ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

# "التعاون الدولي لمكافحة الإرهاب السيبراني"

**إعداد الباحثة:**

**هدى يوسف الزهراني**

**إشراف الدكتورة:**

**غفران عايض سعيد القحطاني**

مشرفة قسم القانون العام

كلية الحقوق

جامعة الملك عبد العزيز

جدة– المملكة العربية السعودية

1445هـ–2024م

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

**الملخص:**

يتلخص محور البحث حول جريمة الإرهاب السيبراني من المنظور القانوني دولياً واقليمياً، حيث تتبلور مشكلة البحث التساؤل الآتي: ما هو التعريف الدولي للإرهاب السيبراني؟ أهداف البحث: تسعى الدراسة في بيان جريمة الإرهاب السيبراني. منهج البحث: اتبعت الباحثة المنهج الوصفي والتحليلي. وقد توصلت الدراسة الى عدد من النتائج والتوصيات اهمها: ان الإرهاب السيبراني لا يختلف عن الإرهاب العادي الا من حيث الوسيلة ومن حيث الانتشار فهو أشد. كما توصي الباحثة بتنظيم الفعاليات العلمية موسميًا للتوعية بخطر الإرهاب. وقد قسمت الباحثة الدراسة إلى ست مباحث: المبحث الأول: عوامل الإرهاب السيبراني، المبحث الثاني: أهداف الإرهاب السيبراني، المبحث الثالث: ماهية الإرهاب السيبراني، المبحث الرابع: أنماط الإرهاب السيبراني، المبحث الخامس: جريمة الإرهاب السيبراني وفقاً للقانون الدولي، المبحث السادس: أهم السوابق قضائية للإرهاب السيبراني.

**الكلمات المفتاحية:** الإرهاب السيبراني، الاتفاقيات الدولية، الجريمة الدولية، السوابق القضائية، آليات مكافحة الإرهاب السيبراني.

**المقدمة:**

ان الناظر والمتأمل يجد أن هنالك مخاطر تهدد أمن الدول، ومن تلك المخاطر ظاهرة الإرهاب، وقد تطورت هذه الظاهرة مع تقدم التكنولوجيا فأصبحت قادرة على تدمير البنية التحتية للدول بشن هجمات إرهابية من خلال الفضاء الإلكتروني، وقد أدى التطور السريع للمعلومات في مجال شبكة الانترنت إلى ظهور آفة جديدة من الجرائم تستعمل التكنولوجيا بطريقة سيئة غير محمودة تؤثر على تنمية المجتمع في مجالات عديدة سياسياً واقتصادياً واجتماعياً، فأصبحنا نواجه مخاطر سيبرانية واقعية تختلف عن الجرائم التقليدية من حيث طبيعتها ووسائلها، تسمى بالجرائم السيبرانية، وهي تقوم باختراق القاعدة الالكترونية تابعة لدولة ما، بغرض التجسس عليها أو تدميرها دون الحاجة لأسلحة متفجرة من قبل جماعات إرهابية مجهولة الهوية مع صعوبة وقوعهم في أيدي السلطات المختصة تستغل نشر الأفكار والأخبار المضللة لتحولها إلى دولة فاشلة.

وبناء على ذلك تطور مفهوم الأمن وأصبح الأمن السيبراني حاجة ملحة للحفاظ على أمن المحتوى الالكتروني للدولة، ومن ثم حاجة الدول إلى اصدار تشريعات دولية لمكافحة الإرهاب السيبراني.

**اولاً: أهمية الدراسة**

**الأهمية العلمية:** تتجلي أهمية دراستنا العلمية بالنظر في حداثة الموضوع، وقلة الدراسات بشأنه، لذا تم تناول آلية مكافحة الإرهاب السيبراني المدمر أمنياً واجتماعياً.

**الأهمية العملية:** تظهر الأهمية العملية بالتصدي لجريمة الإرهاب السيبراني إقليمياً ودولياً تفادياً لما يترتب عليها من تدمير وخسائر فادحة مع صعوبة الكشف عن مرتكبي هذه الجرائم الإرهابية.

## ثانيًا: مشكلة الدراسة

تتمثل مشكلة البحث في الكشف عما يحدث لفضاء الانترنت من غزو إرهابي من قبل المنظمات الإرهابية بهدف تدمير البنية التحتية للإنترنت في كافة أنحاء العالم، وذلك دون استخدام القوة العسكرية بل بإستراتيجيات أكثر دقة وبراعة وتخطيط مع عرض الجهود الدولية لمكافحة هذه الظاهرة قدر المستطاع لما يترتب عليها من تهديد للأمن والسلم الدولي، وذلك من خلال الإجابة على التساؤل الآتي:

**ما هو الإرهاب السيبراني؟**

## ثالثاً: تساؤلات الدراسة

1- ما مفهوم الإرهاب السيبراني؟
2- كيف يعد الإرهاب السيبراني جريمة دولية؟
3- ما هو دور القانون الدولي في محاربة هذه الجريمة الالكترونية؟
4- ما هي صور الإرهاب السيبراني؟

## رابعاً: أهداف الدراسة

تسعى الدراسة لتحقيق عدة أهداف، أهمها:

1- التعريف بماهية الإرهاب السيبراني، وكيفية انتشاره.
2- بيان كيف يعد الإرهاب السيبراني جريمة دولية.
3- التعرف على أهداف الإرهاب السيبراني.
4- ذكر دور القانون الدولي في التصدي للإرهاب الالكتروني.
5- إلقاء الضوء على آليات الدول لمكافحة الإرهاب السيبراني.

## خامسًا: منهج الدراسة

من خلال إتباع المنهج الوصفي، تمكنت الباحثة من وصف ظاهرة الإرهاب السيبراني وبيان دوافعه وخصائصه، وآليات مكافحته، والمنهج التحليلي لتحليل النصوص الموجودة في المواثيق والمعاهدات الدولية المتعلقة بالظاهرة محل الدراسة لمواجهة الإرهاب السيبراني، وسبب اختيار هذا المنهج كونه الأنسب لهذه الدراسة.

## سادساً: الدراسات السابقة

**الدراسة الأولى: الإرهاب السيبراني وانعكاساته على الأمن الوطني.**

إعداد ماجد بن خلاف حمود العنزي، جامعة نايف العربية للعلوم الأمنية، تخصص إدارة الأزمات والكوارث، المملكة العربية السعودية، الرياض، 2020م.

أوجه الشبة والاختلاف بين الدراسة السابقة والدراسة الحالية:

1- أوجه الشبه: تتفق الدراسة السابقة مع الدراسة الحالية في إن كلاهما يتناول موضوع الإرهاب السيبراني وكيفية التصدي له ومحاربته.

2- أوجه الاختلاف: تختلف الدراسة السابقة عن الدراسة الحالية كون الدراسة الحالية تتناول التعريف بالإرهاب السيبراني، ودور المجتمع الدولي في مكافحته بشكل عام بخلاف الدراسة السابقة التي تتمحور حول مدى تأثير الإرهاب السيبراني على الأمن الوطني السعودي تحديداً.

**الدراسة الثانية: استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية، والإرهاب السيبراني.**

إعداد: حازم محمد خليل، جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، مصر، القاهرة، 2023م.

أوجه الشبة والاختلاف بين الدراسة السابقة والدراسة الحالية:

1- أوجه الشبه: تتفق الدراسة السابقة مع الدراسة الحالية في إن كلاهما يتناول موضوع الإرهاب السيبراني، ومدى خطورته على تنمية المجتمع، وإن الحرب في الفضاء الالكتروني يعد مثل ساحة المعركة التقليدية، فيحتاج هجوم ودفاع.

2- أوجه الاختلاف: تختلف الدراسة السابقة عن الدراسة الحالية في كون الدراسة الحالية تتناول مفهوم الإرهاب السيبراني، وبيان خصائصه، وكيف تعاون المجتمع الدولي مع الإقليمي لمكافحة هذا النوع من الإرهاب الذي يهدد الأمن والسلم الوطني والدولي بخلاف الدراسة السابقة التي تتناول ظهور القوة السيبرانية، وبيان طبيعة المجرمين الدوليين خلف هذه الجريمة، وتوضيح دور الوكلاء السيبرانيون.

**الدراسة الثالثة: جريمة الإرهاب عبر الوسائل الالكترونية**

إعداد: مصطفى سعد حمد مخلف، جامعة الشرق الأوسط، كلية الحقوق، 2017.

أوجه الشبه والاختلاف بين الدراسة السابقة والدراسة الحالية:

1- أوجه الشبه: تتفق الدراسة السابقة مع الدراسة الحالية في ان كلاهما يتناول موضوع الإرهاب الالكتروني وبيان مدى خطورته وذكر اركانه.

2- أوجه الاختلاف: تختلف الدراسة السابقة عن الدراسة الحالية في كون الدراسة الحالية تتناول مفهوم الإرهاب السيبراني وكيفية مكافحته دولياً واقليميًا بخلاف الدراسة السابقة تتناول موضوع جريمة الإرهاب عبر الوسائل الالكترونية بشكل مفصل من خلال دراسة مقارنة بين التشريع الأردني والتشريع العراقي.

**المبحث الأول**

**عوامل الإرهاب السيبراني**

تعد مسألة الغايات والأهداف مسألةً أساسيَّةً في جميع الأفعال والأقوال والأعمال التي يقدم أي شخص للوصل لأي هدف كان، ولقد استخدم هؤلاء عدة عوامل للوصول للغاية المقصودة والمنشودة، ومن تلك العوامل ما يلي:

1- عوامل شخصية.

تتعدد الدوافع الشخصية المؤدية للإرهاب السيبراني، ويمكن بيان أهمها فيما يلي:

1- فقدان الشخص لدوره في أسرته، وكذلك في مجتمعه مما يؤدي إلى اكتساب بعض الأمور السلبية.

2- الرغبة في حب الشهرة والظهور، مما يؤثر في على الشخص بحيث لا يكون مؤهلاً لأداء مهامه.

3- نقمة الفرد على المجتمع الذي يقطن فيه [1].

2- عوامل فكرية.

وتتنوع الدوافع الفكرية المؤدية للإرهاب السيبراني، ويمكن إظهار أهمها فيما يلي:

1- عدم العلم بمقاصد أمور الدين المبنية على الأمور الظنية وأمور اليقين التثبت، وكذلك التفسير الخاطئ لمقاصد الشريعة.

2- ظهور الحزبية والتيارات في أوساط المجتمع المسلم.

3- ظهور التطرف والإرهاب والغلو، وكل هذا يزعزع المجتمع [2].

3- عوامل سياسة.

ومن أبرز هذه العوامل العامل السياسي لظاهرة الإرهاب السيبراني، وتتلخص في الآتي:

1- عدم وجود العدالة في أوساط المجتمعات.

[1] الزرفي، علي. (2020)، الجريمة المعلوماتية الماسة بالحياة الخاصة، المكتب الجامعي الحديث، ص 38.

[2] الشمري، غانم مرضي. (2016). الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ص 25.

2- ظهور الظلم في بعض الشعوب والمجتمعات، مما يؤدي لتلك الشعوب حدوث الاضطراب والتطرف والتشدد [3].

**المبحث الثاني**

**أهداف الإرهاب السيبراني**

إن لكل منظمة أو جماعة أو حركة هدف تصغو إليه بأي طريقة وبأي أسلوب من أجل الوصول إليه، ولهذا كان للإرهاب السيبراني أهدافه التي ينشدها، ولهذا استخدمه عدة أهداف لزعزعة الأمن، ومن أهم هذه الأهداف ما يلي:

**1- اختراق سرية البيانات.**

والمقصود باختراق سرية البيانات، أي اكتشاف سرية البيانات الخاصة والوصول للمعلومات الحيوية سواء كانت هذه المعلومات متعلقة بالدول، أو بالأفراد، أو المؤسسات الوطنية، ويتمثل ذلك من خلال الآتي:

1- كسر التشفير: وهذه وسيلة خطيرة بحيث يستطيع المستخدم فهم تلك البيانات، وبهذا تكون بيانات المستخدم مخترقة.

2- عدم مراقبة الداخل: وهذه الخطوة تشكل خطراً عظيما بحيث لا يوجد أي آلية لمراقبة الداخلين على تلك المواقع.

3- إخلال الأمن المادي، والأمن المادي هو: حماية أصول تكنولوجيا المعلومات، مثل: المباني، والمعدات... وغيرها [4].

**2- عدم الحفاظ على سلامة البيانات.**

وهذا الهدف يسعى لعدم تحقيق النزاهة، أو الحفاظ على سلامة البيانات، وذلك بالعبث بها، أو بث محتوها بأي طريقة.

**3- عدم توفير بيانات كافية.**

وعدم توفير البيانات يعني عدم امتلاك القدرة على الوصول إلى المعلومات وتعديلها في الوقت المناسب من قبل المستخدمين المسموح لهم.

[3] القرعان، محمود احمد. (2017). الجرائم الإلكترونية، دار وائل، الأردن، ص 19.

[4] القرعان، محمود احمد. الجرائم الإلكترونية، مرجع سابق، ص 25، وانظر: السند، عبد الرحمن بن عبد الله. (2004). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، جامعة الامام محمد بن سعود الإسلامية، الرياض، مج1 ، ص 33.

**4- عدم حماية الأصول الحيوية.**

ويقصد بالأصول الحيوية البنية التحتية ونظام البيانات والملكية الفكرية، وعدم حماية الأصول الحيوية يعني تعرضها للخسارة، والعواقب الوخيمة [5].

**5- اختراق خصوصية بيانات العملاء.**

وهذا يعني تعرض العملاء للسرقة، أو تعرض بياناتهم للاختراق مما له الأثر الضار على معلومات العملاء [6].

**6- عدم الامتثال للوائح.**

وهذا يعرض المؤسسات لعدم الامتثال للوائح، وهذا يعني أن أصول هذه المؤسسات مخترقة [7].

**المبحث الثالث**

**ماهية الإرهاب السيبراني**

ينطلق الإرهاب بكافة صوره وشتى أنواعه على حقائق وأهداف، ويتميز الإرهاب السيبراني عن غيره من الإرهاب بالطريقة العصرية الحديثة المتمثلة في استخدام الوسائل الإلكترونية التي جلبتها حضارة العصر المتمثلة بالتقنية، ولهذا قام الإرهاب السيبراني بتوظيف طاقته في استثمار هذه الثروة المعلوماتية لتحقيق ما يصبوا إليه في مشروعه الغير المشروع.

إن خطر الإرهاب السيبراني "الإلكتروني" تزداد في الدول التي تدير بنيتها التحتية بالشبكات المعلوماتية، والحواسيب الآلية مما يسهل الوصول إليها، والنيل منها بدلاً من استخدام المتفجرات، وذلك من خلال لوحة المفاتيح مما يلحق الشلل بأنظمة القيادة، والاتصالات وكافة الوسائل ذات الصلة[8] .

ومما سبق يتبين إن ماهية الإرهاب السيبراني "الإلكتروني" يعتمد على استخدام الإمكانات العلمية والتقنية، واستغلال كافة وسائل الاتصال وشبكات المعلومات، من أجل إلحاق الخوف والترويع لدى الآخرين، وكذلك إلحاق الضرر بشتى صوره بهم، وتهديدهم، وهذا هو ماهية الإرهاب السيبراني وحقيقته.

---

[5] الشمري، غانم مرضي، مرجع سابق، ص 31.

[6] القرعان، محمود احمد. مرجع سابق، ص 27.

[7] ينظر: السند، عبد الرحمن بن عبد الله، مرجع سابق، ص 29.

[8] الغامدي، عبد العزيز بن غرم الله. (2017)، جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي، dar alkitab aljami، ص 79.

**المبحث الرابع**

**أنماط الإرهاب السيبراني**

لقد اهتم الخبراء وأخص بالذكر خبراء الجرائم السيبرانية، وأمن المعلومات الإلكترونية بوضع عينات لما وقع من جرائم للسيبرانية، وقام هؤلاء بوضع بحوث ودراسات وتقارير تقوم بمعالجة مثل هذه القضية الخطيرة، ومن أهم هذه الأنماط ما يلي:

**1- القضاء على المواقع والبيانات ونظم المعلومات.**

يقوم الإرهاب السيبراني بتسريب رموز تتعلق بشبكة الإنترنت، وهذه الطريقة يمكن تنفيذها من أي مكان في العالم، وهذه الطريقة لا تحتاج إلى وقت ولا جهد، وكذلك لا يحتاج منفذها إلى تواجد في المكان الذي يريد الهجوم عليه، وبهذا يستطيع شن هجماته بكل سهولة، وتدمير ما يريد تدميره، وإغلاق ما يريد إغلاقه من الموقع ذات الأهمية والحيوية، وتعطيلها تعطيلا تاما، خاصة إذا تمكن من الوصول للأمور ذات الأهمية، مثل: أنظمة القيادة، والاتصالات، وكذلك مواقع البنوك، والطاقة، فمن هنا تصاب هذه المواقع بالشلل التام، وهذه المواقع من أهم المواقع الوطنية التي يهددها الإرهاب السيبراني.

ومن الأمور التي يقوم بها الإرهاب السيبراني هي إرسال عدد كبير من الرسائل الإلكترونية، والغرض من هذا هو: إضعاف القدرة على التخزين الإلكتروني، وهذا يؤدي إلى انهيار المواقع، أو انفجارها فحين إذن تتشتت المعلومات المخزنة على تلك المواقع، وبهذا تتحول هذه المواقع إلى لقمة سائغة ليد الإرهابي، وكذلك تسليط الفيروسات الفاتكة التي تدمر آلاف المواقع والأجهزة الحاسوبية، وأجهزة الهاتف المحمول في فترة وجيزة، [9] وهذا مما لا شك فيه أنه خطر محدق للدول للمجتمعات والأفراد.

**2- الهجوم على النظم العسكرية.**

يستهدف هذا النوع من الإرهاب السيبراني على المواقع العسكرية لأي دولة يريد استهدافها، ويعد هذا النوع من أخطر أنواع الإرهاب السيبراني خاصة أن أهم ما يركز عليه هذا الإرهاب الأسلحة المتطورة، وكذلك نظام الدفاع الجوي، وكذلك الصواريخ ذات التحكم الآلي .[10]

[9] اللبان، شريف درويش. (2016). الإستراتيجية والإعلامية والثقافية لمواجهة داعش. Arab Media & Society، (Issue 21, Spring 2016) ، ص 211.

[10] اللبان، شريف درويش. مرجع سابق، ص 147، 148.

**3- الهجوم على نظام الاتصالات.**

يستهدف هذا النوع من الإرهاب السيبراني على مواقع الاتصالات وشبكات المعلومات، وشبكات الهاتف الدولية والمحلية، وذلك بتعطيلها عبر الهجوم على أبراج بث الإرسال أو بث الاستقبال، وهذا يولد انقطاع التواصل بين أفراد المجتمع، والمؤسسات، ولا شك أن هذا يولد الرعب والخوف في أوساط المجتمع [11].

4- الهجوم على نظام المواصلات.

ولا شك أن هذا النوع من الإرهاب السيبراني يستهدف نظام المواصلات بكافة صورها سواء كانت هذا المواصلات جوية أو بحرية أو برية، فعلى سبيل المثال إحداث خلل في نظام الهبوط للطائرات وإقلاعها، مما ينتج حصول تصادم، أو تعطيل نظام الهبوط مما يؤدي إلى حدوث كوارث إما على ذات الطائرة أو على المطار، وذلك قرصنة معلومات نظام التحكم، وإخلال مواعيد انطلاق الرحلات سواء كانت برية أو بحرية أو جوية [12].

5- الهجوم على النظام الاقتصادي.

يستهدف هذا النوع من الإرهاب السيبراني على البنية التحتية للمجال الاقتصادي، وهذا النوع لا شك فيه أنه يهدد ثاني أهم ركيزة من ركائز الدولة، حيث أصبح هذا المجال هدفاً منشوداً للإرهاب السيبراني [13].

6- الهجوم على محطات الطاقة والمياه.

لقد أصبح نظام شبكات المعلومات خصوصاً عند الدولة المتقدمة من الأمور ذات الأهمية، وذلك لتنظيم الخدمات الكهربائية، وهذا لا شك فيه أنه أصبح لقمة سهلة في أيدي السيبرانية، وهذا الهجوع على هذه الخدمة يؤدي إلى حدوث الخوف في أوساط المجتمع خاصة في انقطاع الخدمة الكهربائية حيث أصبحت عاملا رئيسياً من عوامل الحياة، وذلك الماء لا يمكن توصيله إلى المجتمع إلا عن طريق الطاقة الكهربائية[14].

7- التجسس.

إن نظام التجسس من أهم النظم التي يعتمد عليها الإرهاب السيبراني، وهذا التجسس قد يكون على الدول، أو الأفراد، أو المؤسسات الدولية وغيرها.

---

[11] يونس، عبد الله بن محمد. (2014). شبكات الاستقطاب، مجلة عدن الغد الالكترونية. ص 251.

[12] اللبان، شريف درويش، مرجع سابق، ص 154.

[13] اللبان، شريف درويش، مرجع سابق، ص 152.

[14] اللبان، شريف درويش، مرجع سابق، ص 149.

إن التجسس السيبراني يمتاز بالطرق الحديثة حيث تتمثل هذه الطرق بتوظيف المعلومات حسب الهدف المنشود، وأهم هذه الأهداف: الهدف العسكري، والهدف السياسي، والهدف الاقتصادي.

إن إصابة هذه الأهداف الثلاثة يولد شللا تاما في مسار نهوض الدول.

إن دخول السيبرانية للشبكات وتقنية المعلومات يعد خطراً جسيماً، حيث يهدف للحصول على أسرار الدولة ونقل هذه الأسرار لدول أخرى، ويكمن الخطر إذا كانت هذه الدولة التي وصل إليها المعلومات ذات عداء[15].

**المبحث الخامس**

**جريمة الإرهاب السيبراني وفقاً للقانون الدولي.**

يمكن تقسيم هذا المبحث إلى مطلبين:

**المطلب الأول**

**تعريف جريمة الإرهاب السيبراني**

تعتبر أكثر التشريعات الدولية والعالمية الإرهاب السيبراني جريمة نكراء، حيث يتوفر فيها أبعاد وصور وأشكال مختلفة من الجرائم منها التهديد ونشر الأفكار الضالة والاعتداء على حقوق الآخرين وخصوصياتهم [16].

وعند البحث والتتبع فيما كتب حول هذا الخصوص يتضح أن وجهة نظر المختصين بالإرهاب عموماً والإرهاب السيبراني أو الإرهاب الإلكتروني سواء على المستوى الدولي أو الإقليمي قد انقسمت إلى اتجاهين:

الاتجاه الأول: من لا يرى تعريف الإرهاب عموماً والإرهاب السيبراني خصوصاً إما بسبب صعوبة ذلك، وإما لأنهم يرون أن التعريف قليل الجدوى والفائدة فلا طائل من إضاعة الجهود فيه، بل إن التعريف قد يعود بنتائج عكسية في مجال مكافحة الإرهاب؛ لأن التعريف سيكون ملزماً للجميع بالتزام ما ورد فيه فتضيق من جهود مكافحته، فالواجب عند أصحاب هذا الاتجاه هو الاكتفاء بالوصف فمتى وجد ذو الاختصاص ما ينطبق عليه وصف الإرهاب السيبراني فهو منه انطبق عليه التعريف أو لا، وقد تأثرت كثير من

[15] يونس، عبدالله بن محمد، مرجع سابق، ص 251.

[16] ينظر: الكردي، زين العابدين عواد كاظم. (2018). جريمة الإرهاب المعلوماتي، منشورات الحلبي الحقوقية، بيروت، ص 87.

الاجتماعات والمؤتمرات الإقليمية والدولية بهذا الاتجاه، ومن الأمثلة على ذلك قمة الدول الصناعية التي تم انعقادها في طوكيو سنة 1986م، ومن الأمثلة على ذلك أيضاً المؤتمر الدولي الثامن الذي تم انعقاده في كوبا سنة 1990م[17].

الاتجاه الثاني: من يرى تعريف كلاً من الإرهاب والإرهاب السيبراني؛ لأنه كيف يتم تجريم شيء ومحاربته ولا تعلم حقيقته وماهيته، فالتعريف عندهم يعتبر ضرورة ولازماً من أجل التحذير منه ومحاربته، ووقوفاً في وجه المتلاعبين بمثل هذه المصطلحات حسب مصالحهم الشخصية وأهوائهم الخاصة، أو خدمة لأغراض معينة سياسية أو دينية أو فكرية أو اقتصادية أو غير ذلك[18].

وترى الباحثة انه بالرغم من ان فقهاء القانون الدولي من أصحاب هذا الاتجاه مجمعون على ضرورة وضع الحد والتعريف إلا أن كلمتهم لم تتفق ورؤيتهم لم تتحد في تحديد ماهية وحد وتعريف جريمة الإرهاب السيبراني، فظهرت نتيجة لهذا الاختلاف تعريفات متعددة ومختلفة سواء كان هذا الاختلاف اختلاف في العبارة واللفظ أو اختلاف في المراد والمعنى.

ويعود هذا الاختلاف في الإرهاب السيبراني عند فقهاء القانون الدولي وغيرهم إلى عدة عوامل وأسباب كان لها الأثر البين والواضح في هذا الأمر، ومن أهم هذه العوامل والأسباب:

العامل الأول: عدم اتفاق المختصين بالإرهاب بوجه عام من باحثين وأكاديميين وأمنيين، وكذلك عدم اتفاق فقهاء القانون الدولي بوجه خاص على تعريف وتحديد حقيقة وماهية وحد الإرهاب عموماً[19].

العامل الثاني: تشابه بعض صور الإرهاب بشكل عام أو الإرهاب السيبراني على وجه الخصوص ببعض الأمور والأعمال التي تقوم بها بعض الدول أو الأحزاب السياسية أو الجماعات الدينية وتقرر مشروعيتها إما مطلقاً أو مقيدة ببعض الشروط والأحوال[20].

والذي يبدو أن الأمر يحتاج إلى جهود كثيرة على مستوى دولي يجتمع فيه ذو الكفاءة من أهل الاختصاص المتصفون بالحيادية والموضوعية للتوصل إلى نتائج معقولة ومرضية في مسألة تعريف الإرهاب عموماً والإرهاب السيبراني خصوصاً؛ لأن في كلا

---

[17] ينظر: سعد، حسن المبروك. (2023). جريمة الإرهاب الإلكتروني دراسة مقارنة، رسالة مقدمة لغرض استكمال متطلبات الحصول على درجة الماجستير في القانون الجنائي. الاكاديمية الليبية، ليبيا. ص 9.

[18] ينظر: الجملي، طارق. (2010). مفهوم الجريمة الإرهابية، مجلة الحقوق جامعة الكويت، ع2، ص192. سعد، حسن المبروك، مرجع سابق، ص 10.

[19] ينظر: سعد، حسن المبروك، مرجع سابق، ص 7.

[20] ينظر: سعد، حسن المبروك، مرجع سابق، ص 7، 11.

الاتجاهين السابقين عيباً واضحاً وخللاً بيناً، فمن العيوب الواضحة على الاتجاه الأول الضبابية وعدم ضبط الأمور، وسهولة التلاعب في هذا المجال سواء من جانب أصحاب الفكر المتطرف أو من جانب من يتولى التصدي لهذا الفكر أو يدعي ذلك.

ومن أشد العيوب وأظهرها على الاتجاه الثاني اختلاف وجهات النظر في كثير من الأمور تبعاً للاختلاف السياسي أو الديني أو العقائدي أو غير ذلك، فالفعل الذي تراه الديانة الفلانية أو الحزب الفلاني أو الدولة الفلانية مباحاً ومشروعاً قد يكون عند ديانة وحزب ودولة أخرى جريمة وإرهاباً.

**ومما قيل في تعريف الإرهاب السيبراني ما يلي:**

لم يتعرض القانون المصري لتعريف الإرهاب السيبراني وإنما اكتفى ببيان عقوبة من ارتكب بعض صور الإرهاب السيبراني، كما في المادة التاسعة والعشرين من القانون رقم أربعة وتسعين للعام 2015م في شأن مكافحة الإرهاب، ونص القانون ما يلي: يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن جريمة إرهابية[21].

وجاء في الفقرة الثانية من نفس المادة والقانون ما نصه: ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها...

وكذلك الشأن في القانون الليبي رقم ثلاثة لعام 2014م أو رقم خمسة لعام 2022م التي وضعت بخصوص مكافحة الإرهاب السيبراني الإلكتروني، فلم تتضمن تعريف الإرهاب السيبراني ولكنها تضمنت عدداً من صور هذا النوع من الإرهاب[22].

وقد أصدرت كثير من الدول "مجموعة من الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، إضافة إلى عقد دورات تدريبية... حول موضوع مكافحة جرائم الحاسب الآلي"[23].

[21] القانون المصري رقم 94 لسنة 2015.

[22] القانون الليبي قانون رقم 3 لسنة 2014.

[23] السند، عبد الرحمن بن عبدالله، مرجع سابق، ص 55.

"ففي ماليزيا صدر نظام في عام 1997م للمخالفات الإلكترونية، وقد صنف المخالفات إلى: الوصول غير المشروع إلى الحاسب الآلي والدخول بنية التخريب أو التعديل غير المسموح به وتتراوح العقوبات المحددة بين غرامات مالية تصل إلى 150000دولار ماليزي، مع السجن مدة تصل إلى عشر سنوات.

وفي أيرلندا صدر نظام في عام 2001م للحماية من الجرائم المعلوماتية، يتيح معاقبة الاستخدام غير المسموح به لأجهزة وأنظمة الحاسب الآلي...

أما في الأردن فيجري العمل لإعداد تنظيم يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر الشبكات العالمية للمعلومات، كما تساهم الأردن في إعداد مشروع حول قانون مكافحة جرائم تقنية المعلومات وما في حكمها، والمقدم إلى الإدارة العامة للشؤون القانونية في جامعة الدول العربية"[24].

**المطلب الثاني**

**الإرهاب السيبراني جريمة دولية**

نرى أن الجريمة الدولية هي ما يمس المجتمع الإنساني من اخلال بقواعد القانون الجنائي الدولي ويكون حق العقاب من اختصاص المحكمة الجنائية الدولية بموجب ميثاق روما لعام 1998م.

يقسم فقهاء القانون الدولي الجرائم الدولية إلى عدة أقسام وأبرز هذه الأقسام:

القسم الأول: جرائم الحرب.

القسم الثاني: جرائم ضد الإنسانية.

القسم الثالث: جرائم ضد أمن وسلم البشرية.

وبالنظر في الإرهاب السيبراني الإلكتروني هل يندرج تحت واحد من هذه الأقسام الثلاثة فيصح حينئذ وصفه بأنه جريمة دولية؟ أو أنه لا يمكن ادراجه تحت واحد منها وبناء على ذلك لا يصح وصفه بكونه جريمة دولية؟

للإجابة على هذا السؤال لابد من النظر والتأمل في معنى وحد كل واحد من هذه الأقسام الثلاثة عند فقهاء القانون الدولي، وقد تبين بعد البحث صحة وصف الإرهاب السيبراني بأنه جريمة دولية وأنه يندرج تحت هذه الأقسام، وبيان ذلك كالآتي:

[24] السند، عبد الرحمن بن عبد الله، مرجع سابق، ص 47.

أولاً: أما كونه من جرائم الحرب؛ ترى الباحثة أن جرائم الحرب السيبرانية الإرهابية أصبحت بديلا للحرب التقليدية بالنسبة للقانون الدولي، ومما يدلل على ذلك أن اتفاقيات جنيف وبروتوكولات جنيف عام 1977م قد اعتبرت الأفعال الخطرة جرائم حرب[25]، مع اختلاف الأركان والعناصر والأساليب.

ثانياً: وأما كون الإرهاب السيبراني من الجرائم ضد الإنسانية، ترى الباحثة أن صور الإرهاب السيبراني تتشابه مع الجرائم ضد الانسانية، ويدل على ذلك نظام روما المنشئ للمحكمة الجنائية الدولية في مادته السابعة [26]. ويرى بعض فقهاء القانون الدولي الإرهاب السيبراني الإلكتروني جريمة دولية بحد ذاته [27].

ثالثًا: ونرى أن الأمم المتحدة في المادة الأولى من الاتفاقية الخاصة بعدم القابلية للتقادم في جرائم الحرب والجرائم ضد الإنسانية لعام 1968م[28]، لم تتضمن النص على الجرائم ضد امن وسلم البشرية التي كفلتها ونصت عليها ديباجتها وهذا مناف تمامًا للمواثيق الدولية كافة التي جرمت هذه الأفعال الضارة التي تهدد الامن والسلم الدولي.

كما انه عند عرض الإرهاب السيبراني على الأسس والمعايير المعتبرة والواجب توفرها حتى نتمكن من وصف الفعل بالجريمة الدولية يتبين صحة وصف الإرهاب السيبراني بأنه جريمة دولية، ومن أهم هذه الأسس والمعايير ما يلي:

1- المساس بالمصالح والقيم الدولية، وإذا تأمل الإنسان جرائم الإرهاب السيبراني ومدى انطباق هذا المعيار والضابط عليها يتبن له جلياً دون أدنى شك أو تردد أنه منطبق على الإرهاب السيبراني، فهو العدو اللدود للمجتمع الدولي بأسره، يتعارض مع قيمه، ويضاد مصالحه، ويخالف نظمه وتعاليمه[29].

2- جسامة وعظم النشاط الإجرامي، وذلك بأن يترتب على العمل الإجرامي أثار جسيمة ونتائج وخيمة ضد الإنسانية والمجتمعات والشعوب، وهو ما ينطبق صراحة على الإرهاب السيبراني الإلكتروني[30].

---

[25] ينظر: البروتوكول الأول لعام 1977 الملحق باتفاقيات جنيف.

[26] ينظر: نظام روما الأساسي للمحكمة الجنائية المعتمد في روما 1998م.

[27] ينظر: جمعة، احمد يوسف. (2021). الإرهاب السيبراني والعملات الافتراضية والتجسس الإلكتروني، دار الاهرام، ط1، مصر، ص 70.

[28] ينظر: الأمم المتحدة حقوق الانسان، اتفاقية عدم تقادم جرائم الحرب والجرائم المرتكبة ضد الإنسانية.

[29] ينظر: يوسف، أمير فرج، (2016)، جريمة مكافحة الإرهاب الإلكتروني، دار الكتب والدراسات العربية، الإسكندرية، ص 156.

[30] ينظر: زكور، يونس. (2006). الإرهاب وإشكاليته تحديد المفهوم، مجلة الحوار المتمدن، ع 1785، 2006/12/8م، ص 36.

وبذلك وبما سبق في المبحث الثاني يتبين بوضوح وجلاء أن الإرهاب السيبراني جريمة دولية؛ بل هو جريمة دولية عابرة للحدود حيث لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا"[31]، فلا مكان يحد هذه الجريمة الدولية ولا قيود تمنع انتشارها.

وأما أسباب تصنيف الإرهاب السيبراني جريمة دولية عابرة للحدود فيمكن بيانها في الأمور الآتية:

أولاً: أنه لا يختص بمكان محدد ولا بقعة معينة، فلا حدود تمنعه، ولا حواجز تصده، فـ"لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضراراً فورية لعدد لا يحصى من الضحايا"[32].

ثانياً: جرائم الإرهاب السيبراني لا تحتاج ذوي خبرة وعلم بل تتم من خلال وسائل سهلة الاستخدام.

ثالثاً: أن هذه الجرائم تستخدم وسائل تمكنها من الوصول الى اكبر عدد ممكن من الجمهور الذي يصعب الوصول بمثل هذه الأعداد في الواقع.

رابعاً: الإرهاب السيبراني يتم بواسطة الانترنت فيصل الى جميع العالم فالجمهور المستهدف لا يختص بجهة معينة كما هو الشأن في الإرهاب التقليدي.

خامساً: يعد الإرهاب السيبراني وسيلة سريعة فعالة يبث الإرهابي فكره السام في شتى انحاء العالم بخلاف الإرهاب بالطريقة التقليدية.

سادساً: عدم وجود جهة رسمية تسيطر على الإنترنت [33].

ثامناً: عدم التعاون من بعض الدول والحكومات أو حصول التردد في التعاون من أجل الاتفاق على تحديد الإرهاب وتعريفه، ومن ثم وضع اتفاق دولي لمواجهته والتصدي له، وامتناع تلك الدول إما من أجل تحقيق مصالح مادية أو معنوية أو سياسية[34].

تاسعاً: القدرة على استعمال الأسماء الوهمية والتخفي من خلالها.

---

[31] لطفي، وفاء. (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية، مج 23، ع 1، ص 1.

[32] لطفي، وفاء. مرجع سابق، ص 1.

[33] ينظر: مباركة، سليماني. (2017). الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة عباس خشلة، ع 8، ج1، ص 344. الجزائر.

[34] ينظر: المطرودي، عبد الرحمن، نظرة في مفهوم الإرهاب والموقف منه في الإسلام، الكتاب منشور على موقع وزارة الأوقاف السعودية، ص 51.

ISSN: 2663-5798 || Arab Journal for Scientific Publishing
الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

**المبحث السادس**

**أهم السوابق القضائية للإرهاب السيبراني**

لقد تضافرت الجهود الدولية والإقليمية والمحلية من أجل مكافحة الإرهاب عموماً والإرهاب السيبراني على وجه الخصوص، وقد تنوعت هذه الجهود وتعددت صورها وأشكالها، وقد كان من أهم تلك الجهود المبذولة في سبيل التصدي للإرهاب السيبراني هو متابعة وتعقب وملاحقة المتورطين بهذه الجرائم المنكرة والقبض عليهم ومن ثم تقديمهم للعدالة لمحاكمتهم وإقامة الأحكام التي يستحقونها على جرائمهم، وفي هذا المبحث سأذكر بعض النماذج والأمثلة في هذا الخصوص:

المثال الأول: من أبرز وأشهر السوابق القضائية التي تمت على أشخاص مارسوا الإرهاب السيبراني الإلكتروني القضية التي أقامتها الولايات المتحدة الأمريكية ضد الطالب الأمريكي إيمرسون البالغ من العمر 22 سنة، والذي كان يعرف ويلقب في هذا التنظيم: بأسد الله الشيشاني، وقد قام إيمرسون ومارس العديد من الأعمال الإرهابية السيبرانية كالتحريض على ارتكاب العنف والتخريب ضد دولاً معينة ونشر معلومات تتعلق بصناعة الأسلحة والمتفجرات، وغير ذلك من أعمال الإرهاب الإلكتروني، وقد تم تعقبه وتتبعه حتى قبضت الجهات المختصة عليه، ومن ثم قاموا بتقديمه للعدالة، وقامت المحكمة الأمريكية المحلية للدائرة الشرقية في ولاية فرجينيا في الرابع عشر من شهر يوليو لسنة 2011م بتوجيه عدداً من التهم لهذا الشخص كان من أهمها ضلوعه في الإرهاب السيبراني الإلكتروني[35].

المثال الثاني: الإيقاع بخبير الإرهاب السيبراني لانس مور البالغ من العمر 21 سنة الذي قام بسرقة معلومات تجارية سرية وتم القبض عليه من قبل الجهات المختصة بتهمة الوصول الى جهاز كمبيوتر محمي دون اذن وتم الحكم علي بالسجن والغرامة[36].

الخاتمة:

تناولت الدراسة مفهوم الإرهاب السيبراني من المنظور القانوني، وتناولت نشأته وبيان اختلاف الإرهاب السيبراني عن غيره من حيث الأركان وأهدافه وعوامله وذكر اهم السوابق القضائية ذات الصلة بموضوع الدراسة ودور المجتمع الدولي في التصدي لهذه الجريمة الدولية العابرة للحدود.

[35] ينظر: Pennsylvania Man Sentenced For Terrorist Solicitation And Firearms Offense, press release, july 16, 2023, .https://www.justice.gov/usao-wdpa/pr/pennsylvania-man-sentenced-terrorist-solicitation-and-firearms-offense

[36] ينظر: Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks, PRESS RELEASE , July 19, 2011 , https://www.justice.gov/opa/pr/sixteen-individuals-arrested-united-states-alleged-roles-cyber-attacks

**وقد خلصت الدراسة الى جملة من النتائج والتوصيات أهمها:**

## أولاً: نتائج البحث

الحمد لله الذّي وفقني على إنجاز هذا البحث وقد توصلت في ختامه إلى جملة من النّتائج المهمّة، فمن أهمّها:

- بيان خطر الإرهاب السيبراني على كافة النواحي السياسية والاقتصادية والاجتماعية.
- الإرهاب السيبراني لا يختلف عن الإرهاب العادي إلا من حيث الوسيلة، ومن حيث الانتشار فهو أشد انتشاراً.
- أهم أهداف الإرهاب السيبراني هو زعزعت الأمن، والحاق الضرر في الآخرين.
- أن عوامل الإرهاب السيبراني متنوعة ومختلفة، ولكنها في نهاية الأمر تهدف إلى انتشار الفكر الضال.

## ثانياً: توصيات البحث

- يلتمس من الباحثين والهيئات العلمية بذل المزيد من الجهد في مجال الدّراسات القانونية.
- لابد من التعاون في ابتكار طرق آمنه وذات قوة سيبرانية لتحقيق الامن من الإرهاب السيبراني.
- تنظيم الفعاليات العلمية موسميّا للتّوعية بخطر الإرهاب.
- ضرورة الاستجابة الدولية الى سياسة مشتركة لتفادي انتشار وتوسع الإرهاب السيبراني.

## قائمة المصادر والمراجع:


- الأمم المتحدة حقوق الانسان، اتفاقية عدم تقادم جرائم الحرب والجرائم المرتكبة ضد الإنسانية.
- البروتوكول الأول لعام 1977 الملحق باتفاقيات جنيف.
- جمعة، احمد يوسف. (2021)، الإرهاب السيبراني والعملات الافتراضية والتجسس الالكتروني، دار الاهرام، ط1، مصر.
- زكور، يونس. (2006). الإرهاب وإشكاليته تحديد المفهوم، مجلة الحوار المتمدن، ع 1785.
- سعد، حسن المبروك. (2023). جريمة الإرهاب الإلكتروني دراسة مقارنة، رسالة مقدمة لغرض استكمال متطلبات الحصول على درجة الماجستير في القانون الجنائي. الاكاديمية الليبية، ليبيا.
- السند، عبد الرحمن بن عبد الله. (2004). وسائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها، مج1، جامعة الامام محمد بن سعود الإسلامية. الرياض.
- الجملي، طارق. (2010). مفهوم الجريمة الإرهابية، مجلة الحقوق جامعة الكويت، ع2.
- الزرفي، علي. (2020)، الجريمة المعلوماتية الماسة بالحياة الخاصة، المكتب الجامعي الحديث.
- الغامدي، عبد العزيز بن غرم الله، (2017) جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم المعلوماتية السعودي، daral kitab al jami.
- الشمري، غانم مرضي. (2016). الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن.
- القانون الليبي رقم 3 لسنة 2014.
- القانون المصري رقم94 لسنة 2015.

- القرعان، محمود احمد. (2017). الجرائم الإلكترونية، دار وائل. الأردن.
- الكردي، زين العابدين عواد كاظم، (2018)، جريمة الإرهاب المعلوماتي، منشورات الحلبي الحقوقية، بيروت.
- اللبان، شريف درويش. (2016). الإستراتيجية والإعلامية والثقافية لمواجهة داعش. Arab Media & Society (Issue 21, Spring 2016).
- لطفي، وفاء. (2022). الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجاً، المجلد 23، ع 1.
- مباركة، سليماني. (2017). الإرهاب الإلكتروني وطرق مكافحته، مجلة الحقوق والعلوم السياسية، جامعة عباس خشلة، العدد 8، ج1، الجزائر.
- المطرودي، عبد الرحمن، (2019). نظرة في مفهوم الإرهاب والموقف منه في الإسلام، الكتاب منشور على موقع وزارة الأوقاف السعودية.
- نظام روما الأساسي للمحكمة الجنائية المعتمد في روما 1998م.
- يوسف، امير فرج. (2016) جريمة ومكافحة الإرهاب الإلكتروني، دار الكتب والدراسات العربية، الإسكندرية.
- يونس، عبد الله بن محمد. (2014). شبكات الاستقطاب، مجلة عدن الغد الالكترونية.

- Report, to the Convention for the Protection of Individuals with regard to Automatic Explanatory Report Processing of Personal Data,

28.I.1981,

https://rm.coe.int/16800ca434

- Convention on Cybercrime Budapest, 23.XI.2001,

https://rm.coe.int/1680081561

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار السابع – العدد ثمانية وستون
تاريخ الإصدار: 2 – حزيران – 2024م
www.ajsp.net

# "International Cooperation to Combat Cyber Terrorism"

**Prepared by the researcher:**

**HUDA YOUSEF ALZAHRANI**

**Abstract:**

The focus of the research on the crime of cyber terrorism from an international and regional legal perspective, where the research problem crystallizes the following question: What is the international definition of cyber terrorism? Research objectives: The study seeks to explain the crime of cyber terrorism. Research methodology: The researcher followed the descriptive and analytical method. The study reached a number of results and recommendations, the most important of which are: Cyber terrorism does not differ from ordinary terrorism except in terms of means and in terms of spread, it is more severe. The researcher also recommends organizing scientific events seasonally to raise awareness of the danger of terrorism. The researcher divided the study into six sections: The first section: Factors of cyberterrorism, The second section: The goals of cyberterrorism, The third section: The nature of cyberterrorism, The fourth section: Patterns of cyberterrorism, The fifth section: The crime of cyberterrorism according to international law, The sixth section: The most important Case law on cyber terrorism.

**Keywords:** Cyber terrorism, International agreements, International crime, Case law, Mechanisms for combating cyber terrorism.