوفمبر٢٣، وقد تم توزيع هذه الاتفاقية، المعروفة أيضا باسم اتفاقية الجرائم الإلكترونية، على نطاق واسع على مختلف الأطراف، وتم أتاحتها للمناقشة والتعليق على العديد من المواقع الأوروبية والأمريكية، وهي بمثابة شهادة على الجهود الجماعية التي يبذلها الاتحاد الأوربي ومجلس أوروبا، وكذلك في إطار المنظمات الحكومية ودولية ولجان الخبراء المعنية والتي تركز على التصدي لجرائم الكمبيوتر(٣)، ووقعت على هذه الاتفاقية (٢٦) دولة أوروبية، بالإضافة إلى الولايات المتحدة الأمريكية وكندا وجنوب أفريقيا واليابان، رغم كونها اتفاقية أوروبية المنشأ، إلا أنها اتفاقية ذات طابع عالمي، لكونها مفتوحة للدول الأخرى لطلب

(١) المادة (١)، في الفقرات (أ-ب-ج-د-ز-ي)، من اتفاقية مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية رقم ٢٠٠٠ ، والصادرة عن منظمة الأمم المتحدة، الجلسة العامة في ديسمبر ٢٠٠٠.

(2) Kenneth.c white, Cyber terrorism :modem mayhem,Carlisle barracks, Pennsylvania: u.s. army war college, 1998,p 15

(٣) . يونس عرب، "الاتجاهات التشريعية للجرائم الإلكترونية"، ورقة عمل مشاركة في ورشة عمل بعنوان تطور التشريعات في مجال مكافحة الجرائم الإلكترونية، سلطنة عمان، ٢٠٠٦، ص ١٥ 98,p 15

الانضمام من خارج أوروبا[١]، مما يجعلها إطارا دوليا مفيدا للعمل على مكافحة الإرهاب الإلكتروني الدولي، كما تبرز مقدمة الاتفاقية أهمية جهود الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي، والتنمية ومجموعة الدول الصناعية في مجال المعلوماتية، كما تستعرض مقدمة الاتفاقية أهدافها ومنطلقاتها ومرجعياتها السابقة وهي مبنية على جود إرشادية وتوجيهية ومقاييس إقليمية ودولية، وتفرض الاتفاقية التزامات على الدول الأوروبية أو أي دولة خارج أوروبا توقع عليها أو تنظم إليها، للإقرار العقوبات الملاءمة والتدابير الفعالة لهذه الجرائم سواء أكانت سالبة لحرية الأشخاص الطبيعية أو حرية الأشخاص المعنوية[٢]، وبالرجوع إلى لجان هذه الاتفاقية وأثناء اجتماع لجنة أو فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة المعلوماتية سنة (٢٠١٧) عرض الحاضرون تجاربهم المتعلقة بتنفيذ أنشطة المساعدة التقنية في إطار العمل العالمي لمكافحة الجريمة الإرهابية الإلكترونية، ويشير بعض الخبراء إلى الحاجة إلى إطار قانون دولي لمكافحة شبكات الدولية لجرائم لإرهاب، ويرى بعضهم أن اتفاقية بودابست قد عفا عليها الزمن[٣].

II.ب. المطلب الثاني

الجهود الاقليمية والعربية لمكافحة جرائم الارهاب الالكتروني

بعد التطور الكبير الذي شهده القانون الدولي العام من إنشاء المنظمات الدولية العالمية منها والإقليمية وما لحق المسؤولية الدولية وأركانها من تقدم وتميز على غيرها من المسؤوليات القانونية الأخرى، فقد وجب على الدول ان تنظم إلى المنظمات الدولية بموجب المواثيق الدولية لتلك المنظمات والتعاون فيما بينها من اجل مواجهة مخاطر الارهاب على اختلاف انواعه، فالأمن الالكتروني هو الأكثر وضوحاً لتصدي للإرهاب الالكتروني وما يتركه من تهديد خطير على جميع انحاء العالم، شجع الدول على زيادة بل مضاعفة جهودها في مجال محاربة الارهاب باستخدام التقنيات الحديثة وهذه الاخيرة تمتاز بارتفاع اسعارها وتطلبها اموالاً طائلة قد لا تتوافر لدى باقي اشخاص القانونين العام والخاص سوى الدولة.

نجد ان المنظمات الاقليمية لعبت دورا مهما في محاولة الحد من الجرائم الالكترونية والإرهاب الإلكتروني، نظرا لما نشهده اليوم في ظل ظاهرة العولمة من تغيرات علي الأصعدة كافة، وتعدد المجالات في الجانب الجنائي خاصة، وما افرزه ذلك من سلوكيات

(١) درّار نسيمة، "الأمن المعلوماتي وسبل مواجهة مخاطرة في التعامل الإلكتروني، دراسة مقارنة"، (إطروحة دكتوراه كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد - تلمسان، الجزائر ، ٢٠١٧)، ص ٢٧٣.

(٢) لينا محمد متعب الأسدي، "مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية"، (رسالة ماجستير، كلية الحقوق جامعة النهرين العراق ٢٠١٢)، ص ٦.

(٣) تقرير عن اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فينا في الفترة ١٠ الى ١٣ نيسان ٢٠١٧، ص ٤ ، منشور على شبكة الإنترنت عبر الرابط الاتي: - www.unodc.org/documents/organized-crime/cybercrime/-April ، (آخر زيارة من للموقع في ٢٠/٩/٢٠٢٣.

خطرة تهدد أمن المجتمع الدولي والإقليمي واستقرارها وتنذر بأقدح الأضرار والأخطار، فقد دعت الحاجة إلى اقتراح الخطط والاستراتيجيات الإقليمية، للوقاية ومكافحة الجرائم المستحدثة على الساحة الإقليمية.

في سنة (١٩٨١)، بدأ التقدم بطيئا ولكنه أخذ بالتسارع بعد انتهاء الحرب الباردة، اذ بادر مجلس الاتحاد الأوروبي التصدي للاستخدام غير المشروع لشبكات المعلومات بإصدار العديد من التوجيهات والتوصيات الملزمة في مجال مكافحة الجرائم الالكترونية، والتي تمثل الحد الأدنى الذي يتعين على دول الاتحاد الالتزام به عند إعداد تشريعاتها المتعلقة بها [(١)]، وتضمنت هذه القواعد عددا من الاجراءات الفنية التي يتوجب اتخاذها لحماية نظم المعلومات من كل اشكال الانتهاك، ففي عام ١٩٨٠ وقع مجلس أوربا معاهدة خاصة بحماية الاشخاص من مخاطر المعالجة الآلية للبيانات ذات الطابع الشخصي، والتي دخلت حيز النفاذ في اكتوبر عام ١٩٨٥، وتضمنت عدد من التوصيات تعلقت بوجوب توفير قواعد تكفل حماية البيانات الشخصية من مخاطر المعالجة الآلية، فضلا عن ذلك فقد اصدر مجلس أوربا العديد من التوصيات لحماية ب ولاسيما بيانات الحاسوب.

فضلا عن الجهود التي بذلتها "السوق الأوربية المشتركة" في مجال اصدار القرارات المعنية بحماية الفرد في مواجهة التطور التقني، إذا كانت الحماية الأوربية للبيانات الشخصية لم تصدر حتى عام ١٩٨٢، الا انه في عام ١٩٩٦صدر ارشاد أوربي، يتعلق بالحماية القانونية لقواعد البيانات واعتبار برامج الكومبيوتر ضمن مجال المؤلفات الفكرية الواجب حمايتها[(٢)]، بالإضافة الى ذلك جهود منظمة التعاون الاقتصادي والتنمية، في مجال ارسائها لمبادئ حماية الخصوصية بشأن البيانات الشخصية والتي اهتمت بشكل عملي بحماية الخصوصية عبر الحدود، والتي تبلورت على شكل قواعد ارشادية تم تبنيها رسميا من قبل مجلس المنظمة، غير أن الحدث الرئيس الذي توج جهود الاتحاد الأوربي في هذا المضمار تمثل بإصدار اتفاقية شاملة تتعلق بجرائم الحاسب في اجتماع المجلس بستراسبورغ في عام ٢٠٠٠ تضمن الدعوة الى حماية مجتمعاتها من الجرائم الرقمية ووضع التشريعات الملائمة لمكافحتها، عن الطريق النص على تجريم الافعال التي تشمل اتلاف قواعد البيانات وعمل الحواسيب الآلية وانظمتها، وعقوبة المتسبب بذلك في مثل هذه الجرائم، وضمان التعاون الدولي في مجال التحقيق وتبادل المعلومات لتحقيق الأمن المعلوماتي[٣].

ويعتزم الاتحاد الأوربي في وضع خطة جديدة، يقوم بموجبها بتفتيش اجهزة الكومبيوتر عن بعد لمكافحة الجريمة الرقمية، وهذا من شانه ان يشجع على تبادل المعلومات بين قوات الشرطة الالكترونية لتسهل عليهم ملاحقة ومقاضاة المجرمين بعد ان توجه

(١) أسامة عبد الله قايد، *الحماية الجنائية الخاصة وبنوك المعلومات*، ط ١ ، (القاهرة: دار النهضة العربية، ١٩٩١)، ص ٨٣

(٢) رشيد صبحي جاسم محمد، "الارهاب والقانون الدولي"، (اطروحة دكتورا، جامعة بغداد، كلية القانون، العراق،٢٠٠٣)، ص٢٠٨.

٣ محمد امين، *جرائم الحاسوب والانترنيت،(الجريمة المعلوماتية)*، (عمان: دار الثقافة للنشر والتوزيع، ٢٠٠٩)، ص٧٣

تحذيرات حول الاخطار المحدقة، يلحقها كذلك انشاء فرق تحقيق تعمل عبر الحدود وترخص استخدام دوريات افتراضية لملاحقتهم.

اما على صعيد الاتفاقيات الإقليمية الاجنبية نذكر " الاتفاقية الأمريكية المتعلقة بجرائم الحاسوب الآلي والإنترنت والتي عقدت في (٦-٧) كانون الأول سنة ١٩٩٩ في ولاية كاليفورنيا بالولايات المتحدة الأمريكية، وبمشاركة العديد من المنظمات والهيئات الدولية والممثلين القانونيين، وتم اقترح هذه الاتفاقية لتعزيز الحماية أمن الحاسوب الآلي من الإرهاب الإلكتروني، إذ تضمنت هذه الاتفاقية عدة مواد جاءت لتعزيز مكافحة الإرهاب الإلكتروني وصيانة الحقوق والحريات الشخصية، والحماية لأمن الدولة ومؤسساتها من الأضرار التي تخلفها هذه الجرائم، أما اتفاقية الاتحاد الأفريقي فيما يتعلق بالأمن السيبراني وحماية البيانات الشخصية لسنة ٢٠١٤، فقد جاءت لتغطي نطاقا واسعا من الأنشطة الإلكترونية، والتجارة الإلكترونية، وحماية البيانات والجرائم الإرهابية الإلكترونية، والأمن السيبراني[١].

اما جامعة الدول العربية بدأت جهودها في مكافحة الارهاب الالكتروني بوقت متأخر، حتى عام (١٩٨٣)، والتي توصلت فيه الى الاستراتيجية الأمنية العربية، التي أقرها مجلس وزراء الداخلية العرب، والتي تتضمن ضرورة حماية أمن المواطنين العرب من المحاولات الارهابية في اجتماعها الأول، وبعد عدة محاولات من الجامعة العربية للتصدي للأنشطة الارهابية، وفي اطار الخطة الأمنية العربية تشكلت لجنة الجرائم المنظمة التي تناولت في اجتماعها الأول موضوع جرائم الإرهاب، وبناء على توصيات اللجنة التي عرضت على مجلس وزراء الداخلية العرب في دورته السادسة في عام ١٩٨٧ ،اصدر قرارا يقضي بتكليف الأمانة العامة للمجلس بإعداد مشروع استراتيجية عربية لمكافحة الإرهاب، بالتنسيق مع الأمانة العامة لجامعة الدول العربية، وفي عام ١٩٨٨ اصدر مجلس وزراء الداخلية العرب، قرارا نص فيه على تشكيل لجنة من ممثلي الدول العربية، تكللت هذه الجهود بالقرار الصادر عن مجلس وزراء العرب رقم (٢٢٩) لسنة ١٩٩٦ والمتعلق بإصدار القانون العقوبات العربي الموحد نموذج لقانون العربي، في مجال مكافحة الارهاب الالكتروني والجرائم الحاسوبية [٢].

الا أن إقرار الاتفاقية العربية لمكافحة الإرهاب لم يتم الا في الدورة الـ ١٥ للمؤتمر وزراء الداخلية العرب في ١٩٩٨ ، اذ تم وضع عدد من الآليات لتنفيذ هذه الاستراتيجية لمواجهة الإرهاب ، وقد تضمن مشروع الاستراتيجية العربية لمكافحة الإرهاب عدداً من الاهداف والمقومات والآليات التي تحدد الاسس التي تقوم عليها سياسة مكافحة الإرهاب، والسبل الكفيلة بتحقيق أقصى قدر من التعاون على الصعيد العربي والدولي لتطويق هذه الظاهرة والحد من الاخطار التي تشكلها على الدول المختلفة، فاعتبرت ان الاعمال الإرهابية

(١) درّار نسيمة مصدر سابق ص٢٨٥.
(٢) حنان ريحان مبارك المضحكي، *الجرائم المعلوماتية، دراسة مقارنة*، ط١، (بيروت: منشورات الحلبي الحقوقية، ٢٠١٤)، ص٣٨٣.

هي أعمال عنف منظم يسبب رعباً وفزعاً، كما حددت هذه الاستراتيجية لكل دولة عدة إجراءات، وتدابير للوقاية من الإرهاب يبرز في مقدمتها زيادة دعم الدولة للأسرة بما يكفل التربية السليمة، وتكثيف استخدام وسائل الاعلام المختلفة لتنمية الوعي الوطني والقومي.

حث الدول على اتخاذ تدابير فعالة وحازمة لمكافحة الإرهاب بمختلف صوره واشكاله ، بعد تحديث قوانينها وتشريعاتها الجنائية لتشديد العقوبات على مرتكبي الاعمال الإرهابية ، وتجميد ومصادرة كافة الاموال الموجهة الى هذه الاعمال وتشديد اجراءات المراقبة لمنع تسلل عناصر الإرهاب والتخريب، أو تهريب الذخيرة والمتفجرات، وسعيها الحثيث للحيلولة دون اتخاذ اراضي الدول العربية مسرحا لتخطيط وتنظيم أو تنفيذ اعمال ارهابية . كما تطرقت الاستراتيجية الى موضوع تحديث وتطوير اجهزة الأمن من خلال دعمها بالمؤهلين وتوفير ما تحتاجه من معدات وتقنيات حديثة ، وكذلك وضع خطط وقائية لمنع أي اعمال ارهابية.

و أسفرت الجهود العربية عن ميلاد اتفاقية عربية "لمكافحة جرائم تقنية المعلومات"، ووقعتها الأمانة العامة لجامعة الدول العربية في القاهرة في ديسمبر ٢٠١٠، بهدف تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم الإرهاب الالكتروني، وتتكون الاتفاقية من (٤٣) مادة، منها (٢١) تتعلق بالتجريم، بالإضافة إلى ثماني مواد إجرائية تتعلق بحقوق السلطات المعلومات وتتبع المستخدمين، ومراقبة المواد المخزنة على أجهزة الكمبيوتر الشخصية والأجهزة التقنية، أما الباب الرابع ففي المادة (١٤) نظمت التعاون بتبادل معلومات المستخدمين بين الدول الأعضاء[١]، وكان مجلس الجامعة العربية موفقا بإيراد هكذا نصوص تكافح الجرائم الواقعة عبر الوسائل الإلكترونية، وكذلك تجريم التعدي على حقوق الملكية الفكرية من خلال استخدام تكنولوجيا المعلومات، بالإضافة إلى تجريم وتزيف وتصنيع أو وضع أي معدات أو واد تسهل تزيف، أو تقليد أي صكك اعتماد[٢]، كذلك الحال بالنسبة للاتحاد الأفريقي والامريكي سعوا جاهدين لإقرار اتفاقيات خاصة لمواجهة الإرهاب الالكتروني، فضلا عن دور المؤتمرات والندوات الإقليمية لتصدي للإرهاب الالكتروني.

لابد من الاشارة هنا الى ان دعم الدول للجهود الدولية يلعب دوراً بارزاً في مواجهة هذه الآفة، ففي كل يوم نسمع بانضمام دولة جدية الى التحالفات الدولية لمواجهة الارهاب، مما يزيد من فرص نجاح هذا التحالفات ويسهم في التقليل من عمر الجماعات الارهابية، ويقوض مخططاتها في العبث بالأمن الانساني والأمن التقني، مما يبث الاستقرار في مجالات التعامل ،

(١) صفاء كاظم غازي الجياشي، "جريمة قرصنة البريد دراسة مقارنة"، (رسالة ماجستير ، كلية القانون، جامعة بابل، العراق، ٢٠١٦)، ص ٤٢ .

(٢) رامي متولي القاضي، *مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية*، ط١، (القاهرة: دار النهضة العربية، ٢٠١١)، ص ٧٥.

وتحويل العالم الى عالم خالي من الجرائم الارهابية المحلية منها والعالمية، اذ يثبت الاستقرار في مجالات التعامل التقني والتحول في العالم باسره الى عالم افتراضي خالي من الجرائم الارهابية المحلية منها والعالمية.

الخاتمة

اتخذ الإرهاب الحالي بعدا جديدا ومثيرا للقلق، خاصة في اعقاب الانتشار المقلق للتكنولوجيا الحديثة، حيث إنها تمكن الإرهابيين من تنفيذ عمليات مدمرة ودموية بأقل جهد، اذ يسلطون الضوء على قوة الجماعات الإرهابية، ويقومون بالتعبئة الفكرية وتجنيد إرهابيين جدد، والتعليم والتلقين الالكتروني، والتدريب الالكتروني عن طريق نقل الاساليب والوسائل التي تساعد على تنفيذ الهجمات الإرهابية، فتم أنشاء مواقع الكترونية إرهابية لتوضيح كيفية صنع القنابل والمتفجرات، الأسلحة الكيميائية، ويشرح كيفية اختراق رسائل البريد الالكتروني، وكيفية اختراق مواقع الويب وتشويهها، وكيفية الوصول الى لمواقع المحجوبة، وبعلم طرق نشر الفيروسات، فالإرهاب الالكتروني وينتشر بالخفاء، ويظهر مدى خطورته في الاعتداء على حياة الافراد وتهديد السلم والامن للموطنين ويهدد ابداعات العقل البشري.

الاستنتاجات:

١- أصبح من الواضح أن الارهاب الالكتروني لا يتطلب العنف والقوة عند التنفيذ، بل فقط استخدام أجهزة الكمبيوتر المتصلة بشبكات المعلومات والمزودة ببعض البرامج الضرورية، لأن الإرهاب يشكل تحد متزايد للأمن السيبراني، وتصاعد التهديدات الإرهابية يتطلب ضرورة تعزيز الحماية الرقمية، وتحسين التعاون الدولي.

٢- تستغل الجرائم الارهابية اليوم شبكات الانترنيت لتسبب في احداث خسائر للدول والمنظمات الدولية، مما يتطلب من المنظمات والمجتمع الدولي الحصول على اجهزة متطورة لمواجهه خطر هذه الجرائم وحماية معلوماتها وامن افرادها.

٣- يتميز الارهاب الالكتروني بالجرائم الإرهابية العابرة لحدود الوطنية، وتعبر الدول والقارات، ولا تقتصر على نطاق إقليمي محدد، كما يتميز الإرهاب بتعاون عدة أشخاص للارتكابه، وان مرتكبو الهجمات الإرهابية قد يكونون فرادى أو جماعات، وفي بعض الأحيان يكونون دولا تستخدم الإنترنيت والتكنولوجيا لتحقيق أهدافها والترويج للأفكار الإرهابية.

٤- يمثل الإرهاب الإلكتروني سرقة للمعلومات الحساسة والمهمة لدول وتسريبها مما يؤدي إلى خسائر فادحة تلحق الدولة والمؤسسات التابعة لها والأفراد، إذ يسفر عن ذلك تهديد للأمن الوطني، كما تستخدم سرقة هذه المعلومات كوسيلة للتجسس أو التنافس الاقتصادي والعسكري.

٥- من الصعوبة الكشف أحيانا عن جرائم الإرهاب الإلكتروني، كما أنه من الصعب تقديم أدلة مثل هذه الجرائم بسبب قلة خبرة بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذه الجرائم.، وبسبب النقص السريع في الأدلة الرقمية وسهولة تدميرها، وصعوبة تتبع الهوية الرقمية، كما أن تطور التكنولوجيا المستمر يوفر وسائل حديثة للهجمات الإرهابية يصعب التعرف عليها.

التوصيات :

١- تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع الهجمات الإلكترونية التي تقوم بها الجهات الفاعلة بشكل يمنع الإرهابيين والمتطرفين من إساءة استخدام التطورات والتقنيات التكنولوجية، ويتضمن ذلك التخفيف من تأثير هذا الانتهاك، ومعالجة خطر الهجمات السيبرانية التي يشنها الإرهابيون، وخاصة ضد البنية التحتية الحيوية للدول.

٢-تشجيع التعاون مع القطاعات الخاصة في تقديم التقنيات وتبادل المعلومات والخبرات لحماية ومنع الهجمات الإرهابية على البنى التحتية الحيوية، والعمل على تخفيف من تأثير هذه الهجمات، وإصلاح الأنظمة المستهدفة في حالة وقوع مثل هذه الهجمات، وإنشاء الاتصالات المناسبة والتدخل السريع في حالة الطوارئ.

٣- دعم الابتكار والتشجيع عليه في مجال الأمن السيبراني، وبناء الخبرات في مجالات تكنولوجيا المعلومات والاتصالات وعلوم الطب الشرعي، وتعزيز قدرة وكالات إنفاذ القانون على مراقبة محتوى وسائل التواصل الاجتماعي المتعلقة بالإرهاب، لمنع حركة المقاتلين الإرهابيين امتثالا للالتزامات الدولية التي تعهدت بها الدول في مجال حقوق الإنسان، من خلال وضع الحلول الفعالة لمكافحة الإرهاب، حتى تستطيع ان تقف بوجهة تحديات عصر العولمة.

٤- تشجيع الدول في الإسراع بالانضمام للاتفاقيات الدولية الخاصة لمواجهة جرائم الإرهاب الإلكتروني لا سيما اتفاقية مكافحة الجرائم المعلوماتية، وبروتوكول الأمم المتحدة لمنع ومكافحة الإرهاب، وحث الدول العربية لقيام اتحادات تسعى لمواجهة هكذا نوع الجرائم من خلال تفعيل دور المنظمات وحكومات الدول.

٥- تفعيل دور القواعد القانونية بشكل عام وقواعد الإرهاب بشكل خاص على جميع المواطنين ولا حصانه لأي مواطن سواء أكان أجنبيا أو أحد مواطني الدولة من الإجراءات القضائية في حال كانت هناك أدلة تفيد ارتكابه أو مساهمته في الجرائم الإرهابية، وتطوير الجانب القانوني الدولي عند تعامله مع هكذا قضايا بشكل فعال بوضع عقوبات مناسبة للمتورطين.

٦- العمل على توسيع الدراسات المتعلقة بفكر التنظيمات الإرهابية التي تبث عبر الشبكات الإنترنيت والتي تشجع بدورها على تدريب الآخرين وتوعيتهم ليتسنى لحكومة والجهات المؤسسية المعنية بنشر الفكر الصحيح لمواجه هكذا نوع من الجرائم، وإعداد دورات

تأهيلية للقائمين على إنفاذ القانون لا سيما جهاز الأمن القومي لتطوير من معلوماتهم في مجال تكنولوجيا المعلومات وتدريبهم بشكل يمكنهم من تعاملهم مع هكذا نوع من القضايا، وإنشاء مراكز للتحقيق السيبراني في مختلف الدول لتسهيل التحقيق مع المتورطين وتقديم الدعم الفني.

المصادر

المصادر باللغة العربية:

اولا": الكتب

١- أسامة عبد الله قايد، *الحماية الجنائية الخاصة وبنوك المعلومات*، ط ١ ، القاهرة: دار النهضة العربية، ١٩٩١.

٢- حنان ريحان مبارك، *الجرائم المعلوماتية*، بيروت: منشورات الحلبي الحقوقية، ٢٠١٤.

٣- حنان ريحان مبارك، *الجرائم المعلوماتية، دراسة مقارنة*، ط١، بيروت: منشورات الحلبي الحقوقية، ٢٠١٤.

٤- رامي متولي القاضي، *مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية*، ط١، القاهرة: دار النهضة العربية.

٥- زين العابدين عواد كاظم الكردي، *جرائم الإرهاب المعلوماتي، دراسة مقارنة* ، ط ١ ، بيروت: منشورات الحلبي الحقوقية، ٢٠١٨.

٦- عادل عبد الصادق، *الارهاب الالكتروني نمط جديد وتحديات مختلفة*، مصر: مركز العربي ابحاث الفضاء الالكتروني، ٢٠١٣.

٧- عبد الكريم الردايدة، *الجرائم المستحدثة واستراتيجية مواجهتها*، ط١، الأردن: دار الحامد، ٢٠١٣.

٨- علي جبار الحسيناوي، جرائم الحاسوب والانترنيت، الأردن: دار اليازوري العلمية للنشر والتوزيع، ٢٠٠٩.

٩- علي يوسف الشكري، *المنظمات الدولية*، عمان: دار الصفاء للنشر والتوزيع، ٢٠١٢.

١٠- محمد سعادي، *أثر التكنولوجيا المستحدثة على القانون الدولي العام*، مصر: دار الجامعة الجديد، ٢٠١٤.

١١- محمود احمد القرعان، *الجرائم الالكترونية*، الأردن: دار وائل للنشر والتوزيع، ٢٠١٧

١٢- محمود رجب فتح الله، *الوسيط في الجرائم المعلوماتية*، الإسكندرية: دار الجامعة الجديدة، ٢٠١٩.

١٣- مصطفى يوسف كافي، وآخرون، *الإعلام والإرهاب الإلكتروني*، ط ١ ، الأردن: دار الإعصار العلمي للنشر والتوزيع، ٢٠١٥.

١٤- يونس عرب، *جرائم الكمبيوتر والإنترنت*، بيروت: اتحاد المصارف العربية، ٢٠٠٢.

ثانياً: الرسائل والاطاريح

١-اسراء طارق جواد كاظم، "جريمة الإرهاب الالكتروني دراسة مقارنة"، رسالة ماجستير تقدمت بها الى كلية الحقوق جامعة النهرين،٢٠١٢.
٢- درّار نسيمة، "الأمن المعلوماتي وسبل مواجهة مخاطرة في التعامل الإلكتروني، دراسة مقارنة"، إطروحة دكتوراه كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد - تلمسان، الجزائر ، ٢٠١٧.
٣-رشيد صبحي جاسم، "الارهاب والقانون الدولي"، رسالة ماجستير، كلية القانون جامعة بغداد، العراق، ٢٠٠٣.
٤-صفاء كاظم غازي الجياشي، "جريمة قرصنة البريد دراسة مقارنة"، رسالة ماجستير ، كلية القانون، جامعة بابل، العراق،٢٠١٦.
٥-غازي عبد الرحمن، "الحماية القانونية من الجرائم المعلوماتية"، اطروحة دكتورا، كلية الحقوق، الجامعة الاسلامية، لبنان، ٢٠٠٤.
٦-لينا محمد متعب الأسدي، "مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية"، رسالة ماجستير، كلية الحقوق جامعة النهرين العراق ٢٠١٢.

ثالثاً: البحوث والمقالات

١-حسن طوالبة ، "الارهاب الدولي"، *بحث منشور في مجلة الحكمة ، بغداد* ، العدد ٢١ ، السنة الرابعة ، (٢٠٠١).
٢-حمدان رمضان محمد، "الارهاب الدولي وتداعياته على الامن والسلم العالمي دراسة تحليلية من منظور اجتماعي"، *بحث منشور في مجلة ابحاث التربية الاساسية جامعة الموصل*، (٢٠١١).
٣-خليل يوسف جندي، "المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني(دراسة مقارنة)"، *بحث منشور في مجلة القانون للعلوم السياسية، جامعة كركوك*، (٢٠١٨).
٤-سامر مؤيد عبد اللطيف، "الإرهاب الإلكتروني وسبل مواجهته"، *بحث منشور في مجلة كربلاء العلمية، العراق*، ع١٤، (٢٠١٦).
٥-صباح كزيرة، امال كزير، "الارهاب الالكتروني وانعكاساته على الامن الاجتماعي، دراسة تحليله"، *مجلة التراث*، (٢٠١٨).
٦-عبد الله بن عبد العزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات"، *بحث مقدم الى المؤتمر الدولي الأول حول حماية أمن المعلومات وخصوصيته في قانون الإنترنت، المنعقد بالقاهرة*، في المدة من ٢-٤ يونيو، (٢٠٠٨).

٧-مجمع البحوث والدراسات الاكاديمية السلطان قابوس لعلوم الشرطة، "الجريمة الالكترونية"، *عمان*، (٢٠١٦).

رابعا: القوانين والمواثيق الدولية

١- اتفاقية مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم ٢٠٠٠.
٢- الاتفاقية الدولية لمكافحة الاجرام المعلوماتي ٢٠٠١.
٣- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.
٤- اتفاقية الاتحاد الأفريقي فيما يتعلق بالأمن السيبراني وحماية البيانات الشخصية لسنة ٢٠١٤.

خامساً: المصادر الانكليزية:

1- Kenneth.c white, Cyber terrorism :modem mayhem,Carlisle barracks, Pennsylvania: u.s. army war college, 1998

سادساً: المواقع الالكترونية :

١-حوراء رشيد مهدي الياسري: "الإرهاب الإلكتروني وطرق مواجهته ٢٠١٧ "، مقالة منشورة على شبكة الانترنيت.

https://m.annabaa.org/arabic/informatics/11123

٢-ريهام عبد الرحمن، "اثر الارهاب الالكتروني على تغير مفهوم القوة في العلاقات الدولية، دراسة حالة تنظيم داعش"، بحث منشور على شبكة الانترنيت، ٢٠١٦.

https://democraticac.de/?p=34528

٣-علي مطر، "الارهاب الالكتروني في القانون الدولي: نوع جديد لم يتم التعامل معه بعد"، مقال صحفي2013.

https://www.inbaa.com/%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8

٤-سامر عبد اللطيف، نوري رشيد الشافعي، "دور المنظمات الدولية في مكافحة الارهاب الرقمي، جامعة كربلاء، ٢٠١٦"، بحث منشور على الانترنيت

https://search.emarefa.net/ar/detail/BIM-938322-%D8%AF%D9%88%D8%B1-%D8%A7%D9%84%D9%85%D

٥-يونس عرب، "الاتجاهات التشريعية للجرائم الإلكترونية"، ورقة عمل مشاركة في ورشة عمل بعنوان تطور التشريعات في مجال مكافحة الجرائم الإلكترونية، سلطنة عمان، ٢٠٠٦.

https://www.mohamah.net/law/%D8%A8%D8%AD%D8%AB-%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A-%D9%87%D8%A7%D9%85-%D8%AD%D9%88%D9%84-%D8%AA%D8%B7%D9%88%D9%8A%D8%B1-%D8%A7%D9%84%D8%AA%D8%B4%D8%B1%D9%8A%D8%B9%D8%A7%D8%AA-%D9%81%D9%8A-%D9%85/.

٦- تقرير عن إجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فينا في الفترة ١٠ الى ١٣ نيسان ٢٠١٧، ص ٤ ، منشور على شبكة الإنترنت عبر الرابط الاتي:

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/V1701247_A.pdf .

Sources

Sources in Arabic:

-First: Books

1- Osama Abdullah, Commander of Special Criminal Protection and Information Banks, ed., Dar Al Nahda Al Arabiya, Cairo, Cairo 1991.
2- Hanan Rayhan Mubarak, Information Crimes, Al-Halabi Human Rights Publications, Beirut, 2014
3- Hanan Rayhan Mubarak, Information Crimes, A Comparative Study, 1st edition, Al-Halabi Legal Publications, Beirut, 2014.
4- Rami Metwally Al-Qadi: Combating cybercrimes in comparative legislation and in light of international agreements and conventions, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo.
5- Zain Al-Abidin Awad Kazem Al-Kurdi: Information terrorism crimes, a comparative study, 1st edition, Al-Halabi Legal Publications, Beirut, 2018.
6- Adel Abdel Sadiq, Cyber terrorism: a new pattern and different challenges, Al-Arabi Center for Cyberspace Research, Egypt, 2013.
7- Abdul Karim Al-Radaida, New Crimes and the Strategy to Confront Them, 1st edition, Dar Al-Hamid, Jordan, 2013.
8- Ali Jabbar Al-Husseinawy, Computer and Internet Crimes, Al-Yazouri Scientific Publishing and Distribution House, Jordan, 2009.

9- Ali Youssef Al-Shukri, International Organizations, Dar Al-Safaa for Publishing and Distribution, Amman, 2012
10- Muhammad Saadi, The Impact of New Technology on Public International Law, New University House, Egypt, 2014.
11- Mahmoud Ahmed Al-Qur'an, Electronic Crimes, Dar Wael for Publishing and Distribution, Jordan, 2017
12- Mahmoud Ragab Fathallah, Mediator in Information Crimes, New University House, Alexandria, 2019
13- Mustafa Youssef Kafi, and others: Media and Electronic Terrorism, 1st edition, Dar Al-Assar Al-Alami for Publishing and Distribution, Jordan, 2015.
14- Younis Arab, Computer and Internet Crimes, Union of Arab Banks, Beirut, 2002.

Second: Theses and dissertations

1- Israa Tariq Jawad Kazem, the crime of electronic terrorism, a comparative study, a master's thesis submitted to the Faculty of Law, Al-Nahrain University, 2012.
2- Darrar Nasima: Information security and ways to confront risks in electronic dealings, a comparative study, doctoral dissertation, Faculty of Law, Department of Law, Abu Bakr Belkaid University - Tlemcen, Algeria, 2017.
3- Rashid Subhi Jassim, Terrorism and International Law, Master's Thesis, College of Law, University of Baghdad, Iraq, 2003.
4- Safaa Kazem Ghazi Al-Jayashi: The crime of mail piracy, a comparative study, Master's thesis, College of Law, University of Babylon, Iraq, 2016
5- Ghazi Abdel Rahman, Legal Protection from Information Crimes, doctoral thesis, Faculty of Law, Islamic University, Lebanon, 2004
6- Lina Muhammad Mutaib Al-Asadi, The effectiveness of the provisions of the criminal law in combating information crime, Master's thesis, Faculty of Law, Al-Nahrain University, Iraq, 2012

Third: Research and articles

1- Hassan Tawalba, International Terrorism, research published in Al-Hikma Magazine, Baghdad, Issue 21, Fourth Year, 2001.
2- Hamdan Ramadan Muhammad, international terrorism and its repercussions on global peace and security, an analytical study from

a social perspective, research published in the Journal of Basic Education Research, University of Mosul, 2011.
3- Khalil Youssef Jundi, Legislative confrontation of information crime at the international and national levels (comparative study), research published in the Journal of Law for Political Science, Kirkuk University, 2018
4- Samer Moayed Abdel Latif: Cyber terrorism and ways to confront it, research published in Karbala Scientific Journal, No. 14, Iraq, 2016
5- Sabah Kazira, Amal Kazira, cyber terrorism and its repercussions on social security, its analysis study, Al-Turath Magazine, 2018
6- Abdullah bin Abdulaziz bin Fahd Al-Ajlan: Electronic terrorism in the information age, research presented to the first international conference on protecting information security and privacy in Internet law, held in Cairo, from June 2-4, 2008.
7- Sultan Qaboos Academy of Research and Studies for Police Sciences, Electronic Crime, Oman, 2016

Fourth: International laws and conventions

1- Convention against the Misuse of Information Technology for Criminal Purposes No. 2000
2- The International Convention against Cybercrime 2001
3- The Arab Convention on Combating Information Technology Crimes of 2010
4- The African Union Convention on Cybersecurity and Personal Data Protection of 2014

English sources:

1- Kenneth.c white, Cyber terrorism :modem mayhem,Carlisle barracks, Pennsylvania: u.s. army war college, 1998

websites:

1- Hawra Rashid Mahdi Al-Yasiri: Cyber terrorism and ways to confront it, 2017, an article published on the Internet.
https://m.annabaa.org/arabic/informatics/11123
2- Reham Abdel Rahman, The impact of cyber terrorism on changing the concept of power in international relations, a case study of ISIS, research published on the Internet, 2016.
https://democraticac.de/?p=34528
3- Ali Matar, Cyber terrorism in international law: a new type that has not yet been dealt with, newspaper article 2013.

https://www.inbaa.com/%D8%A7%D9%84%D8%A7%D8%B1%D9%87%D8%A7%D8%A8

4- Samer Abdel Latif, Nouri Rashid Al-Shafi'i, the role of international organizations in combating digital terrorism, University of Karbala, 2016, research published on the Internet. https://search.emarefa.net

5- Younis Arab, Legislative trends in cybercrime, working paper participating in a workshop entitled The development of legislation in the field of combating cybercrime, Sultanate of Oman, 2006. https://www.mohamah.net

6- Report on the meeting of the expert group on conducting a comprehensive study on cybercrime, which was held in Vienna from 10 to 13 April 2017, p. 4, published on the Internet via the following link: https://www.unodc.org/crime/cybercrime/Cybercrime-