مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015

المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

البعد الدولي لمكافحة جريمة الإرهاب الالكتروني
The international dimension of fighting against the crime of cyberterrorism

سعاد بنور *
جامعة عبد الحميد بن باديس - مستغانم (الجزائر)
souad.bennour@univ-mosta.dz

تاريخ إرسال المقال: 15-07-2021 تاريخ قبول المقال: 28-08-2021 تاريخ نشر المقال:20-01-2022

الملخص :
يعد الإرهاب الالكتروني نمطا جديدا من الإرهاب يهدد البنية التحتية للمجتمعات الحديثة، وخطرا يشغل الدول التي هي عرضة لهجمات الإرهابيين والجماعات المتطرفة عبر الانترنت من خلال ممارستهم لنشاطها الإرهابي من أي مكان في العالم ضد المؤسسات الحكومية والشركات الاقتصادية، وإن غياب الحدود المكانية في الشبكة المعلوماتية بالإضافة إلى عدم وضوح الهوية الرقمية للمستخدم في بيئته الافتراضية المفتوحة يصعب من مهمة الدول في مكافحة هذا النوع من الإجرام الذي قد يتعدى حدودها الإقليمية، الأمر الذي يستدعي تدخلا وتعاونا دوليا لمكافحة جريمة الإرهاب الالكتروني.
الكلمات المفتاحية: تكنولوجيا، قرصنة الكترونية، التجسس، الإرهاب الرقمي، تسليم المجرمين، جريمة الالكترونية.

Abstract:
Cyberterrorism is a new pattern of terrorism that threatens the infrastructure of modern societies and concerns States that are vulnerable to attacks by terrorists and extremist groups via the Internet through their terrorist activity from anywhere in the world against government institutions and economic companies and the absence of physical boundaries in the information network, as well as the obscure digital identity of the user in its open virtual environment, makes it difficult for States to combat this type of crime, which may go beyond their territorial borders, and thus requires international intervention and cooperation to fight against the crime of cyberterrorism.
Key words: technology, cyberhacking , espionage, digital terrorism, extradition, cyber crime.

***المؤلف المرسل**

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

المقدمة:

أصبح الإرهاب الالكتروني خطرا يهدد الدول من خلال استخدام الانترنت ومختلف التقنيات العلمية والتكنولوجية من أجل تنفيذ أعمال إرهابية يتعذر ويصعب تنفيذها على أرض الواقع، تنفذ من قبل أشخاص تتوفر فيهم القدرة والكفاءة والخبرة في استخدام التقنية المعلوماتية، لأغراض تشمل توسيع الأنشطة الإرهابية في التجنيد والتوجيه والتمويل والتغلب على الإجراءات الأمنية والقضائية.

ويعد الإرهاب الالكتروني نمطا جديدا من الإرهاب الذي لا يعتمد على استخدام الأسلحة وإنما عبر توظيف الإرهابيين للأنظمة المعلوماتية للإعلام الآلي ضد الأنظمة المدنية والعسكرية، وهو ما يؤدي إلى تهديد الأمن الوطني والدولي على حد السواء، لهذا سعت أغلب الدول الى اعتماد مجموعة من التدابير والإجراءات لمواجهة الإرهاب الالكتروني، إلا أن هذه الجهود محدودة وتحتاج إلى تعزيز التعاون الدولي والإقليمي للتصدي لمثل هذا النوع من الإرهاب، والإشكالية المطروحة هي ما مدى فعالية التعاون الدولي في مكافحة جريمة الإرهاب الالكتروني؟ وما هي الآليات الدولية المتاحة للتصدي لها؟

إجابتنا على الإشكالية المطروحة تكون بإتباع المنهج الوصفي والاستقرائي والتحليلي لمختلف النصوص القانونية الدولية، وتحليل واستقراء الآراء الفقهية المتعلقة بمكافحة جريمة الإرهاب الالكتروني، بهدف الوصول إلى الآليات الدولية لمكافحة هذا النوع من الإجرام ومساعدة الدول على صياغة منظومة قانونية فعالة تتصدى للجريمة الإرهابية في الفضاء الالكتروني.

المحور الأول: جريمة الإرهاب الالكتروني في ضوء النصوص القانونية الدولية

ترتب على ظاهرة الجريمة الالكترونية تنامي الأعمال الإجرامية الإرهابية عبر الوسائل الالكترونية داخل حدود الدولة وخارجها، الأمر الذي أدى إلى دق ناقوس الخطر لدى المنظمات والمؤسسات الدولية للبحث عن آليات وتدابير من شأنها مكافحة هذه الجرائم، ودعوة المجتمع الدولي إلى التصدي لها.

أولا: مفهوم جريمة الإرهاب الالكتروني

أدى التطور الالكتروني وقيام الحكومات والمؤسسات الالكترونية الى تغيير أنماط الجريمة الالكترونية، فظهر الإرهاب بشكله المعاصر، والذي يعرف بالإرهاب الالكتروني أو الرقمي أو المعلوماتي، وقبل للتطرق لجريمة للإرهاب الالكتروني لابد من وضع إطار مفاهيمي لها.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

1- تعريف الإرهاب الالكتروني

لغويا وفي اللغة الفرنسية عرف قاموس لاروس الفرنسي "Larousse" الإرهاب الالكتروني "Cyberterrorisme"على أنه "مجموعة من الهجمات الخطيرة (فيروسات، قرصنة...الخ، واسعة النطاق على الحواسيب، الشبكات وأنظمة الإعلام الآلي لمؤسسة أو هيئة أو دولة، ترتكب لخلق فوضى عامة من شأنها بث الرعب"[1]، وفي اللغة الانجليزية عرف على أنه "استخدام الحواسيب والانترنت لمهاجمة أو تخويف أعداد كبيرة من الناس من أجل تحقيق أهداف سياسية أو لإجبار الحكومة على فعل شيء ما"[2].

يتكون مصطلح الإرهاب الالكتروني "CyberTerrorism" من كلمتين : "Cyber" وتعني الفضاء الالكتروني، و "Terrorism " وتعني الإرهاب، أما معاجم اللغة العربية فاكتفت بتعريف والإرهاب وقصدت به الخوف والرعب والفزع[3].

أما دوليا عرفت الأمم المتحدة الإرهاب الالكتروني بأنه "استخدام الانترنت لنشر أعمال إرهابية"، ويبدو أن هذا التعريف جد مختصر وغير دقيق مقارنة بالتعريف الوارد في تقرير اللجنة الدولية للصليب الأحمر التي عرفت الإرهاب الالكتروني على أنه "عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف إلى تحقيق أغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير أو تغيير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة من الأهداف في العلم الحقيقي كالصناعات والبنى الأساسية، ولعل من بين الأسباب التي

---

[1] Cyberterrorisme : "Ensemble des attaques graves (virus, piratage, etc.) et à grande échelle des ordinateurs, des réseaux et des systèmes informatiques d'une entreprise, d'une institution ou d'un État, commises dans le but d'entraîner une désorganisation générale susceptible de créer la panique". https://www.larousse.fr/dictionnaires/francais/cyberterrorisme/186900, consulté le 26/05/2021.

[2] Cyberterrorism is" the use of computers and the internet to attack or frighten large numbers of people, usually in order to achieve political aims or to force a government to do something". https://www.collinsdictionary.com/dictionary/english/cyberterrorism , consulté le 26/05/2021.

[3] ابن منظور أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر ودار، بيروت، 1955 ، المنجد في اللغة، دار المشرق، بيروت، ط 29، 1986م، ص 280.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

عرقلت طرق مواجهة هذه الظاهرة الإجرامية هو تأخر المجتمع الدولي في الوصول إلى تعريف محدد لمعنى الإرهاب بحد ذاته"[4].

من بين التعاريف الفقهية للإرهاب الالكتروني، أنه "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 الالكترونية".

2- خصائص جريمة الإرهاب الالكتروني

تتميز جريمة الإرهاب الالكتروني بالخصائص التالية:

– الإرهاب الالكتروني جريمة عابرة للحدود

يعتبر الإرهاب الالكتروني عابر للحدود الإقليمية متعدد الجنسيات لا تجمعه قضية وطنية أو إيديولوجية سياسية أو دينية، يهدف إلى تحقيق أكبر الخسائر المادية والبشرية في ظرف وجيز مستعملا أسلحة رقمية متطورة، حيث ساهم التحول الرقمي والتكنولوجي وعولمة الجريمة إلى الانتشار الواسع والسريع للأعمال الإجرامية الرقمية التي اجتازت الحدود الإقليمية للدول لتنفيذ الجماعات الإرهابية هجماتها في مختلف أنحاء العالم، فاعتمدت على الوسائل التكنولوجي والفضاء الرقمي في تجنيد الإرهاب وإلحاقهم بالجماعات الإرهابية مستغلة بذلك أهم شرائح المجتمع[5]، إدراكا مدى خطورة الإجرام المرتكب عبر الفضاء الالكتروني بوصفه إجراما عابرا للحدود فقد تم التوقيع على اتفاقية بودابست لمكافحة جرائم المعلوماتية والاتصالات من طرف عدة دول في العاصمة المجرية من بينها أعضاء من الاتحاد الأوروبي، كندا، أمريكا، اليابان، جنوب إفريقيا.

- المساس بالبنية التحتية للدول والمؤسسات الحكومية

انتشار التكنولوجيا وتطور وسائل الاتصال الحديثة سلاح ذو حدين، يمكن استخدامها من أجل تسهيل الاتصالات حول العالم وانتقال الثقافات وتقريب المسافات بين الدول، ولكن استخدمها غير قانوني وغير المشروع من طرف الإرهابيين من شأنه أن يؤدي إلى اختراق وتخريب النظم المعلوماتية للمؤسسات المدنية والعسكرية،

[4] تقرير اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، رقم31، لسنة 2011، ص .67

[5] ايمان بن سالم، جريمة التجنيد الالكتروني للإرهاب، وفقا لقانون العقوبات الجزائري، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018، ص 06.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

والمؤسسات الحيوية كمحطات الإمداد بالطاقة الكهربائية والماء، والمرافق النووية لإحداث خسائر بشرية ومادية، قد تفوق خسائر الحروب والكوارث الطبيعية[6].

تشير دراسات حديثة إلى تعرض البنية التحتية الالكترونية في جميع أنحاء العالم في واحدة من أكبر الهجمات الالكترونية لهجوم جانب شبكة روبوتية من الأجهزة الموصولة المقرصنة، بدأ من كاميرات مراقبة الى المسيَّرات، وأثارت مخاوف على الصعيد العلمي، وفي سنة 2017 أكد مكتب التحقيقات الفدرالي الأمريكي على الفرص المختلفة المتاحة لمرتكبي الجرائم الالكترونية للنفاذ إلى انترنت الأشياء وأجهزة أخرى الى جانب المعلومات المرفقة بهذه الشبكات[7].

-سهولة ارتكاب جرائم الإرهاب الالكتروني

أضحت الوسائل التكنولوجيا الحديثة ومختلف الوسائل الرقمية متاحة للجميع وسهلة الولوج، مما سهل الأمر على الإرهابي المعلوماتي التحكم في مختلف التقنيات وبأبسط الوسائل كالحاسوب أو هاتف محمول، وشبكة الأنترنت، من أجل تهديد استقرار الأمن الوطني والدولي، وإن السمة العالمية لشبكات المعلومات تشكل وسيلة سهلة الاستخدام وقليلة التكلفة مما يهيأ الفرصة للإرهابيين في الوصول إلى أهدافهم غير المشروعة والقيام بهجومهم الإرهابي الالكتروني[8].

- صعوبة اكتشاف وإثبات جرائم الإرهاب الالكتروني

إن الطابع الدولي لجرائم الإرهاب الالكتروني التي تتجاوز حدود الدولة ليشمل عدة دول، وكذا الخبرة والكفاءة العالية التي يتمتع بها الإرهابي المعلوماتي في مجال تقنية المعلومات تجعل من الصعب اكتشاف هوية مرتكب الجريمة وتحديد مكانه[9]، ومن الصعب إثبات مثل هذه الجرائم أمام نقص الخبرة لدى بعض الجهات الأمنية والقضائية في البحث والتحري وكشف هذه الجرائم التي يسهل على إرهابي خبير في المعلوماتية محو آثارها في الفضاء الالكتروني.

---

[6] مصطفى يوسف كامل، جرائم الفساد، غسيل الأموال، السياحة، الإرهاب الالكتروني، المعلوماتية، مكتبة المجتمع العربي للنشروالتوزيع، 2014، ص .143

[7] تقرير الاتحاد الدولي للاتصالات، بشأن المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني، الوثيقة C20/65، جنيف، 2020، ص .07

[8] حوراء رشيد مهدي الياسري، الارهاب الالكتروني وطرق مواجهته، مركز الفرات للتنمية والدراسات الاستراتيجية، متاح على الموقع الالكتروني: http://fcdrs.com/polotics/766 ،تاريخ الاطلاع 2021/05/28.

[9] أمير فرج يوسف، المرجع السابق، ص 219.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

ثانيا: الإطار القانوني الدولي لجريمة الإرهاب الالكتروني

تشكل اتفاقية بودابست لمكافحة جرائم المعلوماتية والاتصالات التي وقعت عليها 30 دولة سنة 2001 إطار قانوني مرجعي للجرائم الالكترونية بصفة عامة وجريمة الإرهاب الالكتروني بصفة خاصة سيما وأن هذه الاتفاقية جاءت عقب الهجمات الإرهابية التي تعرضت لها الولايات المتحدة الأمريكية بتاريخ 2001/09/11، الأمر الذي أثار اهتمام الدول بالتصدي لهذه الجريمة التي اتخذت صفة العالمية.

جاءت هذه لمعالجة إشكالية دولية الجرائم الالكترونية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجرائم وتعقب مرتكبيها والمساعدة على الاستدلال عليهم وضبطهم[10]، ولتحدد أفضل طرق التحقيق في جرائم الانترنت، وقد فصلت في أنواع الجرائم الالكترونية التي شملت جريمة الإرهاب الالكتروني.

ثم أشارت الأمم المتحدة في قرارها الصادر سنة 2006 تحت عنوان " إستراتيجية الأمم المتحدة لمكافحة الإرهاب" إلى مكافحة الإرهاب بجميع أشكاله ومظاهره على الانترنت، وفي 2009 اعتمدت منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات على الصعيد الدولي اتفاقية بين حكومات الدول الأعضاء التي صرحت في المادة الثانية منها أن الإرهاب المعلوماتي يشكل أحد التهديدات الرئيسية في مجال أمن المعلومات الدولي، وحددت في المادة الثالثة منها المجالات الرئيسية للتعاون والتي من بينها التصدي للتهديدات باستخدام تكنولوجيا المعلومات والاتصالات لأغراض إرهابية.

وعلى المستوى الإقليمي تناولت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[11] الصادرة في 21 ديسمبر 2010 جريمة الإرهاب الالكتروني بشيء من التفصيل، حيث حددت في مادتها 15 بعض مظاهر الجرائم الإرهابية المرتكبة بواسطة تقنية المعلومات[12].

---

[10] ليندة شرا بشة، السياسة الدولية والاقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، كلية الحقوق، جامعة الجلفة، الجزائر، المجلد رقم 01، العدد الأول، سنة 2009، ص 247.

[11] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، على الرابط التالي: http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pd

[12] المادة (15) الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:
1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

ثالثا: مظاهر جريمة الإرهاب الالكتروني في ضوء القانون الدولي

لجريمة الإرهاب الالكتروني عدة مظاهر قرتها المنظمة العربية لمكافحة جرائم تقنية المعلومات نذكر منها:

1- نشر أفكار ومبادئ إرهابية والدعوة إليها

من خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة والدعوة إلى مبادئها المنحرفة، والسيطرة على وجدان الأفراد، واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة، والتي تتعارض مع مصلحة المجتمع[13]، وهنا يبرز دور الفضاء الالكتروني وتقنيات الإعلام والاتصال في نشر مبادئ وأفكار الجماعات الإرهابية، التي تتيح للإرهابيين من جمع أتباع وأنصار عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الالكترونية[14].

2- تمويل العمليات الإرهابية

تستغل الجماعات الإرهابية المعلومات الشخصية المالية لمستخدمي الشبكة المعلوماتية، وبطاقات الائتمان، والأشخاص ذوي القلوب الرحيمة لدفع التبرعات المالية لأشخاص اعتباريين يشكلون واجهة لهؤلاء الإرهابيين باستعمال الوسائل الالكترونية والطرق الاحتيالية التي لا تدع مجال للشك بأن المتبرع يساعد التنظيمات الإرهابية.

تجمع الجماعات الإرهابية التبرعات من خلال بطاقة الائتمان عبر شبكة الانترنت، وهي وسيلة آمنة بعيدا عن التحويلات البنكية والمؤسسات المالية المراقبة، وهروبا من البيانات الشخصية، وعدم كشف الهوية، لأن من سمات الإرهابي السرية والكتمان[15]، إضافة إلى استخدام البطاقات الالكترونية المسروقة للهيمنة على حسابات بنكية قد تستخدمها هذه الشبكات في تمويل عملياتها لوجستيا من خلال الدخول إلى كلمة السر والتصرف في أموال الحسابات بحرية تامة[16].

---

[13] - محمود أحمد القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، الأردن، 2017. ص .208

[14] - محمود أحمد القرعان، نفس المرجع، ص .207

[15] هاني خميس أحمد، المرجع السابق، ص .14

[16] هايل عبد المولى طشطوش، الإرهاب المعاصر، دار البداية، الاردن، 2014، ص 211.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

3- التدريب على العمليات الإرهابية:

الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب الارهابي، كما قامت بعض الجماعات الإرهابية من بانتاج أدلة إرشادية للعمليات الارهابية تتضمن وسائل التدريب والتخطيط والتنفيذ والتخفي، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الارهابيين في مختلف أنحاء العالم.

4- تسهيل الاتصالات بين التنظيمات الإرهابية:

تعتبر التقنيات العلمية والتكنولوجية الحديثة السلاح الأشد فتكا من قبل الإرهابي المعلوماتي في تنفيذ هجماته على الأمن والسلم الدوليين، ويعد الفضاء الالكتروني مجالا خصبا لتواصل بين الإرهابيين للاستعداد لأعمالهم الإجرامية، حيث تتيح لهم التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة بعيدا عن أعين الناظرين مما يسهل على الإرهابيين ترتيب تحركاتهم.

5- نشر طرق صناعة المتفجرات المستعملة في العمليات الإرهابية

تستخدم الأنترنت في الدرجة الأولى للتنسيق وتبادل الخبرات والمهارات والأساليب الإرهابية، حيث أنشئت مواقع الكترونية لبيان كيفية صناعة القنابل والمتفجرات[17] والأسلحة الكيماوية الفتاكة، ولشرح كيفية اختراق البريد الالكتروني، وكيفية اختراق وتدمير المواقع الالكترونية، والدخول إلى المواقع المحجوبة ولتعليم طرق نشر الفيروسات.

6- نشر الإشاعات والفتن والاعتداء على الأديان والمعتقدات:

تعمل الجماعات الارهابية الى إضعاف معنويات أعدائها مثل الحكومات عن طريق إضعاف القوة الدينية وكسب التعاطف وخلق الخوف والفوضى وهي المصالح الأساسية التي تجعل الارهابيين يلجئون لاستخدام وسائل الإعلام والاتصال، والتي تتمثل في إخلال النظام العام والأمن المعلوماتي، والتأثير الالكتروني السلبي على الانسجام بين الأديان، الأعراق، الأقاليم، الجماعات والطوائف[18].

7- إنشاء مواقع إرهابية الكترونية

استغلت العديد من التنظيمات الارهابية الطبيعة الاتصالية لشبكة الانترنت من أجل بث أفكار الارهاب ولإبراز قوة التنظيم الارهابي عن طرق تصميم مواقع افتراضية تمثل

[17] هايل عبد المولى طشطوش، المرجع السابق، ص 210 .

[18] هاني خميس محمد، مفاهيم الأسس العلمية للمعرفة، الارهاب الالكتروني، المركز الدولي للدراسات المستقبلية والاستراتيجية، مصر، العدد 27، مارس 2007، ص .13

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

الجماعات الارهابية، وهي مواقع في تنامي وارتفاع[19]، حيث أحصت إحدى الدراسات الاعلامية أن المنظمات الإرهابية لجأت الى إنشاء العديد من المواقع الالكترونية المتطرفة ، قدرت ب 2000 موقع إلكتروني سنة 1997، و 4350 موقع خلال سنة 2005، و6000 موقع سنة 2008، ليتجاوز حاليا أكثر من60 ألف موقع الكتروني إرهابي[20].

8- تدمير المواقع والبيانات الالكترونية

تشن التنظيمات الارهابية هجمات الكترونية قصد تدمير المواقع والبيانات الالكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية التحتية وتدميرها، وتستهدف المؤسسات العسكرية كمراكز القيادة والتحكم العسكرية، وأيضا المؤسسات السياسية والاقتصادية، ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومؤسسات المصارف والأسواق المالية، وذلك من أجل إخضاع إرادة الشعوب والمجتمعات الدولية.

9- التهديد الالكتروني

قد يلجأ الارهابي الى أسلوب التهديد والترويع عن طريق الاتصالات والشبكات المعلوماتية بإرسال رسائل تهديد الكترونية عبر البريد الالكتروني أو عن طريق المواقع والمنتديات وغرف الحوار والدردشة الالكترونية، وقد يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، كما قد يكون التهديد بالقيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية، والتهديد بتدمير البينة التحتية المعلوماتية[21].

10-التجسس الالكتروني

تحولت وسائل التجسس من الطرق التقليدية الى الطرق الالكترونية نحو الأهداف العسكرية والسياسية والاقتصادية، خاصة مع ظهور الشبكة المعلوماتية وانتشارها عالميا ومع توسع التجارة الالكترونية التي لم تسلم من أهداف التجسس الاقتصادي ناهيك عن التجسس الذي يطال الأشخاص والدول والمنظمات والهيئات والمؤسسات الدولية والوطنية، ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الارهابية

---

[19] حكيم غريب، الجريمة الالكترونية والجهود الدولية لمكافحتها، المجلة الجزائرية للدراسات السياسية، المجلد 2، العدد الأول، 2015، ص .75

[20] بدر احمد، الإرهاب الإلكتروني أدواته وآثاره وأساليب الوقاية والعلاج، 16-1-2017، بحث منشور متاح على الموقع الإلكتروني: http://baathparty.sy/site/arabic/index.php?node=552&cat=15369

[21] احمد فتحي سرور، المواجهة القانونية للارهاب، دار النهضة العربية، القاهرة، 2008، ص 120.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

وأجهزة الاستخبارات غير القانونية من أجل الحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدولة أخرى معادية، واستغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة[22].

المحور الثاني: التعاون الدولي مكافحة جريمة الإرهاب الالكتروني

وضعت الدول استراتيجيات من أجل مكافحة كافة الجرائم التي ترتكب عبر الوسائط الالكترونية شأن جريمة الإرهاب الالكتروني إذا ارتبطت بصفة مباشرة أو غير مباشرة بمشروع فردي أو جماعي يسعى إلى خلق نوع من الاضطراب في النظام العام بواسطة التخويف أو الترهيب أو العنف[23]، ولم نعد اليوم نتحدث عن النظام العام بمفهومه الكلاسيكي، وإنما نتحدث عن النظام العام الافتراضي للدول التي تسعى جاهدة على إيجاد ترسانة قانونية متطورة وزاجرة في سياق البحث والتحري عن الدليل الرقمي[24].

أولا: الجهود الدولية والإقليمية لمكافحة جريمة الإرهاب الالكتروني

تنوعت الجهود الرامية الى مكافحة الارهاب الالكتروني بمختلف صوره، إلا أن هناك صعوبات عديدة تعترض التعاون الدولي لا سيما فيما يخص عدم وجود نموذج موحد لجرائم الارهاب الالكتروني الذي يقتضي توحيد النظم القانونية، الأمر الذي جعلنا نبحث هذه الجهود على الصعيد الدولي والأوروبي والعربي.

1- مكافحة جريمة الإرهاب الالكتروني على الصعيد العالمي

إزاء تزايد وتنامي ظاهرة الارهاب المعاصر الممارس عبر الفضاء الكتروني عملت الأمم المتحدة الى اتخاذ تدابير جماعي لدحض تهديدات السلام والأمن الدولي، حيث اعتمدت الدول الأعضاء في الأمم المتحدة بتاريخ 08 سبتمبر 2008 استراتيجية موحدة لمكافحة الارهاب بجميع أشكاله وأنواعه، تشمل تعزيز قدرة الدول على مكافحة التهديدات الإرهابية و تحسين تنسيق أنشطة الأمم المتحدة في مجال مكافحة الارهاب، وفي سبيل تنفيذ هذه الاستراتيجية أنشيء مركز الأمم المتحدة الدولي لمكافحة الارهاب سنة 2011، وقد ظهرت مبادرات جديدة لإنشاء المنتدى العالمي للانترنت لمكافحة

[22] محمد محمود القرعان، المرجع السابق، ص 220.

[23] فؤاد براي، ظاهرة الإرهاب الرقمي وموقف المشرع المغربي منه، مجلة مغرب القانون، 2018، مقال منشور على موقع: https://www.maroclaw.com/ ، تم الاطلاع عليه بتاريخ 2021/05/30، التوقيت 13:15.

[24] عبد الله بن سليمان، الإجرام المعلوماتي في التشريع المغربي، دار الأمان، الرباط، المملكة المغربية، 2017، ص 247.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

الارهاب بالشراكة بين الأمم المتحدة فيسبوك ومايكروسوفت ويوتيوب لمعالجة مثل هذه القضايا.

ويعد الاتحاد الدولي للاتصالات (ITU) هو الهيئة الوحيدة المسئولة عن مكافحة الإرهاب الإلكتروني من بين هيئات الأمم المتحدة، كما أن الأمم المتحدة كانت قد أنشأت الشبكة الدولية الإعلامية للعدالة الجنائية (UNCIDIN) وهي متخصصة في المجال الإلكتروني.

كما يهتم الإنتربول بمواجهة الجرائم الإلكترونية وعلى رأسها الإرهاب الإلكتروني، فتعمل منظمة الإنتربول على تحليل وسائل التواصل الإجتماعي للوصول إلى البيانات والأدلة التي تدين الإرهابيين وتدل على أماكن تواجدهم لتسهيل الوصول إليهم ومنع هذه العمليات الإرهابية سواء التي تتم على أرض الواقع أو تلك الإلكترونية[25].

2- مكافحة جريمة الإرهاب الالكتروني على الصعيد الاقليمي

يعتبر المجلس الأوروبي لمكافحة الإرهاب المجلس الوحيد الذي تناول بشكل متعدد الأطراف قضية الاستخدام الإرهابي للإنترنت، حيث تمت صياغة اتفاقية الجريمة السيبرانية (Convention on Cybercrime) واتفاقية منع الإرهاب لمحاربة الإرهاب الإلكتروني والاستخدام الإرهابي للتكنولوجيا والإنترنت، كما أن الاتفاقية الأوروبية لمنع الإرهاب تتميز بأنها تشمل الإرهاب الإلكتروني.

وتهتم رابطة أمم جنوب شرق آسيا (ASEAN) بالتعاون بين دول جنوب شرق آسيا في مختلف المجالات ومن بين هذه المجالات التعاون لمكافحة الإرهاب الإلكتروني، وذلك من خلال منتدى الآسيان الإقليمي (ARF) والذي يتكون من 28 دولة يعملون من خلال هذا المنتدى على تبادل المعلومات ودراسة العديد من القضايا الخاصة بالإرهاب الإلكتروني.

كما قامت منظمة التعاون الاقتصادي لمنطقة أسيا والمحيط الهادي (APEC) بعد اجتماع بانكوك 2003 للدول الأعضاء بالاتفاق على التعاون بين القطاعين العام والخاص لمواجهة الجرائم الإلكترونية وفقًا للاتفاقيات والمعاهدات الدولية وخاصة اتفاقية الجريمة الإلكترونية.

[25] استراتيجية الأمم المتحدة لمكافحة الإرهاب، مكتب مكافحة الإرهاب - فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب ،متاح على:- https://www.un.org/counterterrorism/ctitf/ar/un-global-counter-terrorism-strategy

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

3- مكافحة جريمة الإرهاب الالكتروني على المستوى العربي

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[26] الصادرة سنة 2010، والتي تضمّ العديد من الجرائم الإليكترونية مثل سرقة بطاقات الائتمان، وجرائم الإنترنت والإرهاب الإلكترونيّ، وتصنيع الفيروسات أو نشرها، والقرصنة واختراق الأنظمة، والوصول والاختراق غير المشروع، وغير ذلك. وتهدف هذه الاتفاقيّة إلى تعزيز التعاون بين الدول العربيّة في محاربة الجرائم الإلكترونيّة، وتؤكد على أهمية تنفيذ قوانين حقوق الملكيّة. وتطبق العقوبات على منتهكي شروط ولوائح الاتفاقيّة.

ثانيا: آليات التعاون الدولي لمكافحة جريمة الإرهاب الالكتروني

تنوعت الجهود الدولية في مجال مكافحة جرائم الإرهاب الالكتروني، حيث تم اتخاذ العديد من الآليات للحد والتقليل منها شملت آليات التعاون الإجرائي وأيضا آليات التعاون القانوني والقضائي.

1- آليات التعاون الإجرائي لمكافحة جريمة الإرهاب الالكتروني

تكمن خطورة الأعمال الإرهابية الإلكترونية في اعتمادها على تقنيات متقدمة مثل أجهزة تصنت على شبكات الاتصال، وبرمجيات التشفير، وبرمجيات اختراق أنظمة أمن الشبكات والحاسبات، كما أن الشبكة الآلية الواحدة قد تضم ملايين الحواسب أو الأجهزة المتصلة بالإنترنت التى يمكن استخدامها لشن هجمات متنوعة لأغراض إجرامية كالتخريب والإرهاب والتهديد والابتزاز، الأمر الذي جعل القانون الدولى شأن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الى اعتماد مجموعة من الآليات لمكافحة الارهاب الالكتروني تتمثل فيما يلي:

- **الحفظ العاجل للبيانات المعلوماتية والأمر بتسليمها:**

يقصد بالتحفظ العاجل للبيانات المعلوماتية توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية[27]،

[26] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، على الرابط التالي:
http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pd

[27] بوعنادة فاطمة الزهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013، ص 71.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

ويشمل إجراء الحفظ: المعلومات أو الصور أو الرسائل أو الأصوات التي تعد يتم تخزينها ومعالجتها ونقلها بواسطة تقنية المعلومات، كالأرقام والرموز والأحرف[28].

- **تفتيش المعلومات المخزنة:**

من أجل الكشف عن الجرائم الارهابية ومتابعة مجريمي الإرهاب الالكتروني لابد من تفتيش البيانات المخزنة في تقنية المعلومات أو جزء منها أو إحدى وسائط تخزين المعلومات الالكترونية شريطة التقيد بالضوابط القانونية للتفتيش و احترام الحياة الخاصة للأشخاص، وفي هذا الصدد تلزم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بضرورة تفتيش المعلومة المخزنة[29].

- **اعتراض بيانات المحتوى**

من بين التدابير الإجرائية لردع الإرهاب الالكتروني اعتراض بيانات المحتوى التي الذي نصت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات دون تعريفه، وبالرجوع الى اتفاقية بودابست لسنة 2001 نجدها تعرف بيانات الحركة بأها "بيانات كومبيوتر متعلقة باتصال عن طريق نظام كومبيوتر والتي تنشأن عن نظتم كومبيوتر يشكل جزءا في سلسلة الاتصالات توضح المنشأ والوجهة والزمن والتاريخ والحجم، والمدة ونوع الخدمة الأساسية"[30].

2- التعاون القانوني والقضائي لمكافحة جريمة الإرهاب الالكتروني

أمام تزايد الجرائم الالكترونية التي طالت لدول البنية التحتية للدول، والمؤسسات الحكومية تزايد حجم التعاون الدولي لمكافحة الإرهاب الالكتروني ليشمل التعاون في المجال القانوني والقضائي.

- **تسليم المجرمين:**

عرفت المعاهد النموذجية لتسليم المجرمين الصادر بقرار الجمعية العامة للأمم المتحدة رقم 116/45 تسليم المجرمين على أنه: "مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى ليحاكم بها أو ينفذ فيها الحكم الصادر عليه من محاكمتها"، وفي هذا الشأن ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتسليم مرتكبي الجرائم الالكترونية بما

[28] المادة 02 من الاتفاقية العربية لمكافحة جرائم تقتية المعلومات لسنة 2010.

[29] المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

[30] التقرير التفسيري لاتفاقية بودابست 2001.

مجلة الدراسات القانونية (صنف ج) - Journal OF LEGAL STUDIES (Class C)
مجلة علمية دولية سداسية محكمة صادرة عن مخبر السيادة والعولمة – جامعة يحيى فارس بالمدية (الجزائر)
ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

فيها الإرهاب الالكتروني، وأجازت أيضا الامتناع عن تسليم مواطنيها على أن تتعهد للدول الأطراف الأخرى التي تتقدم اليها بطلب الملاحقة بالمتابعة القضائية ضد مواطنيها الذين ارتكبوا جرائم الكترونية في هذه الدول.

-المساعدة المتبادلة بين الدول

تشمل مجالات المساعدة المتبادلة إجراء التقديم التلقائي للمعلومات بين الدول، حيث أجازت كلا من اتفاقية بودابست لمكافحة جرائم المعلوماتية لسنة 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات للدول الأطراف أن تقدم لبعضها معلومات تحصلت عليها من خلال التحقيقات التي تقوم بها مصالحها المختصة بدون طلب مسبق للمساعدة في إطار التعاون من أجل مواجهة الجريمة الالكترونية والإرهاب الالكتروني، مع جواز طلب إحاطة المعلومات بالسرية التامة في حالة خشية تعرض المصالح الجوهرية للدولة للخطر.

خاتمة

الثورة الكبيرة والطفرة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات كانت السبب وراء بروز مصطلح الإرهاب الإلكتروني أو الإرهاب الرقمي, وشيوع استخدامه، وزيادة خطورة الجرائم الإرهابية وتعقيدها، سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة، فأصبح الإرهاب الإلكتروني هاجسًا يخيفُ العالم الذي يتعرض لهجمات الإرهابيين عبر التكنولوجيًا الحديثة، فالإرهاب والإنترنت مرتبطان عن طريق ممارسة الأعمال التخريبية لشبكات الكمبيوتر والإنترنت.

مما سبق يمكن نستنتج بأنه لا يوجد جهد دولي مُوحَّد لمواجهة الإرهاب الإلكتروني، كما أنه لا توجد حتى جهود موحدة لوضع إطار قانوني لمكافحة كل ما يتعلق بالإرهاب الإلكتروني. خاصة وأن الإرهاب الإلكتروني أصبح أكثر خطورة من غيره من أنواع الإرهاب، لذا يجب على كافة الدول على المستويين الدولي والإقليمي توحيد الجهود ومكافحة الإرهاب الإلكتروني للحفاظ على أمن الدول الداخلي والخارجي. إفراد نصوص قانونية مستقلة لجريمة الإرهاب الالكتروني سواء على المستوى الدولي أو الاقليمي، وبناء عليه نقترح مجموعة من الاقتراحات:

- إيجاد منظمة قانونية دولية تحت مظلة الأمم المتحدة يعهد اليها توحيد توثيق جهود الدول لمكافحة الإرهاب الالكتروني.
- ضرورة إدراج الإرهاب الدولي في قائمة الجرائم الدولية المنصوص عليها في النظام الأساسي للمحكمة الجنائية الدولية.

ISSN 2437-0304
EISSN: 2602-5108
رقم الإيداع القانوني: 3039 -2015
المجلد: 08 العدد: 01 السنة: جانفي 2022 م-جمادى الآخرة 1443 هـ ص: 01 - 16

- الدعوة الى ابرام اتفاقية دولية وثنائية للحد من الارهاب الدولي، وتبادل الخبرات والمعلومات.
- تعزيز التعاون الدولي في مجال المراقبة الالكترونية ومعاقبة مرتكبي الجرائم الإرهابية عبر الوسائط الالكترونية ووضع استراتيجيات لتسليم المجرمين.
- إشراك المجتمع المدني ومؤسساته في التعاون والتبليغ عن المواقع ذات علاقة بالإرهاب والعمليات الإرهابية.
- نشر الثقافة الوقائية وتوعية المجتمع بمخاطر الإرهاب الالكتروني والتصدي لكل محاولات نشر أفكار الكراهية والعنف و الإقصاء، ونشر ثقافة الحوار واحترام الديانات والثقافات على اختلافها.

قائمة المراجع

أولا: المؤلفات

- احمد فتحي سرور، المواجهة القانونية للإرهاب، دار النهضة العربية، القاهرة، 2008.

- أمير فرج يوسف، الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، الإسكندرية، 2011.

- عبد الله بن سليمان، الإجرام المعلوماتي في التشريع المغربي، دار الأمان، الرباط، المملكة المغربية، 2017.

- هايل عبد المولى طشطوش، الإرهاب المعاصر، دار البداية، الاردن، 2014.

محمود أحمد القرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، الأردن، 2017.

-مصطفى يوسف كامل، جرائم الفساد، غسيل الأموال، السياحة، الإرهاب الالكتروني، المعلوماتية، مكتبة المجتمع العربي للنشر والتوزيع، 2014.

ثانيا: الأبحاث العلمية

- ايمان بن سالم، جريمة التجنيد الالكتروني للإرهاب، وفقا لقانون العقوبات الجزائري، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، برلين، ألمانيا، 2018.

بوعنادة فاطمة الزهرة، مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013.

- بدر احمد، الإرهاب الإلكتروني أدواته وآثاره وأساليب الوقاية والعلاج، 16-1-2017، بحث منشور متاح على الموقع الإلكتروني:
http://baathparty.sy/site/arabic/index.php?node=552&cat=15369

- فؤاد براهي، ظاهرة الإرهاب الرقمي وموقف المشرع المغربي منه، مجلة مغرب القانون، 2018، مقال منشور على موقع: https://www.maroclaw.com/ .

- ليندة شرا بشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية، مجلة دراسات وأبحاث، كلية الحقوق، جامعة الجلفة، الجزائر، المجلد رقم 01، العدد الأول، سنة 2009.

- حوراء رشيد مهدي الياسري، الإرهاب الالكتروني وطرق مواجهته، مركز الفرات للتنمية والدراسات الإستراتيجية، متاح على الموقع الالكتروني: http://fcdrs.com/polotics/766 .

- حكيم غريب، الجريمة الالكترونية والجهود الدولية لمكافحتها، المجلة الجزائرية للدراسات السياسية، المجلد 2، العدد الأول، 2015.

- هاني خميس محمد، مفاهيم الأسس العلمية للمعرفة، الارهاب الالكتروني، المركز الدولي للدراسات المستقبلية والاستراتيجية، مصر، العدد 27، مارس 2007.

رابعا: المعاجم

-ابن منظور أبو الفضل جمال الدين محمد بن مكرم، لسان العرب، دار صادر ودار، بيروت، 1955 ، المنجد في اللغة، دار المشرق، بيروت، ط 29، 1986.

- https://www.larousse.fr/dictionnaires/francais/cyberterrorisme/186900 .

- https://www.collinsdictionary.com/dictionary/english/cyberterrorism.

خامسا: النصوص القانونية الدولية

- اتفاقية بودابست لمكافحة جرائم المعلوماتية والاتصالات على الرابط التالي: https://rm.coe.int/budapest-convention-in-arabic/1680739173

-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، على الرابط التالي:

http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/27adcb7a-5539-4b36-9d9a-28b91f578bac.pd

سادسا: التقارير الدولية

-إستراتيجية الأمم المتحدة لمكافحة الإرهاب، مكتب مكافحة الإرهاب - فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب، متاح على:-https://www.un.org/counterterrorism/ctitf/ar/un-global-counter-terrorism-strategy

- تقرير اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، رقم31، لسنة 2011.

- تقرير الاتحاد الدولي للاتصالات، بشأن المبادئ التوجيهية لاستعمال البرنامج العالمي للأمن السيبراني، الوثيقة C20/65، جنيف، 2020.

التقرير التفسيري لاتفاقية الجريمة الالكترونية، متاح على: https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174