مجلة الباحث العربي
Arab Researcher Journal
ISSN: 2709 – 0647/DOI: 10.57072

مجلد 6 عدد 2 (2025)

الحماية الجنائية الدولية في مواجهة الجرائم السيبرانية وآلياتها
(الإرهاب السيبراني الدولي نموذجاً)

International Criminal Protection in the Face of Cybercrimes
(International Cyber Terrorism as a Model)

د. مصطفى نجاح مراد، مدرس القانون الدولي العام بكلية القانون جامعة الكنوز –البصرة –العراق
Dr. Moustafa Nagah Mourad, Lecturer of Public International Law, Faculty of Law, Al kunooze University , Basra, Iraq.
https://doi.org/10.57072/ar.v6i2.169

نشرت في 2025/06/27

المستخلص:

مما لاشك فيه أن التطور الذي نعيشه في عصر ثورة المعلومات والاتصالات أفرز لنا العديد من أنواع الجرائم المستحدثة الأشد خطورة ومنها الجرائم السيبرانية والتي أفرزت بدورها جملة من التحديات على المجتمع الدولي نظراً لصعوبة إثباتها ومعرفة مرتكبيها لأنها بطبيعتها جريمة عابرة للحدود والقيود، ولذلك نتناول في هذا البحث إحدى صورها وهي جريمة الإرهاب السيبراني الدولي من حيث وضع تعريف محدد ودقيق لجريمة الإرهاب السيبراني وخصائصها وتعزيز ومضاعفة الجهود الدولية في مكافحتها خاصة في تلك الدول التي لم تبادر بعد إلى تعديل تشريعاتها الداخلية بما يضمن تجاوز القوالب القانونية التقليدية العتيقة بما يتواكب مع مناهضة هذا النوع من الجرائم السيبرانية ولذلك فإن العمل على إرساء قواعد التعاون الإقليمي الدولي في مجال التكنولوجيا ومكافحة الجرائم السيبرانية التي تتم عبر الفضاء السيبراني وكذلك السعي نحو إيجاد إطار قانوني للتعاون الدولي الجنائي قضائيا وأمنياً بات أمراً ضرورياً ولزاماً للغاية التي بات والاعتراف بوجودها أصبح أمراً حتمياً كما نعترف بمخاطرها وهو أمر لا فكاك منه في ظل التطور التكنولوجي المتلاحق في أساليب تلك الجرائم بما يجعل من صعوبة مكافحتها دون تكاتف وتلاحم الجهود الدولية أمراً يجب الوقوف عليه ويجب أن يعمل المجتمع الدولي من الآن على قدم وساق من أجل وضع تشريعات جنائية وطنية ودولية لمواجهة هذا النوع من الجرائم بالإضافة لجملة من التوصيات للحد من هذه الجرائم.

الكلمات المفتاحية: الجرائم السيبرانية، المجتمع الدولي، التعاون الدولي الجنائي.

Abstract:

There is no doubt that the development we are living in the era of the information and communications revolution has produced for us many types of newly emerging crimes that are more dangerous, including cybercrimes, which have produced a number of challenges for the international community due to the difficulty of proving them and identifying their perpetrators because they are, by nature, a crime that crosses borders and restrictions. Therefore, in this research, we have addressed one of its forms, which is the crime of international cyberterrorism, in terms of establishing a specific and precise definition of the crime of cyberterrorism and its characteristics, and strengthening and doubling international efforts to combat it, especially in those countries that have not yet taken the initiative to amend their domestic legislation to ensure that they go beyond the old traditional legal templates in line with combating this type of cybercrime. Therefore, working to establish the rules of regional and international cooperation in the field of technology and combating cybercrimes that take place through cyberspace, as well as striving to find a legal framework for

استلم البحث في 2024/12/17 قبل للنشر في 2025/06/12

international criminal cooperation, judicially and security-wise, has become a very necessary and binding matter, the recognition of which has become inevitable, as we recognize its dangers as an inescapable matter in light of the successive technological development in the methods of these crimes, which makes it difficult to combat them without cooperation. The cohesion of international efforts is something that must be addressed, and the international community must work from now on to develop national and international criminal legislation to confront this type of crime, in addition to a set of recommendations to reduce these crimes.

Keywords: Cybercrimes, international community, international criminal cooperation.

المقدمة:

إن ما يشهده العالم من ثورة تكنولوجيا المعلومات والاتصالات في الآونة الأخيرة ساهم في ظهور مجتمع معلوماتي سهل أمور الحياة على الأفراد وفي نفس الوقت افرز لنا آثاراً سلبية ناتجة عن استخدام تلك التكنولوجيا حيث سهلت ارتكاب أفعال إجرامية ضارة للعالم بأسره في شتى المجالات والأمر لا يخلو من مخاطر جسيمة ومعقدة من ذوي المصالح والأهداف الخبيثة التي وجدت من الفضاء السيبراني وسيلة مثلى للسطو والإرهاب والتخويف للدول والأفراد على حد سواء حال استخدام تلك الوسائل من وسائل الاتصال الحديث الفضائي.

فنشأت صور جديدة من الجرائم وهي الجرائم المستحدثة التي تختلف كلياً وجزئياً عن الجرائم التقليدية إذ أنها ترتكب عن طريق التهديدات والهجمات السيبرانية عبر الفضاء السيبراني وهي ما يسمى بالجرائم السيبرانية وتعتبر من أخطر أنواع الجرائم الدولية لما تشكله من مخاطر تهدد العالم على مستوى الأفراد أو الدول كانت متقدمة أو نامية بمؤسساتها وبقطاعيها العام والخاص، وقد ساهم في نجاح هؤلاء الإرهابيون في مسعاهم وتحقيق أهدافهم ظهور تلك الشبكات المعلوماتية التي ربطت التنظيمات الإرهابية ببعضها وزادت من التنسيق بينهم لارتكاب جرائم أطلق عليها جرائم الإرهاب السيبراني التي تعتبر من أهم وأخطر التحديات التي يواجهها المجتمع الدولي بأسره، وقد يتخذ ذلك الإرهاب صورا متباينة من إنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات (الإنترنت) بهدف بث ونشر أفكارهم الضالة وتجنيد ارهابيين جدد من جهة وبالسطو والولوج إلى مواقع تخص دول وسرقة المعلومات والبيانات وتدميرها أو محوها واختراق البنية التحتية لمؤسسات هذه الدول وقطاعاتها الحيوية من دفاع وأمن وصحة وغيرها أو أفرادها أو شركات القطاع الخاص باختلاف الاحوال وبحسب الاهداف المطلوبة لزعزعة سيادة الدول وتهديد أمنها القومي من جهة أخرى.

وهذا الموضوع يحتل حيزاً كبيراً من المهتمين بالقانون الدولي لما أحاط بتعريف الإرهاب السيبراني الدولي الكثير من الغموض باعتباره نوعاً مستحدثاً من الجرائم ومرتبطاً بظهور ثورة المعلومات والاتصالات وفي ضوء ما سبق غدت الضرورة إلى وضع تعريف جامع مانع لجريمة الإرهاب السيبراني الدولي ولكن لم يجمع الفقهاء على تعريف موحد بمنأى عن الاختلاف وكذلك وضع العقوبات والجزاءات التي تتناسب مع جسامة الفعل ومقدار الضرر سواء في الانفس أو الأموال أو كليهما وتعزيز الجهود الدولية في مواجهة جرائم الإرهاب السيبراني الدولي وباتت الحاجة ملحة للتعاون الدولي والإقليمي في سن تشريعات صارمة لمواجهة هذا النوع من الجرائم المستحدثة.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

- وضع تعريف دقيق ومحدد وواضح وجامع لجريمة الارهاب السيبراني الدولي.
- التأكيد على دور المجتمع الدولي في ضرورة التعاون الدولي والإقليمي ووضع استراتيجية موحدة لمواجهة جرائم الإرهاب السيبراني الدولي والحد منها.
- ضرورة إيجاد الحلول التشريعية والعملية والأكاديمية للحماية من جرائم الإرهاب السيبراني الدولي.
- الوقوف على التحديات القانونية الناتجة عن جرائم الإرهاب السيبراني الدولي.
- تجاوز القوالب القانونية التقليدية العتيقة بما يتواكب مع هذا النوع من الجرائم السيبرانية.

- إيجاد إطار قانوني للتعاون الدولي الجنائي قضائياً وأمنياً في مواجهة الإرهاب السيبراني.
- تعزيز الثقافة القانونية في مجال القانون الدولي الجنائي بهذا النمط الجديد من الجرائم السيبرانية.

إشكالية الدراسة:

ويطرح هذا الموضوع إشكالية تتمحور حول: ماهية جريمة الإرهاب السيبراني الدولي والآليات الجنائية الدولية والإقليمية والوطنية لمواجهة هذا النوع من الجرائم؟

وتتضح الإجابة على الإشكالية الرئيسية من خلال سبر أغوار البحث والتدقيق والتمحيص للإجابة على الاسئلة الاتية:

- ما مفهوم الإرهاب السيبراني الدولي؟
- ما مدى أهمية مواجهة جرائم الإرهاب السيبراني الدولي؟
- ما موقف بعض التشريعات الداخلية إزاء هذه الجرائم؟
- ما مدى تطبيق قواعد القانون الدولي الساري وما دور الاتفاقيات والمعاهدات والمنظمات والمؤتمرات الدولية في مواجهة هذه الجرائم؟

الدراسات السابقة:

هناك العديد من الدراسات التي تناولت موضوع الإرهاب السيبراني ومنها التجربة المصرية في مواجهة هذا الاخير، والإرهاب السيبراني: المفهوم والسمات والأنماط، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، وغيرها من الدراسات العديدة للوقوف على تعريف موحد على لهذه الجرائم والمسؤولية الناشئة عنها سواء كانت جنائية أو مدنية وسبل مواجهتها.

منهج الدراسة:

سوف نتبع أكثر من منهج، من تم سوف نستخدم المنهج الاستقرائي الاستنباطي في قراءة الدراسات السابقة والابحاث المتعلقة بالموضوع، واستنباط الحلول والافكار واعادة توظيفها بما يخدم البحث، وكذلك المنهج التحليلي باستعراض النصوص والاتفاقيات الدولية المرتبطة بالبحث ودراستها وتحليلها، وسوف نستخدم المنهج المقارن للوقوف على التشريعات المقارنة للوصول إلى أفضل السبل لمعالجة اشكالية البحث

خطة الدراسة:

مطلب تمهيدي: ماهية الحق في الخصوصية وجريمة الإرهاب السيبراني الدولي

الفرع الأول: مفهوم الحق في الخصوصية

الفرع الثاني: مفهوم جريمة الإرهاب السيبراني الدولي وخصائصها

المبحث الأول: الآليات والجهود الدولية والإقليمية في مواجهة جريمة الإرهاب السيبراني الدولي

المطلب الأول: دور الاتفاقيات والمنظمات الدولية والإقليمية في مواجهة جرائم الإرهاب السيبراني الدولي

المطلب الثاني: دور المؤتمرات والندوات والملتقيات الدولية والإقليمية في مواجهة جرائم الإرهاب السيبراني الدولي

المبحث الثاني: نماذج تطبيقية لجرائم الإرهاب السيبراني الدولي والجهود الوطنية لمواجهتها

المطلب الأول: الجهود الوطنية المصرية في مواجهة جرائم الإرهاب السيبراني الدولي

المطلب الثاني: النماذج التطبيقية لجرائم الإرهاب السيبراني الدولي.

مطلب تمهيدي:

ماهية الحقّ في الخصوصية وجريمة الإرهاب السيبراني الدولي

الفرع الأول: مفهوم الحق في الخصوصية

إن الحماية الجنائية تعد من أنواع الحماية القانونية في مجملها على حقوق وحريات وكيان الإنسان ذلك القانون الجنائي الذي تنفرد نصوصه بتحقيق تلك الحماية ولا مانع من اشتراك غيره من فروع القانون الأخرى لتحقيق ذلك الهدف وتلك الغاية.

وبوجه عام فإن المقصود بالحماية الجنائية الدولية لحقوق الإنسان في هذا الشأن "مجموعة القواعد القانونية التي تتصف بالعمومية والتجريد والتي وضعتها الجماعة الدولية في صورة معاهدات ملزمة وشرعت لحماية حقوق الإنسان من عدوان السلطة العامة وحدها الأدنى والتي تمثل القاسم المشترك بين

بني البشر في إطار من المساواة وعدم التمييز تحت إشراف ورقابة دولية خاصة.

في هذا الخصوص فقد نص النظام الأساسي للمحكمة الجنائية الدولية على الطبيعة القانونية للحماية الجنائية لحقوق الإنسان المنتهكة خلال ديباجة النظام الأساسي والتي نصت في الباب الأول على إنشاء المحكمة يكون لغرض حفظ السلم والأمن الدوليين وللحفاظ على الروابط المشتركة بين الشعوب والمتمثلة في ثقافات الشعوب وأيضاً ينص النظام الأساسي كذلك على الجرائم الداخلة في اختصاص المحكمة والتي تشكل انتهاكاً صريحاً لحقوق الإنسان

الحق في حماية البيانات الخاصة والشخصية والمقصود بذلك حماية كافة المدونات الخاصة والشخصية للمستخدمين من منشورات وصور وارقام ومناسبات وهو ما صدر عن الجمعية العامة للأمم المتحدة إذ أكدت على حق الإنسان في الخصوصية الذي لا يسمح بتعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أوفي شؤون اسرته أو بيته أو مراسلاته وحقه في التمتع بحماية القانون من مثل هذا التدخل ولا يخفى على منصف أن وسائل التقنية الحديثة قد ساهمت بشكل عظيم في رفاهية نشر وتوثيق ونقل البيانات ولكن على جانب آخر قد يكون ذلك المحتوى عرضة للتجسس أو الاختراق أو التدمير أو المحو من خلال شبكة المعلومات وفي هذا المقام نعرض بإيجاز نظرا لأهميته لجانب مما تناولته الاعلانات الدولية في تقرير الحق في الخصوصية لكافة البيانات الشخصية.

أولاً: الإعلان العالمي لحقوق الإنسان 1948 في المادة 12 قرر أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون اسرته أو مراسلاته ولا لحملات تمس شرفه وسمعته".

ثانياً: إعلان القاهرة حول حقوق الإنسان في الاسلام 1990 وتضمنت المادة 18 فقرة ب "للإنسان الحق في الاستقلال بشؤون حياته الخاصة في مسكنه واسرته واتصالاته ولا يجوز التجسس أو الرقابة أو الإساءة لسمعته".

ثالثاً: العهد الدولي الخاص للحقوق المدنية والسياسية لسنة 1966 المادة 17 منهم تضمنت أنه "لا يجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصياته أو في شؤون اسرته".

وتأكيداً على الحق في خصوصية بيانات الأشخاص الشخصية في الاتفاقيات الإقليمية لحقوق الإنسان ومنها:

أولاً: الميثاق العربي لحقوق الإنسان لعام 2004 في فقرته الثالثة من المادة 2 حينما نص على أنه لا يجوز اخضاع حرية الإنسان في اظهار دينه أو عقيدته أو ممارسة شعائره إلاّ للقيود التي ينص عليها القانون

ثانياً: الاتفاقية الأوروبية لحقوق الإنسان سنة 1950 حينما نصت على: لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.

ثالثاً: الاتفاقية الأمريكية لحقوق الإنسان 1969 لحماية الحق في الخصوصية والتي قررت أنه لا يجوز أن يتعرض أحد لتدخل غير مشروع أو تعسفي في حياته الخاصة أو شؤون اسرته أو من منزله أو مراسلاته.

رابعاً: الميثاق الافريقي لحقوق الإنسان والشعوب 1981 حيث نص في مادته الرابعة على أنه لا يجوز انتهاك حرمة الإنسان ومن حقه احترام حياته وسلامته البدنية والمعنوية لا يجوز حرمانه من هذا الحق تعسفياً.

وترتيباً على ما تقدم نجد أنه حرصت كل المواثيق والعهود الدولية والإقليمية على حماية البيانات الخاصة والشخصية للمستخدمين لأنها تمثل انتهاكاً شديداً لحرمة الإنسان وحقه في الاستقلال والحرية وذلك بحماية بياناته الشخصية ومراسلاته بشكل شديد في كل الازمنة والعصور والثقافات والحضارات.

ونحن نرى في هذا المقام أن عملية إصباغ الحماية الجنائية بشكل كامل على الجرائم السيبرانية والمعلوماتية التي ترتكب عبر الفضاء السيبراني على النطاق الدولي تحتاج لمزيد من الوقت وتظافر الجهود الدولية بشكل مضاعف للحد من مخاطرها لأنه من الصعوبة عملية الإثبات في مثل هذه الجرائم وتضارب المصالح بين الدول بما قد يخل باكتمال ووضع

حماية جامعة مانعة تستعصي على الفهم والحيلولة دون حدوثها.

الفرع الثاني: مفهوم جريمة الإرهاب السيبراني الدولي وخصائصها

أولاً: مفهوم جريمة الإرهاب السيبراني الدولي:

الإرهاب لغة هو التخويف والترويع وبث الرعب في النفوس وما يعنينا هنا هو الإرهاب ليس بمعناه التقليدي بالمواجهة المسلحة أو العمليات التي تقوم بها أفراد أو جماعات بالاستناد إلى دوافع ذات طبيعة سياسية في الغالب الاعم من الحالات وزعزعة الاستقرار والطمأنينة لدى الدول والشعوب.

اما المعنى الاصطلاحي فقد تناولته الاتفاقية العربية لمكافحة الإرهاب الموقعة في القاهرة عام 1998: وهو كل فعل من أفعال العنف أو التهديد به أيّاً كانت بواعثه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى القاء الرعب بين الناس أو الترويع بإيذائهم أو تعريض حياتهم أو حريتهم أو أمنهم أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الاملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها وكذلك تعريض الموارد الوطنية للخطر (الدرويش، 2017).

وذكرت كلمة الإرهاب بمعنى الخوف والفزع في القران الكريم حيث قال تعالى "قال ألقوا فلما ألقوا سحروا أعين الناس واسترهبوهم وجاءوا بسحر عظيم" صدق الله العظيم سورة الأعراف آية 116.

وذكرت في موضع آخر من كتاب الله بمعنى الروع حيث قال تعالى "وأعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم وآخرين من دونهم لا تعلمونهم الله يعلمهم" سوره الأنفال آية 60.

إنما الإرهاب المقصود في بحثنا هذا وهو المرتبط بالثورة التكنولوجية التي شهدها العالم في الحقبة الاخيرة وخصوصاً في فترة الثمانينيات وتناوله بعض الفقهاء بكونه "التقاء ما بين الفضاء السيبراني والإرهاب" (كريمة غلاف وزهوره جلال، 2020) ويرتبط بهذا الإرهاب السيبراني تعطيل نظم السيطرة والرقابة السيبرانية بحيث أضحى مشكلة في عمل الأجهزة والمرافق الحكومية فضلاً عن إحداث الضرر الجسيم وهو ما سوف نتناوله بشيء من التفصيل على النحو التالي.

يمكن تعريف الإرهاب السيبراني بأنه "نشاط إجرامي يتم من خلال شبكة الإنترنت بهدف بث الافكار المتطرفة سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد وإفساد عقائدهم وإذكاء تمردهم واستغلال معاناتهم في تحقيق مآرب خاصة تتعارض مع مصالح المجتمع والجماعة (بوادي ح.، 2006)، ولمزيد من تحليل التعريف السابق نجد أنه "العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل السيبرانية الصادر عن الدول أو الجماعات أو الأفراد على الإنسان أو دينه أو نفسه أو عرضه أو عقله أو ماله وذلك بغير حق.

وثمة رأي آخر في الفقه إلى أن الإرهاب السيبراني يعني أنه: "كل هجوم مدبر بدوافع سياسية ضد المعلومات أو أنظمة الكمبيوتر أو برامج الكمبيوتر والبيانات التي ينتج عنها عنف ضد أية أهداف غير عسكرية أو أنشطة مجموعات أو عملاء سريين (المشرف، 2004).

وثمة رأي آخر إلى أنه كل فعل إجرامي يرتكب باستخدام إمكانيات الحاسوب أو الاتصالات وينتج عنه عنف أو تدمير أو تعطيل للخدمات لخلق حالة من الخوف نتيجة للاضطراب بغرض إكراه الحكومة أو الجمهور للقبول بأجندة سياسية أو اجتماعية أو فكرية (المشرف، 2004).

وثمة رأي آخر بأنه عمل إجرامي يتم الاعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه متلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة (عطية، 2014).

ونحن نرى أن جريمة الإرهاب السيبراني عبارة عن هجوم مجهول المصدر ممنهج وموجه عن طريق الأجهزة الالكترونية عبر الفضاء السيبراني لتدمير المعلومات أو البرامج أو سرقة البيانات أو محوها أو إتلافها لتعطيل الخدمات وخلق حالة من الاضطرابات في الدول أو المؤسسات أو تهديد الأفراد بالخوف والعنف.

أو كل فعل من مصدر مجهول يصدر من خلال الحاسوب وأية أجهزة إلكترونية عبر الفضاء السيبراني من شأنه التهديد بإلحاق الضرر أو تنفيذ تلك التهديدات بغرض تحقيق أجندة أو هدف ضد دولة أو مؤسسة أو أفراد سواء بسرقة بيانات أو

محوها أو بث معلومات من تلك الجماعة بما فيه تحقيق الضرر للدولة أو الكيان (الضحية المستهدفة) سواء كان ضررا في الأموال أو الارواح أو البنية التحتية للضحية".

وقد أدى الفضاء السيبراني إلى تحول الإرهاب إلى تهديد عالمي وأصبح ذلك الإرهاب جريمة عابرة للحدود القومية والدولية من حيث النشاط والخطط والتمويل والأعضاء وقد تصاعدت أنشطة الجماعات الارهابية عبر الفضاء السيبراني وتم استخدام المنجزات التكنولوجية في ممارسة الإرهاب والتي استطاع الإرهابيون من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض (ربيع حسن وسيد رفاعي، 2001).

ثانياً: خصائص جريمة الإرهاب السيبراني الدولي:

سبق وأن تناولنا سابقاً أن جريمة الإرهاب السيبراني قد اختلف الفقهاء في وضع تعريف جامع مانع لها إلاّ أنه بوجه عام يمكن توصيفها بأنها استخدام الوسائل السيبرانية والتقنيات الرقمية الصادرة عن الدول أو الجماعات أو الأفراد ضد شخص طبيعي أو اعتيادي بدوافع قد تكون سياسية في الغالب الاعم منها بهدف إخافته أو تهديده أو التأثير فيه مادياً أو معنوياً أو التأثير كذلك في القرارات الحكومية أو الرأي العام.

وهناك عدة خصائص وسمات يتميز بها الإرهاب السيبراني الدولي عن باقي الجرائم وتحول دون اختلاطه أو التباسه بالإرهاب التقليدي العادي (خليفة، 2021) وتلك الخصائص يمكن إيجازها على النحو التالي:

أ. الحاسب الآلي هو أداة ارتكاب جريمة الإرهاب السيبراني: من المسلم به في القوانين الجنائية لدى كافة الدول أن أداة الجريمة تلعب عنصراً هاماً للغاية في إثبات الجريمة ونسبتها إلى فاعلها وعلى النحو الاخر فأن الإرهاب السيبراني لابد من وجود جهاز الحاسوب الذي لا مناص منه لارتكاب الجريمة وهو النافذة التي تطل بها شبكة الإنترنت على غيرها من الأجهزة المستهدفة الضحية (لطفي و.، الجهود الدولية في مجال مكافحة الإرهاب السيبراني، التجربة الماليزية نموذجاً، 2022).

ب. جريمة الإرهاب السيبراني عابرة للحدود: تعتبر تلك الجريمة غير خاضعة لنطاق إقليمي محدد فهي بذلك قد تمتد آثارها عبر الدول والقارات فقد يكون المجرم في دولة بينما الضحية في دولة أخرى تماماً وجنسيات مختلفة أيضاً حيث لا حدود في مواجهة الجريمة الخاصة بالإرهاب السيبراني وذلك بفضل تطور التكنولوجيا والاتصالات التي مهدت للتنظيمات الإرهابية المجال الخصب والأرض الملائمة لارتكاب أنشطتها الإرهابية على الصعيد الرقمي مما أسبغ على تلك الجرائم ظاهرة العالمية (بونس، 2014).

ج. جريمة الإرهاب السيبراني ترتكب عبر شبكة الإنترنت: إن شبكة النت هي حلقة الوصل بين القائم بالجريمة والضحية الأمر الذي دعا إلى ضرورة تطوير نظم الأمن السيبرانية تباعاً للحماية والحد من الإرهاب السيبراني ويقصد بالشبكة العالمية ارتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات.

د. صعوبة الإثبات في جرائم الإرهاب السيبراني: وهو من أهم سمات جريمة الإرهاب السيبراني حيث يظهر ذلك في سرعة غياب ومحور طمس وتدمير الدليل الرقمي (الفتلاوي، 2004) حيث يظل الفاعل غير معلوم في الكثير من الجرائم المعلوماتية بل قد يظل اكتشاف وقوع الجريمة لفترة خاصة في مجال الاختراق وهو ما يساعد الإرهاب السيبراني على الحركة داخل المواقع المستهدفة، كذلك فإن عنصر صعوبة الإثبات قد يمثل أحد أهم الأسباب المساعدة في ارتكاب جرائم الإرهاب السيبراني لأنها تعطي الجاني أملاً في الافلات من العقوبة.

هـ. الإرهاب السيبراني يتطلب خبرة ودراية عالية من القائمين عليه: لابد أن يتوفر عنصر الخبرة العميقة والدراية الفنية الواسعة في استخدام الحاسب الآلي وكذلك توافر سعة الافق والحيلة فلابد أن يكون لديهم العلم بالتقنية الحديثة ومهارات ومعارف الكمبيوتر والإنترنت.

و. جريمة الإرهاب السيبراني تتطلب في الغالب تعاون أكثر من شخص.

ز. جريمة الإرهاب السيبراني من الجرائم ذات الخطورة: وهي من أهم الخصائص المنسوبة لجريمة الإرهاب السيبراني وهي خاصة ليست مستقلة بذاتها بل مرتبطة باستعمال التقنيات الحديثة التي أصبح لا غنى عنها مطلقاً في العالم بأسره والتي أصبحت بها قوام الحياة بحيث لا يمكن الاستغناء عنها مطلقاً فجريمة الإرهاب السيبراني يمكن أن تؤدي إلى إلحاق الضرر حتى بالدولة الاكثر تقدماً وليس هناك من سبل وطرق لمواجهتها والسيطرة عليها بشكل كامل.

ح. الهدف من جريمة الإرهاب السيبراني والنظم المعلوماتية: يكمن الهدف من تلك الجريمة في الحصول على المعلومات والبيانات السيبرانية المحفوظة على أجهزة الحاسوب أو المنقولة عبر شبكة الإنترنت حيث تساعد هذه المعلومات المستهدفة في الوصول إلى أهدافها الإرهابية (القحطاني ع.، 2017).

وعلى ذلك فإن المعلومات ليست مستهدفة بذاتها وإنما يراد منها الوصول إلى تحقيق أهداف أخرى مثل الاستيلاء على الأموال من الجهاز المصرفي أو الوصول إلى الأشخاص أو الجهات المستهدفة وبناء على ما تقدم يمكن الجزم بأن الإرهاب السيبراني يستهدف النظم المعلوماتية وهو الحد الفاصل بينه وبين صور الإرهاب الأخرى بما فيها الإرهاب التقليدي وهو وسيلة آمنة بطبيعتها لتحقيق أهداف الجاني غير المباشرة فضلاً عما قد يؤدي اليه من خسائر فادحة في الاقتصاد المستهدف نتيجة تعطيل سير المرافق الاقتصادية أو الاجتماعية سواء العامة أو الخاصة (الحلاوي، 2006).

وبناء على ما تقدم نجد أن جريمة الإرهاب السيبراني متفردة بجملة من السمات التي أضحت مميزة لها دون غيرها من صور وأشكال الإرهاب الأخرى وإن كان المجتمع الداخلي يسعى إلى مواجهتها بما أوتي من قوة ووضع نظم حماية تكفي مواجهة تلك الجرائم الحديثة.

المبحث الأول:

الآليات والجهود الدولية والإقليمية في مواجهة جريمة الإرهاب السيبراني الدولي

تمهيد وتقسيم:

إن المجتمع الدولي الذي اكتوى بنيران وأضرار وأخطار الإرهاب السيبراني الدولي بات حريصاً كل الحرص على وضع أطر وتنظيم وقواعد حاكمة له لأنه نظام جديد من الحروب الـ غير التقليدية والتي قد تفوق في أضرارها وأخطارها الحروب التقليدية فضلاً عن عدم التكلفة المادية الهائلة التي تتطلبها هذه الاخيرة فكان ذلك شبه رادع للدول في التفكير كثيراً قبل الاقدام على أي نظام مسلح ولكن الأمر في الإرهاب السيبراني الدولي غير ذات تكلفة مقارنة بتكلفة الحروب التقليدية لذلك سارعت الدول كافة ومن خلال الجهود العالمية والدولية والإقليمية والوطنية لتنظيمه ومجابهة ذلك النوع من الحروب الحديثة (لطفي و.، 2022) واتخاذ أكثر من سبيل مساعد في ذلك مثل تأمين المواقع بشكل أكثر تعقيداً وتوحيد التشريعات المؤثمة لتلك الهجمات بقدر المستطاع وزيادة حدود اتفاقيات تبادل المجرمين وغيرها من الإجراءات والتدابير الاحترازية التي سوف نعرضها بشيء من التفصيل كالآتي:

الفرع الأول: دور الاتفاقيات والمنظمات الدولية والإقليمية في مواجهة جرائم الإرهاب السيبراني الدولي

- **اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام 2001:**

بعد معاناة الدول في المجتمع الدولي من أذى ودمار وخسارة نتيجة لتعرضها للإرهاب السيبراني وحرصاً على مصالح المواطنين في كافة الدول فقد تقدمت في العاصمة المجرية بودابست اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر وتبادل الاطراف في جهة النظر والمناقشة حتى تم إعداد مسودتها النهائية التي تم اقرارها في 2001/11/23 والمعروفة باتفاقية الجرائم الإلكترونية أو السيبرانية.

وقد قامت 26 دولة أوروبية بالتوقيع على تلك الاتفاقية بالإضافة إلى كندا وأمريكا وجنوب افريقيا واليابان وبالرغم من أنها اتفاقية ذات صبغة أوروبية الا أنها ذات طابع عالمي

لكونها مفتوحة لكافة الدول التي تريد الانضمام حتى من خارج أوروبا مما يجعلها ذات صفة دولية بلا مراء في ذلك.

وتُعدّ من أول وأهم المعاهدات الدولية الخاصة بمكافحة الجرائم السيبرانية وكان من أهم أهدافها بناء سياسات جنائية للدول الأوروبية من أجل محاصرة كافة تلك الجرائم من خلال التنسيق بين تشريعات الدول والتعاون القضائي المشترك بالإضافة إلى تحديد وبيان العقوبات المقررة لتلك الجرائم في التشريعات المحلية والوطنية للدول المشاركة وقام المجلس الأوروبي بالإشراف الكامل على تلك الاتفاقية ودخلت حيز النفاذ في 2004/7/1 وكذا البروتوكول الإضافي الأول لعام 2003 لاتفاقية الجريمة الإلكترونية الخاص بالأفعال التي ترتكب عبر أنظمة الحاسب الآلي والمتعلقة بالتمييز العنصري وأيضاً البروتوكول الإضافي الثاني للاتفاقية بشأن تعزيز آليات التعاون بين الدول والمساعدة المتبادلة وكشف الأدلة لمكافحة هذا النوع من الجرائم السيبرانية.

تصنيف اتفاقية بودابست للجرائم السيبرانية:

لقد نصت تلك الاتفاقية بعد مقدمة استعرضت أهداف الاتفاقية ومرجعيتها السابقة وما تقوم به من تدابير وإجراءات دولية وتعاون دولي إقليمي من أربعة فصول مختلفة فقد نصت الاتفاقية على تسمية وحصر مجموعة من الاعمال الإرهابية عبر الوسائل السيبرانية غير المشروعة وحث كل الدول الأعضاء على تجريمها في تشريعاتها الداخلية، وكذلك راعت تلك الاتفاقية مزيداً من الشمولية بكافة صور وأشكال جرائم تقنية المعلومات بحيث يكون تقسيم وتصنيف تلك الجرائم إلى خمسة أشكال وصور من الجرائم السيبرانية على النحو التالي:

- الوصف الأول هو خاص بمضمون وجوهر جرائم تقنية المعلومات وهي الجرائم الموصوفة بأنها ضد سرية البيانات وسلامتها وإتاحة النظم والبيانات.
- الوصف الثاني وهو خاص ببيان الانتهاكات التي تمارس عبر الحاسوب والتي تتعلق بالمساس بالمصالح القانونية المحمية من قوانين العقوبات المحلية وتضم معها جرائم الغش المعلوماتي والتزوير المعلوماتي.
- الوصف الثالث وهو الجرائم الخاصة بالمضمون والمحتوى الذي يخص النشر غير المشروع أو الانتاج غير المشروع كذلك المادة 9 من الاتفاقية.
- الوصف الرابع وهو خاص بجرائم المعلومات المتعلقة بحقوق الملكية الفكرية.
- الوصف الخامس الأحكام المضافة والخاصة بالشروع أو المساهمة والجزاءات والتدابير والإجراءات الموضوعة طبقاً للمعايير والمقاييس الدولية بالنسبة لمسؤولية الأشخاص المعنوية (الأشخاص الاعتبارية) كالمؤسسات والشركات.

وتأسيساً على ما تقدم من أحكام اتفاقية بودابست عام 2001 شرع الإتحاد الأوروبي في إنشاء أجهزة معاونة لتحقيق أهداف وأغراض الاتفاقية لمكافحة هذا النوع من الجرائم منها جهاز آليورو بول والمركز الأوروبي لمكافحة الجريمة المعلوماتية والذي تم افتتاحه في جانفي 2013 لتحقيق هذا الغرض.

ومن الملاحظ أن الاتفاقية قد مضى عليها ما يناهز العشرون عاماً مما جعل البعض يصفها بأنها أصبحت قديمة لظهور أنماط جديدة من التكنولوجيا الرقمية والاتصالات والشبكة العنكبوتية وظهور أنماط حديثة من الإرهاب السيبراني (تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية،2017) ومع ذلك تعد تلك الاتفاقية بداية طيبة وأصلا لكل ما سوف يطرأ من اتفاقيات تواكب حداثة جرائم الإرهاب السيبراني.

وقد أشارت المذكرة الايضاحية لاتفاقية بودابست عام 2001 أن الهدف الأساسي منها وذلك طبقاً للوارد في المواد المادة 2 إلى المادة 13 هو تحسين وإصلاح وسائل وطرق ومنع وقمع الاجرام المعلوماتي وذلك باعتبار بعض التصرفات والإجراءات من قبيل الأفعال المجرمة جنائياً وهو ما يجعل الأمر يسيراً في مكافحة هذا النوع الحديث من الجرائم على المستوى الوطني والدولي في آن واحد (أحمد، 2011) وفي هذا الشأن سوف نعرض بعض مواد هذه الاتفاقية فيما تناولته من صور لجرائم الإرهاب السيبراني والبروتوكول المكمل لها على النحو التالي:

أولاً: الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة:

وهو ما تناولته المادة العاشرة من الاتفاقية بوجوب وحتمية تجريم الانتهاكات العمدية على الملكية الفكرية التي زاد

انتشارها مع زيادة استعمال أجهزة الحاسوب وقد نوهت الاتفاقية في مذكراتها التفسيرية إلى انتهاكات الملكية الفكرية وتحديداً حق المؤلف والتي تعد من أكثر الجرائم انتشاراً على شبكة الإنترنت الأمر الذي قد يضر بأصحاب وحائزي حقوق المؤلف حيث تتم جريمة الإرهاب السيبراني في هذه الحالات بأن يتم إعادة البث والانتاج للأعمال المحمية عبر شبكات الإنترنت دون تصريح أو موافقة المؤلف أو صاحب حق الملكية كل تلك الإجراءات كانت ضرورة ملحة في وضع نصوص تشمل على جزئيات ذات طابع جنائي وفرض تعزيز التعاون الدولي في هذا المجال الهام (الخن، 2011)، وقد انتقد جانب من الفقه هذه المادة لأنها أغفلت الكثير من انتهاكات الملكية الفكرية مثل حقوق وبراءات الاختراع والعلامات التجارية وهو أمر شائع للغاية مما يبعث على خوف الأفراد وانتهاكات حقوقهم الاصلية التي كفلها القانون.

ونحن نرى في هذا الخصوص أن المادة العاشرة وإن كانت تعرضت لانتهاك حقوق الملكية الفكرية دون غيره من حقوق مشابهة كحقوق وبراءات الاختراع إلاّ أن الدول الموقعة على الاتفاقية يمكنها تضمين ذلك في قوانينها الداخلية وجعلها من الوقائع والجرائم ذات الطابع الجنائي دون الحاجة إلى الوقوف على المعنى الضيق لما أوردته المادة العاشرة.

ثانياً: جريمة التزوير المعلوماتي التزوير المتصل بالحاسب الآلي:

وهو ما تناولته المادة السابعة من اتفاقية بودابست من أنه يجب على كل دولة طرف أن تتبنى من الإجراءات التشريعية أو أية إجراءات أخرى بما يكفل التجريم وفقاً للقانون الوطني نية الغش أو نية إجرامية مشابهة لذلك من أجل عمل تقرير غير مصرح به بالبيانات المسجلة والأمن والثقة في البيانات المخزنة وكذلك عمليات الادخال والاتلاف والمحو والطمس تشكل أعمال مماثلة ومشابهة ولها حكم جرائم التزوير حيث أن جرائم التزوير المعلوماتية من الجرائم ذات الخطورة الشديدة بالإضافة لسهولة ارتكابها ولذا طالبت المادة السابقة الدول الأعضاء تضمين نصوص في قوانينها الداخلية لمكافحة ومواجهة جريمة التزوير المعلوماتي باعتبارها موازية لجريمة تزوير المحرر الورقي وذلك بإدخال أو تعديل أو حذف أو اخفاء بيانات الكمبيوتر على نحو يظهر بياناته غير أصلية لتكون مقبولة قانوناً وكأنها بيانات أصلية لم يطرأ عليها أي شكل من أشكال التزوير أو التغيير أو التعديل أو ما شابه ذلك.

ونحن نرى أن المادة السابعة سالفة الذكر قد تكون الحاجة إلى تعميم تجريمها من الاهمية القصوى في كل الدول الأعضاء في الاتفاقية نظراً لأنها قد تضر باقتصاديات الدول ضرراً بالغاً إذا تعمد الجناة في جرائم الإرهاب السيبراني محو أو طمس أو حذف أو إضافة معلومات مغلوطة لمنتجات أو سلع من إنتاج دولة معينة ونسبتها لآخرين لما في ذلك من ضياع أموال طائلة بالإضافة إلى أن الأمر مقصور على اسم أو علامة تجارية أو اسم تجاري لسلعة أو خدمة على أنها أصلية وهي مقلدة فتكون الخسارة من الناحيتين فتكون الخسارة من الناحيتين لأن المستهلك يجهل حقيقة الامور وتصبح نظرية الاثراء بلا سبب موجودة ومتوفرة في تلك الحالات لذا نرى أن إدراج تلك السلوكيات والجرائم الخاصة بالمادة السابعة سالفة الذكر ضمن العقوبات الجنائية قولاً واحداً واجب الاتباع والمراعاة بشكل دقيق.

رابعاً: جريمة الاعتداء على سلامة النظام:

وهو ما تناولته المادة الخامسة من الاتفاقية وهو في مجمله يهدف إلى الولوج وإفساد نظام البيانات المعلوماتية حيث تضمنت أنه يحق على كل طرف من الدول الموقعة على الاتفاقية أن تتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية للتجريم وفقاً للقانون المحلي الداخلي أو الوطني لمكافحة الاعاقة الخطيرة إذا تم ذلك عمداً ودون حق لوظيفة نظام الحاسوب وذلك عن طريق إدخال أو نقل أو اضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية (5، 2001) ويتضح أن تلك المادة تهدف إلى المطالبة بتجريم هذا الاعتداء وهو تخريب الحاسوب الذي يتصل بحياة المواطن أو أمن الدولة أو مؤسساتها ووضع الاعاقة (التعطيل) العمدية للاستخدام الشرعي للنظم المعلوماتية ويشترط لذلك أن يكون حجم الاعاقة جسيما ليصل إلى مرتبة التجريم الجنائي وقد اتجه بعض فقهاء القانون الدولي إلى أن الاعتداء على المؤسسات المالية كالبنوك والبورصة إلى آخره يمثل ارهاباً وتخويفاً للمواطن كما يهدد ممتلكاته ويضعف ثقته في مؤسسات الدولة.

ونحن نرى أن الضرر في حالة تعطيل النظم المعلوماتية لأي دولة عن طريق شبكات الإنترنت لا يقتصر على المالي والاقتصادي فقط إنما يمتد أيضاً إلى سلامة وأمن الدولة والمواطن إذا تم تعطيل مرافق حيوية متصلة بحياة المواطن من مرافق عامة مثل النفط والمياه والكهرباء وهو ما يفوق الضرر الناتج عن الضرر المالي أضعافاً مضاعفة فضلاً عن أن التعطيل قد يوجهه إلى معلومات أمنية وعسكرية لدولة ما فيكون حجم الضرر أكبر وأعظم ولذلك فإننا نرى أن تجريم مثل هذا السلوك يجب أن يكون تجريماً جنائياً أيّاً كان حجم التعطيل للبيانات المعلوماتية وذلك بالنظر إلى جسامة الضرر وليس بساطة الفعل.

خامساً: جريمة الاعتداء على سلامة البيانات:

والمادة الرابعة تطالب أن يكون التجريم أيضاً في حالة تعطيل بيانات الحاسوب وليس البيانات المعلوماتية بشكل عام وهو ما تناولته هذه المادة من الاتفاقية من حيث أنه يجب على كل طرف من الدول الموقعة أن يتبنى من الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية للتجريم وفقاً للقانون المحلي أو القانون الوطني إذا حدث ذلك بشكل عمدي ودون حق أي أضرار أو محو أو تعطيل أو إتلاف أو طمس بيانات الحاسوب (الرابعة، 2001).

وأشارت المذكرة التفسيرية للاتفاقية إلى أن الهدف من تقرير هذا النص هو وضع حماية للبيانات وبرامج الحاسوب مثل تلك الحماية المكفولة للأشياء المادية مثل ممتلكات الأشخاص من أموال وعقارات وسيارات وذلك ضد الأضرار التي قد تحدث عمداً وكذلك المصالح القانونية المحمية لأن التصرفات سابقة الذكر لا يتم العقاب عليها إلاّ إذا تمت بدون وجه حق وهي في حقيقتها تمثل اعتداء على الأشخاص عن طريق الاعتداء على بياناتهم الشخصية التي هي حق خاص مكفول لهم مثل ملكيتهم للأشياء المادية ويشمل ذلك أيضاً حماية البيانات الشخصية لرؤساء الدول بصفتهم المعنوية (أحمد، 2011).

سادساً: جريمة الاعتراض غير القانوني:

والهدف من تلك الحالة في الاتفاقية هو حماية الحق في احترام نقل البيانات والاتصالات وليس مجرد تخزينها أو الاحتفاظ بها فقط وكذلك التسجيل التقليدي للمحادثات الهاتفية بين الأشخاص وهي حالة شائعة جداً في الحياة العامة وهذه الحقوق كانت مكفولة قبل ذلك بنص المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان وهو ما تناولته المادة الثالثة من الاتفاقية حيث تضمنت على أنه يجب على كل طرف أن يتبنى من الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية وذلك بقصد الغش وأن ترتكب في حاسوب آلي يكون متصلاً عن بعد بحاسوب آخر.

سابعاً: جريمة الدخول أو الولوج غير القانوني:

وهو ما تناولته الاتفاقية في مادتها الثانية حيث تضمنت على أنه يجب على كل طرف أن يتخذ من الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقاً للقانون المحلي أو الداخلي وذلك للولوج العمدي لكل أو جزء من جهاز الحاسوب دون حق كما يمكن أن يشترط في ذلك أن ترتكب جريمة في حاسب آلي يكون متصلاً بحاسب آخر عن بعد.

ووفقاً لهذه المادة يدخل في نظام التجريم الجنائي الأفعال الخاصة بالقرصنة (الدسوقي، 2017) والسطو الدخول غير المشروع في النظام المعلوماتي أو أي تعدي على أمن الدولة أو مؤسساتها لانتهاك السرية والسلامة وإتاحة النظم والبيانات المعلوماتية بدون وجه حق (إبراهيم، الجرائم المعلوماتية، 2009).

ثامناً: جريمة إساءة استخدام أجهزة الحاسوب:

وهو ما تناولته المادة السادسة من الاتفاقية على أنه إقرار الإجراءات التشريعية وغيرها من الإجراءات كلما كان ذلك ضرورياً وذلك في إطار تجريم الإنتاج أو البيع أو الحصول بغرض الاستخدام أو التوفير لجهاز يشمل برنامج كمبيوتر حاسب آلي يتم تصميمه أو تطويقه بشكل أساسي لغرض ارتكاب أي من الجرائم المنصوص عليها في إطار المواد الثانية والثالثة والرابعة والخامسة من هذه الاتفاقية وكذلك كلمة السر الخاصة بالكمبيوتر أو الكود السيفري للدخول أو بيانات مماثلة تمكن من الدخول لمنظومة المعلومات بأكملها أو أي جزء بقصد استعمال الجهاز في ارتكاب أيّاً من الجرائم الواردة في المواد سالفة الذكر وكذلك حيازة عنصر من العناصر

المشار إليها بنية استخدامها في ارتكاب الجرائم الإرهابية السيبرانية (مزغيش، 2017) وتعني المادة السابقة بمكافحة ومقاومة أنشطة استخدام أجهزة الحاسوب في ارتكاب أعمال بيع أو شراء وإحالة في ذلك إلى المواد الثانية والثالثة والرابعة والخامسة من نفس الاتفاقية وكذلك السطو وسرقة كلمة السر أو كود الخادوم للدخول بشكل غير مشروع إلى أجهزة الغير أو حتى مجرد حيازة أي من العناصر السابقة فيكون العقاب في ذلك عقاب ذو طبيعة جنائية وهو ما تطالب به هذه المادة الدول الأعضاء الموقعين على الاتفاقية.

تاسعاً: الشروع والاشتراك:

وهذا ما تناولته المادة الحادية عشر من الاتفاقية وهي تتبنى أحكام المساهمة الجنائية وكذلك مرحلة الشروع في ارتكاب الجريمة وإحالة الاتفاقية في ذلك إلى المواد الأولى والثانية حيث طالبت الأعضاء الموقعين باتخاذ إجراءات وتدابير تشريعية لتجريم أفعال المساهمة الجنائية والاتفاقي والتحريض والمساعدة على ارتكاب الجريمة وذلك في الجرائم التي ترتكب بشكل عمدي أو ما تراه الدولة وتختار منها وأيضاً الشروع عمداً في ارتكاب احدى الجرائم المنصوص عليها في المواد السابقة الثالثة والخامسة والسابعة والثامنة والتاسعة من هذه الاتفاقية التي سبق وأن تناولناها بالتفصيل في مجمل البحث (الوهاب، 2017).

واتجه جانب من الفقه إلى أن الاتفاقية راعت النص على الجرائم التكميلية أو غير المكتملة في ارتكاب الجرائم الواردة في المواد إثنين وخمسة وسبعة وثمانية وتسعة ولم تنص عليها الاتفاقية في موادها الأخرى فوجب مراعاة تجريم أفعال الاشتراك الجنائي والشروع في الجريمة لكي تكتمل أغراض الاتفاقية في مكافحة كل أشكال وصور ومراحل الإرهاب السيبراني بكافة صوره.

نحن نرى في هذا الخصوص وتلك المادة أنه كان يمكن للاتفاقية أن تنص صراحة في كل مادة على مطالبة الدول الأعضاء الموقعين على إيراد أو النص على أعمال الاشتراك أو الشروع الجنائي ضمن العقاب المطالب به في القوانين الوطنية المحلية للدول الأعضاء وعدم إفراد مادة منفردة للنص على الشروع والمساهمة الجنائية حتى يضحي الأمر واضحاً لكل الدول الموقعة وينتهي أي خلاف أو جدل أو اختلاف في تفسير بين دولة وأخرى مما قد يجعل من بعض الأفعال أو السلوكيات بمنع عن التجريم خصوصاً وأن مجال تقنين الاتصالات والمعلومات والشبكة العنكبوتية كل يوم في تطور جديد وحديث ومستمر.

عاشراً: الإجراءات والجزاءات:

وهو ما طالبت به المادة 13 من الاتفاقية وهو أن تضمن الدول الأعضاء من خلال إجراءاتها التشريعية عقوبات تتناسب مع درجة خطورة السلوك أو الفعل بما يحقق الردع العام والردع الخاص بحيث يضحى العدول عنها أمراً سائداً وسواء كان العقاب جنائي أو مالي أو سالباً للحرية وبما يتوافق مع سياسة الردع التي تنتهجها كل دولة في سبيل مكافحة عمليات الإرهاب السيبراني (ناجي، الحماية الجنائية لوسائل الاتصال – دراسة مقارنة، 2008).

قد أعقبت الاتفاقية مضموناً مفاده إلزام الدول الأعضاء أو أي دولة تنضم للاتفاقية سواء من المجموعة الأوروبية أو من غيرها بإقرار جملة من العقوبات الملائمة والتدابير الفعالة لجرائم الإرهاب السيبراني أيّاً كان شكل أو طبيعة العقوبة وسواء كانت العقوبة سالبة لحرية الشخص الطبيعي أو حرية الأشخاص المعنوية الأشخاص الاعتبارية (الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجرائم المعلوماتية، 2012).

إشارة إلى البروتوكول الإضافي الأول لاتفاقية بودابست لعام 2001 مجلس أوروبا سلسلة المعاهدات الأوروبية رقم 189 الصادر في عام 2003.

وهو قد عني بشكل أساسي بجرائم الإرهاب السيبراني الدولي بشأن تجريم أي أفعال ذات صبغة عنصرية أو كراهية الأجانب التي يتم ارتكابها عمداً وبدون حق عن طريق أنظمة الحاسوب والأهم في ذلك البروتوكول المكمل ما ورد في المادة السادسة منه وما تناولته من ارتكاب جرائم دولية من الأفعال التي تشكل بحد ذاتها جرائم إبادة جماعية أو جرائم ضد الإنسانية والمتعارف عليها في القانون الدولي وهي تلك القرارات ذاتها الملزمة للمحكمة العسكرية التي تم إنشاؤها بموجب اتفاقية لندن في عام 1945 أو قرارات أي محكمة دولية أخرى تم إنشاؤها بموجب وثائق دولية ذات صلة ويقر باختصاصها ذلك الطرف فإن تلك الجرائم إذا تمت عبر الفضاء السيبراني

تعتبر جرائم إرهاب سيبراني دولي تندرج ضمن الجرائم المذكورة أعلاه (السنباطي، 2009)، وكذلك تناولت المادة السابعة من البروتوكول أن كل دولة طرف تعتمد من التدابير التشريعية ما يلزم لتجريم أفعال المساعدة والتحريض على أي من الجرائم السالف ذكرها في المادة السادسة من هذا البروتوكول إذا ارتكبت بدون حق وعن طريق العمد في قانونها الداخلي.

وأيضاً البروتوكول الإضافي الثاني لاتفاقية بودابست أوضح الجوانب الإجرائية لتعزيز سبل التعاون مع مقدمي الخدمات مع الكيانات الأخرى والمساعدة بين الدول من خلال سلطاتها في إجراءات الضبط والتفتيش والكشف عن الأدلة عبر الحدود في الجرائم ذات الصلة بأنظمة الكمبيوتر (الجرائم السيبرانية)، وكذلك الإجراءات الخاصة بالمساعدة المتبادلة في حالات الطوارئ والتحقيق المشترك وذلك لسهولة الإثبات في هذه الجرائم وضبط مرتكبيها مع تطبيق الشروط والضمانات في القوانين المحلية بما يكفل حقوق الإنسان وحرياته.

- **مساعي وجهود منظمة الأمم المتحدة في مواجهة جرائم الإرهاب السيبراني الدولي:**

حيث تضمن ميثاق الأمم المتحدة بعد الحرب العالمية الثانية بنصه على: بخصوص التهديد أو استعمال القوة ضد السلامة الإقليمية أو الاستقلال السيادي لأي دولة ولا يخفى أن تلك العبارة الواردة في الميثاق لم تتضمن أي نص صراحة على استخدام المعلومات كأداة للإرهاب والترويع والتخويف (الإرهاب السيبراني) إلا أن الميثاق وقد كان الهدف منه أولاً واخيراً مكافحة النزاعات المسلحة في العلاقات بين الدول إلا أنه بمفهوم عمومية اللفظ وعدم التخصيص فإنه يمكن اعتبار مثل هذا النوع من ضمن العدوان المقصود بعمومية اللفظ لأنه يمس العلاقات الدولية وسيادة الدول ويهدد العلاقات الدولية باستعمال القوة (الصادق، 2009) وأن مفهوم القوة هنا ليست القوى العسكرية إنما يمكن إدراج قوة السلاح السيبراني ضمن منظومة القوى الجديدة في العصر الراهن لما تمثله من أضرار قد تفوق وتتجاوز القوة التقليدية وعلى ذلك فإن تلك الجرائم الخاصة بالتقنية المعلوماتية لا تتفق البتة مع مقاصد وميثاق الأمم المتحدة قولاً واحداً (سامر مؤيد عبد اللطيف ونوري رشيد الشافعي، 2016).

هذا وتسعى الأمم المتحدة على نطاق آخر من خلال حقائبها المختلفة والوكالات والبلدان التابعة لها في تعظيم مكافحة الجرائم السيبرانية فيما يتصل بها من أمور متشابكة ومرتبطة بتلك الجرائم مثل مؤتمرات منع الجريمة ومعاملة السجناء (الشكري، 2012)، وكذلك مؤتمرات الجمعيات الدولية لقانون العقوبات الذي يعقد كل خمس سنوات وكذلك المؤتمر السابع الذي عقد في ميلانو بإيطاليا عام 1980، والذي نادى بضرورة الاستفادة من التطور العلمي المتزايد في مواجهة الظواهر الإجرامية المتعلقة بالحاسب الآلي ثم كان المؤتمر التاسع للأمم المتحدة في القاهرة عام 1995 الذي أكد على وجوب حماية مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين الدول في هذا الشأن (الجمعية الدولية لقانون العقوبات جهة استشارية للأمم المتحدة، 1989).

وفي عام 2000 عقدت الأمم المتحدة اتفاقية خاصة لمكافحة إساءة استخدام التكنولوجيا الإجرامية والذي أكد على ضرورة التنسيق والتعاون بين كافة الدول في مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية (اتفاقية، 2000)، وفي عام 2010 نبه مجلس الأمن التابع للأمم المتحدة في القرار رقم 1963 إلى زيادة استخدام الإرهابيين للتكنولوجيا الجديدة وللمعلومات والاتصالات والإنترنت لأغراض التجنيد وهي عناصر جديدة عبر الإنترنت وكذلك التحريض على دعم الأعمال الإرهابية.

ثم كان في عام 2015 القرار رقم 2255 أكثر عمومية لسرد طرق الإرهابيين في استعمال تكنولوجيا الاتصالات والمعلومات خاصة شبكة الإنترنت من أجل تسهيل وتيسير وتنفيذ أعمالهم الإرهابية أو التحريض عليها أو التجنيد لها، وفيما يخص جهود الأمم المتحدة سواء كان في ميثاقها الرئيسي أو هيئاتها أو مؤتمراتها أو توصياتها كان مؤتمر الأمم المتحدة لمنع الجريمة وتحقيق العدالة الجنائية لسنة 2010 في السلفادور بالبرازيل تحت عنوان إستراتيجيات شاملة في تحديات عالمية والذي تم تنظيمه لمنع الجريمة وتحقيق العدالة الجنائية وتطورها في العالم بأسره وقد تضمن جدول أعمال هذا المؤتمر أهم بند خاص بموضوع البحث وهو جرائم الإنترنت والتعاون الدولي في مواجهة ومقاومة ورصد هذه الجريمة باعتبارها أصبحت سائدة بشكل متعاظم (الجنابي،

2017) في المجتمع الدولي في الوقت الراهن، وكذا المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة في دورة عام 2010 بعنوان الأمن السيبراني فرص وتهديدات وتحديات وحذر المشاركون من حرب سيبرانية على مستوى العالم وتنسيق الاستجابة من الأمم المتحدة لتوحيد الأداء والتعاون الدولي لمواجهة هذه الجرائم التي ترتكب عبر الفضاء السيبراني (الدين، 2023).

- **الإتحاد الدولي للاتصالات:**

في عام 1965 وفي باريس تم إنشاء هذه المنظمة تحت اسم التلغراف الدولي ثم تم تعديل الاسم بعد ذلك إلى الاسم المذكور أعلاه وتم الانضمام إلى منظمة الأمم المتحدة وأصبحت تعمل تحت عباءة منظمة الأمم المتحدة وتحت لوائها كإحدى المنظمات المتخصصة وتضم في عضويتها 482 عضواً من كافة الشركات العالمية والدولية والصناعية سواء في القطاع الحكومي أو القطاع الخاص وقد عمدت تلك المنظمة إلى العمل حول الأمن السيبراني الدولي وتم دعوة كافة الدول الأعضاء لوضع إطار قانون للأمن السيبراني الدولي وحماية كافة المعلومات خاصة المتعلقة بالبنية التحتية للدول المشاركة.

ثم جاء عام 2005 ليتم عقد قمة عالمية لمجتمع المعلومات لأجل محاربة الجرائم الخاصة بالإرهاب السيبراني بتونس وطالبت تلك القمة بتنسيق الجهود والآليات في مجال تكنولوجيا الاتصالات عبر إطلاق برنامج الأمن السيبراني العالمي وذلك من أجل إيجاد حلول لدعم الثقة والأمن في المجتمع المعلوماتي والرقمي ونتج عن هذا المقترح جمل من الوثائق التي حصنت عالم المعلومات والشبكة العنكبوتية وكانت خاصة بتسخير تكنولوجيا المعلومات والاتصالات لأغراض تنمية إدارة الإنترنت –الأمن السيبراني– النفاذ الميسر إلى الاتصالات– بناء القدرات– التنوع الثقافي– البنية التحتية.

ولم تكن نهاية المطاف للاتحاد الدولي للاتصالات في عام 2007 نحو توجيه الجهود صوب القارة السمراء أفريقيا وذلك لحث الدول الأفريقية نحو حشد مواردها وامكانياتها المالية والفنية والتقنية من أجل ذلك الهدف وتم رصد مبلغ هائل لذلك الغرض يناهز 55 مليار دولار لصناعة التكنولوجيا والمعلومات الآمنة (محمود م.، 2001).

بل استكمالاً لجهود الإتحاد الدولي للاتصالات فقد تم التوقيع على اتفاقية لإنشاء المركز الإقليمي للأمن السيبراني في المنطقة العربية عام 2012 مع هيئة تقنية المعلومات في سلطنة عمان من ضمن مبادرات الإتحاد ومنظمة إمباكت ومن أهداف المركز التنسيق الإقليمي في مجال الأمن السيبراني وزيادة كفاءته وتحسين البنية التحتية وترتيب الفعاليات والمشاريع في المنطقة ويتبنى المركز إستراتيجية الأمن السيبراني في المنطقة العربية من خلال إنشاء مركز وطني في جميع الدول لمواجهة الجرائم السيبرانية وسن القوانين التي تجرم الاستخدام غير المشروع لتقنية المعلومات وتنمية القدرات وتطوير وزيادة كفاءة الأفراد والمؤسسات في مجال الأمن السيبراني وإلزام الدول بالتعاون الدولي والإقليمي لمواجهة هذا النوع من الجرائم التي تحدث عبر الفضاء السيبراني (الموقع الرسمي للاتحاد الدولي للاتصالات؛ www.it.int/or/action/pages).

المطلب الثاني:

دور القرارات والمؤتمرات والندوات الدولية والإقليمية في مواجهة جريمة الإرهاب السيبراني الدولي

الفرع الأول: قرارات الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية (الإرهاب السيبراني الدولي)

سارعت الأمم المتحدة عبر جمعيتها العامة إلى إصدار جملة قرارات لمواجهة جرائم الإرهاب السيبراني الدولي إيمانا منها بخطورة ذلك النوع المستحدث من الجرائم السيبرانية والمعلوماتية التي تتم من خلال الحاسب الآلي نذكر منها الآتي:

قرار الجمعية العامة للأمم المتحدة رقم 45 121/لسنة 1990: هذا القرار كان البداية الصريحة لتبني آليات مكافحة أضرار جرائم الإرهاب السيبراني الدولي الذي أيد فيه توصيات مؤتمر منظمة الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين والقرار المتعلق بالجرائم ذات الصلة بالحاسوب الذي

أوجب على كافة الدول تكثيف الجهود لمكافحة إساءة استعمال الحاسوب بفاعلية أكبر (الثامن، 1990).

القرار رقم 63/55 عام 2000 والقرار 121/56 لسنة 2001 وذلك بشأن مكافحة سوء استخدام تكنولوجيا المعلومات: وفي هذا الشأن فقد أوصى القرار الأول بأن تضمن الدول في قوانينها الداخلية وممارساتها عدم توفير أي ملاذٍ امن لكل من يسيء استخدام تكنولوجيا المعلومات وكذلك العمل على حماية سرية المعلومات والبيانات وسلامة أنظمة الحاسوب ضد أي اعتداء غير مشروع مع وضع عقوبة مناسبة لذلك.

ودعا القرار رقم 121/56 كافة الدول الأعضاء أن تأخذ في الاعتبار أعمال لجنة منع الجريمة والعدالة الجنائية عند وضع التشريعات الخاصة بمكافحة جرائم الإرهاب السيبراني الدولي.

وفي عام 2002 أصدرت الأمم المتحدة القرار رقم 239/57 والخاص بإرساء ثقافة دولية وعالمية للأمن السيبراني بهدف دعم الجهود الوطنية لتبادل المعلومات والتعاون في هذا الشأن على نطاق وطني وإقليمي ودولي كما أكد هذا القرار أن الأمن السيبراني من الحقوق الأساسية الحيوية للمعلومات وهو مسؤولية تقع على عاتق حكومات الدول بالتنسيق مع اصحاب المصلحة ذوي الشأن.

وفي عام 2005 صدر القرار رقم60/177 عن الأمم المتحدة والخاص بتشجيع ودعم التعاون الدولي في مجال مكافحة الجرائم السيبرانية وتقديم المساعدة بكافة أشكالها للأعضاء في هذا المجال.

وفي عام 2004 سارعت الأمم المتحدة عبر جمعيتها العامة بإنشاء مجموعة تضم مجموعة من الخبراء الحكوميين وذلك من أجل دراسة ووضع تصور لتأثير تطورات تكنولوجيا الاتصالات والمعلومات على الأمن القومي للدول وكذلك وضع توصيات للفريق في اجتماعه السنوي من أجل ذلك الهدف.

وفي عام 2010 صدر القرار رقم 64/211 عن الأمم المتحدة كذلك دعا كافة الدول إلى تحديث قوانينها الداخلية في مجال مكافحة الجرائم السيبرانية وخصوصية البيانات والسرية والشخصية والتجارية وكذلك التوقيع الإلكتروني ودعا القرار أيضاً إلى اعتماد اتفاقيات إقليمية في هذا الشأن (SCHJIBERG., 2008).

ثم كان عام 2010 حينما قدم مجموعة الخبراء تقريراً أشاروا من خلاله إلى التهديدات التي تثيرها عمليات الإرهاب السيبرانية والأمن السيبراني من تهديد للسلم والأمن الدوليين وضرورة إيجاد توجه دولي موحد بما يتفادى الأضرار الجسيمة لتلك السلوكيات غير المشروعة في الفضاء السيبراني.

توصيات الفريق ذوي الخبرة المكلف بملف الأمن السيبراني:

انتهى ذلك الفريق المكلف من الجمعيات العامة للأمم المتحدة إلى عدة توصيات أهمها:

- ضرورة تبادل المعلومات بشأن التشريعات والمعلومات الوطنية وتقنيات وسياسات نظم أمن الاتصال وأفضل الممارسات في هذا الشأن.
- ضرورة تحقيق تدابير وإجراءات بناء الثقة في مجال الحد من مخاطر استخدام الدول لتكنولوجيا الاتصالات والمعلومات.
- أهمية مواصلة الحوار والخبرات بين الدول لمناقشة كافة المعايير الخاصة باستخدام تكنولوجيا المعلومات والاتصالات للحد من مخاطرها وأضرارها وكذلك حماية البنية التحتية للدول.
- وضع وتحديد تدابير لدعم القدرات في الدول النامية والأقل نمواً.

وصدر القرار 41/65 لسنة 2011 والذي صدقت عليه الجمعية العامة للأمم المتحدة وتلك المصادقة على تقرير فريق الخبراء الحكوميين والخاص بمجال المعلومات والاتصالات السلكية واللاسلكية المرتبطة بالأمن الدولي محذراً في هذا التقرير من عواقب الحروب السيبرانية الكارثية مثل التشويش على نظم الملاحة الجوية والبحرية أو قطع إمدادات الغاز أو الكهرباء على السكان المدنيين وأهمية مراعاة كل الأطراف الدولية في نزاعاتها المسلحة باحترام قواعد القانون الدولي الإنساني إذا مارست أيّاً من وسائل الحرب السيبرانية.

وكذلك تم تشكيل الفريق الثالث من الخبراء في عام 2012، ولم يتوصل إلى أي مبادئ خاصة بالسلوك السيبراني.

ويعد تقرير الخبراء الصادر في عام 2014 من أبرز ما توصل اليه التقرير هو أن القانون الدولي ينطبق على الفضاء

السيبراني وتحمل المسؤولية للدول التي يثبت قيامها بهذا الفعل.

وفي عام 2019 أنشأت الجمعية العامة فريقاً مكون من خبراء من خمسة وعشرون دولة وصدر تقريره النهائي عام2021 الذي تضمن معايير السلوك المقبول في الفضاء السيبراني (عبد الحمزة، 2022).

وفي عام 2015 قدمت مجموعة (g g a) التابعة للأمم المتحدة تقريراً تضمن عدة توصيات هامة للغاية منها:

– ضرورة تطبيق القانون الدولي على الفضاء السيبراني.

– عدم استهداف البنية التحتية للدول واعتبار أي دولة مسؤولة بشكل مباشر عن أي هجمات سيبرانية تنطلق من أراضيها، وأشار ذلك التقرير إلى أن تلك التوصيات هي غير ملزمة وهي توعية للدول ولكنها خطوة في طريقة تطوير إطار معياري يتم الاتفاق عليه بين الدول (عسكر، وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسات التجسّس وقت السلم، 2021).

ونحن نرى أن نهاية التقرير الصادر عام 2015 من مجموعة (g g a) التابعة للأمم المتحدة وإن كان متفقاً مع آراء وتصور مجموعة الخبراء الحكوميين المعنيين بالأمن السيبراني إلا أن افتقاد وخلو التوصيات من عنصر الإلزام وجعله اختيارياً وطواعية للدول يخرج الأمر من مقتضاه لأن عنصر الإلزام هو ما يسبغ القوة للقرار أو التوصية أو القاعدة القانونية ولذا فإنها وإن كانت من قبيل التوصيات فكان ينبغي وضع تدابير وإجراءات وعقوبات للدول المخالفة والتي لا تلتزم بما جاء بتلك التوصيات باعتبارها ضمير العالم الناطق بما فيه خير للدول والمجتمعات والأفراد لأن عواقب سوء استخدام الأمن السيبراني والجرائم الخاصة بالإرهاب السيبراني الدولي تمس البشرية بأكملها وليست حكراً على مجتمع بعينه أو دولة بذاتها خاصة مع اختلاف الرؤى بين الدول وتضارب المصالح فيما يمكن اعتباره اعتداء سيبراني من عدمه فكان الأولى وضع نص موحد وعام وجامع ومانع ومجرداً لما يمكن اعتباره سلوكاً غير مشروع من ممارسات أمن المعلومات والتكنولوجيا الخاصة بالاتصالات وجرائم الأمن السيبراني وتطبق على أي دولة تخالف ذلك قولاً واحداً مع ضمان أن يكون الأمر فيه قدر من الإلزام ولو حتى التلويح بعقوبات اقتصادية على الدول المخالفة لذلك أو أي نوع من أنواع العقوبات يتفق عليها المجتمع الدولي في هذا الصدد لضمان الالتزام من الدول وجدية التنفيذ.

الفرع الثاني: جهود المؤتمرات والملتقيات والندوات الدولية والإقليمية في مواجهة جرائم الإرهاب السيبراني الدولي

- **المؤتمر الدولي السابع للطب الشرعي الرقمي والجرائم السيبرانية (سيول كوريا الجنوبية):**

وعقد في عام 2015 وكانت محاور ذلك المؤتمر خاصة بكشف هذا النوع من الجرائم من خلال الطب الشرعي الرقمي ودوره في مساعدة جهات التحقيق في جرائم الإرهاب السيبراني وكشف الأدلة لإنفاذ القانون وتأكيد المعلومات وكانت أهم محاور هذا المؤتمر أيضاً تخصصات هامة مثل علم الكمبيوتر– القانون تحليل البيانات– التمويل– الأجهزة الشرطية وكان المؤتمر يجمع بين الباحثين في هذا المجال وأيضاً المستخدمين لتلك الأجهزة.

- **مؤتمر الرياض حول مكافحة جرائم الإنترنت 2015:**

عقد هذا المؤتمر بالمملكة العربية السعودية بالعاصمة الرياض بهدف بيان ورفع مستويات مكافحة الجرائم المعلوماتية والاستفادة من التجارب المحلية والدولية والإقليمية في هذا الشأن في مجال الحاسوب والإنترنت واشتمل جدول أعمال هذا المؤتمر على بيان الأسباب والآثار والاتجاهات الحديثة لمكافحة تلك الجرائم وكذلك رفع درجة الوعي العام بأثرها وعواقبها وحماية البنية التحتية من أخطار تلك الجرائم وكذلك طرح وبحث سبل مواجهتها عن طريق الأمن السيبراني (مكافحة جرائم الإنترنت، 204).

- **مؤتمر نيويورك 2015 للأمن السيبراني الدولي الخامس لإنفاذ القانون والصناعة والخبراء الأكاديميين:**

بمشاركة من جامعة فوردهام الأمريكية وكذلك بوجود ممثلين عن وكالة التحقيقات الفيدرالية الأمريكية وعدد كبير من أصحاب المناصب الهامة والقيادية عالمياً في مجال إيجاد وبحث وتحليل جرائم الإرهاب السيبراني وذلك رغبة في توحيد كافة الجهود الدولية من أجل إيجاد وتوفير قدر من الأمن في مجال عالم تقنية المعلومات والإنترنت والفضاء السيبراني

بشكل عام (القحطاني م.، 2016)، وهو ما يعكس رغبة الولايات المتحدة في مكافحة مثل هذا النوع من الجرائم المستحدثة على الساحة الدولية والعالمية والإقليمية.

- **مؤتمر أبو ظبي لتجريم الإرهاب السيبراني في عام 2017:**

كانت من أهداف هذا المؤتمر الذي عقد على أرض دولة الإمارات العربية تعزيز التعاون الدولي في حل المشاكل والتحديات التي قد تواجه الفاعلين والسلطات التشريعية ذات الاختصاص الحكومي وكذلك المنظمات الدولية وانتهى المؤتمر إلى عدة توصيات في مجال مكافحة جرائم الإرهاب السيبراني (الرياض، 2017) منها:

أولاً: إنشاء هيئة وطنية خاصة بالمعلومات والحريات والأمن السيبراني مهمتها وضع سياسات وإستراتيجيات تتوافق مع القانون لرصد ومقاومة المحتوى الرقمي الذي قد يشمل مخاطر إرهابية أو ينطوي على ذلك.

ثانياً: تحرك موحد ومنسق ومتسارع بين كل الدول لتبني كافة القرارات والتوصيات الصادرة عن مجلس الأمن والجمعية العامة للأمم المتحدة وكذلك المنظمات الإقليمية كجامعة الدول العربية وذلك فيما يخص مكافحة المخاطر والتهديدات الخاصة بالإرهاب السيبراني الدولي.

ثالثاً: تجريم كافة لجان التنسيق بين الجماعات الإرهابية التي تهدف إلى تبادل المعلومات أو التخطيط لتنفيذ جرائم إرهابية أو نشر خطابات تدعو للتطرف وكذلك التحريض على ارتكاب أعمال إرهابية أو بث خطابات عبر الإنترنت تدعو للكراهية أو التمييز أو العنف سواء على أساس ديني أو عرقي أو طائفي أو سياسي.

رابعاً: دعوة الدول الأعضاء إلى وضع مقتضيات هذا الاتفاق وتبني مبادئه في قوانينها الداخلية ووضع العقوبة الملائمة له في كل ما يتعلق بجرائم الإرهاب السيبراني سواء كانت عقوبة سالبة للحرية أو عقوبة مالية أو كلاهما معاً.

- **مؤتمر مسقط عام 2014 للأمن السيبراني:**

وهو المؤتمر الإقليمي الثالث للأمن السيبراني الذي استضافته سلطنة عمان بالتعاون مع الإتحاد الدولي للاتصالات في عام 2014 وناقش المؤتمر كافة سبل تأمين وحماية البنية التحتية الحساسة للمعلومات الوطنية وقد بلغ عدد المشاركين في هذا المؤتمر حوالي 250 متخصصاً في مجال تكنولوجيا المعلومات والاتصالات و28 متحدثاً في هذا المؤتمر وتمت مناقشة وطرح وصياغة التوجيهات المشتركة وخطط المواجهة للتهديدات الناشئة للقطاع العالمي والإقليمي في سبيل الوصول إلى رؤية مشتركة لسبل مواجهة جرائم الإرهاب السيبراني (مؤتمر مسقط الإقليمي الثالث للأمن السيبراني، 2014) وتستعد في الوقت الراهن مدينة مسقط باستضافة الحدث الإقليمي الأكبر وهو الاسبوع الإقليمي للأمن السيبراني من 28–31 اكتوبر القادم 2024.

- **ملتقى تقنية المعلومات الثالث بالبحرين عام 2009:**

ومن خلال هذا المؤتمر تم بحث كيفية حماية الشبكة المعلوماتية من كافة صور الإرهاب السيبراني (ملتقى تقنية المعلومات لية تقنية المعلومات جامعة البحرين، 2024) خاصة فيما يتعلق بسرعة المعلومات أو درجة أهميتها والإجراءات المتخذة من جانب الحكومة وكذا مناقشة الأزمات والكوارث السيبرانية والتقنيات المتبعة على المستوى الدولي.

- **ملتقى مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية 2009:**

حيث اتفق الحضور على ضرورة مناقشة كافة أنواع الجرائم المعلوماتية من كافة نواحيها سواء الأمنية أو الاجتماعية أو الاقتصادية أو الإستراتيجية وكذلك انتحال الشخصيات وجرائم الابتزاز الخاصة بالمرأة ووصفها بأكثر الصور سلبية على التقاليد الاجتماعية العربية (http://www.sharjah.ac.ae.com).

- **الملتقى الدولي الخامس في سوريا لأمن المعلومات لعام 2009:**

وقد أنتهى هذا المؤتمر إلى عدة توصيات نذكر منها:

- مطالبة قطاع التعليم القيام بالبحث العلمي في مجال أمن المعلومات والأمن السيبراني.
- إسراع السلطات المختصة بإصدار ما يلزم من تشريعات لمكافحة جرائم الإرهاب السيبراني الدولي.

- التوعية الدائمة بأهمية نظم أمن المعلومات وتبني سياسة أمنية مناسبة لمكافحة مثل هذا النوع من الجرائم.
- ضرورة نشر الوعي الكاف لدى المواطنين حول مفهوم التوقيع السيبراني وأهميته، وكذا قرار السيد رئيس مجلس الوزراء رقم12 لعام 2024 والمتضمن التعليمات التنفيذية لقانون حماية البيانات الشخصية (القرار رقم 12 لعام 2024 على الموقع الإلكتروني للموقع الرسمي لوزارة الاتصالات، 2024).

ونحن نرى أنه وإن كنّا نثمن كل المؤتمرات والندوات والفعاليات التي عقدت على المستوى الدولي والإقليمي الا أنها تأخرت بعد الوقت في مواجهة هذا التحدي الجديد الخطير وهي بطبيعتها توصيات لا ترقى لدرجة الإلزام للدول المشاركة بها وانما ذات قيمة أدبية للدول وكنا نأمل أن يكون هناك منظمات دولية وإقليمية تصدر نفس القرارات الملزمة للدول كافة بحيث يغدو الخروج عليها مسؤولية دولية تضع مخالفيها موضع المساءلة والحساب والعقاب في القانون الدولي العام.

المبحث الثاني:
النماذج التطبيقية لجرائم الإرهاب السيبراني الدولي والجهود الوطنية في مواجهتها

المطلب الأول:
نماذج لبعض الجهود الوطنية في مواجهة جرائم الإرهاب السيبراني الدولي
(الموقف المصري في مواجهة جرائم الإرهاب السيبراني الدولي)

الفرع الأول: دور الحكومة المصرية في مواجهة جرائم الإرهاب السيبراني الدولي

شهدت مصر حراكاً قوياً في مكافحة الجرائم السيبرانية حيث كانت من أولى الدول التي أعلنت انضمامها للاتفاقيات العربية لمكافحة تلك الجرائم والإرهاب السيبراني وفي خطوة لاحقة أعلنت مصر عن إنشاء المجلس الأعلى للأمن السيبراني للحيلولة من آثار ممارسات اختراق أمن المعلومات على الأمن القومي المصري وتأمين كافة الخدمات السيبرانية بشكل فعال من مخاطر استهداف البنية التحتية للدولة، ومن مظاهر اهتمامات مصر بقضايا الأمن السيبراني خلال السنوات الماضية الآتي:

في عام 2009 أنشأت وزارة الاتصالات المركز المصري للاستجابة لطوارئ الإنترنت والحاسب الآلي لإتاحة خدمة الرصد والاستجابة للحوادث على مدار 24 ساعة يومياً جميع أيام الأسبوع. وعقد مؤتمر القاهرة للجريمة السيبرانية والتنمية الاقتصادية لتحديد مفهوم جريمة الإرهاب السيبراني وبياناتها وانتهى لضرورة وضع تشريعات داخلية تعاقب مرتكبي هذه الجرائم (العريان، 2011).

وفي عام 2012 شاركت في التدريبات السيبرانية العملية التي نظمها فريق الاستجابة لطوارئ الحاسوب بآسيا والمحيط الهادي، وفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي، والإتحاد الدولي للاتصالات، كما اتفقت مصر على التعاون المشترك مع فريق الطوارئ للحاسوب بالولايات المتحدة، ووكالة أمن الإنترنت الكورية في مدينة سيول، والهيئة الماليزية للأمن السيبراني كما نظمت البعثات الخاصة إلى فنلندا واستونيا لاستكشاف سبل وآليات التعاون لمواجهة الجرائم السيبرانية عبر فرق الاستجابة لطوارئ الحاسوب وفى مجال التوقيع الإلكتروني، وعرض إستراتيجية الأمن السيبراني المصري في إحدى الجلسات الرئيسية لمنتدى حوكمة الإنترنت في أذربيجان، وأيضاً شاركت مصر في مؤتمر بودابست للفضاء الإلكتروني في المجر، وأخيراً بداية التشغيل لخدمة اختبار الاختراق (فوزي، 2019).

وفي عام 2013 حصل المركز على عضوية اللجنة التوجيهية لفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامي واحتل المركز الثالث حسب تقييم الأمن السيبراني العالمي للاتحاد الدولي للاتصالات ونظم الجهاز القومي لتنظيم الاتصالات ورشة العمل الأولى للأمن السيبراني ومواجهة الجرائم السيبرانية بالقرية الذكية، لبحث ودراسة وتحليل التطورات في مجال الأمن السيبراني في شتى المجالات وتم تشكيل اللجنة الوطنية لحماية الطفل على الإنترنت وفي عام 2014، احتلت مصر المركز 27 من بين 193 دولة وفقاً لما جاء في مؤشر قياس استعدادات الدول

في مجال الأمن السيبراني الصادر عن الإتحاد الدولي للاتصالات وشركة ABI (الموقع الرسمي لوزارة الاتصالات المصرية، 2024).

وفي عام 2015 أطلقت مصر إستراتيجية جديدة موحدة في مجال الأمن السيبراني بعنوان الأمن السيبراني آفاق وتحديات وذلك من خلال المؤتمر السنوي لتطوير الصناعة وتناولت تلك الإستراتيجية طرق وسبل تأمين الشبكات الخاصة بالبنية التحتية وكذلك تطبيقات التحكم الصناعية وتأمين الخدمات السيبرانية (محمود ا.، 2020).

وفي عام 2016 قامت مصر بعقد المؤتمر الإقليمي الخامس للأمن السيبراني بمدينة شرم الشيخ وأشرف على تنظيمه المركز العربي الإقليمي للأمن السيبراني تحت عنوان تعاون بلا حدود من أجل تعزيز كافة الجهود الإقليمية في المنطقة العربية في هذا الشأن، وكذلك استضافت مصر منتدى فرست الإقليمي للمنطقة العربية والإفريقية من أجل تبادل الخبرات والتعاون مع المنظمات الدولية ذات الصلة لمواجهة خطر النشاط السيبراني.

وفي عام 2017 أصدر الإتحاد الدولي للاتصالات تقرير مؤشر قياس استعداد الدول في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية لتعزيز الجهود على نطاق دولي، فقد جاءت مصر في المركز الرابع عشر عالمياً من أصل ١٩٣ دولة، كما جاءت في المركز الثاني عربياً فيما يتعلّق بمستويات الالتزام بالأمن السيبراني بعد سلطنة عمان التي جاءت في المركز الرابع عالمياً والأول عربياً كما ورد التقرير مؤكداً على أن مصر كرست كل ما تملك من جهود للاستعداد التام والكامل لمواجهة الهجمات السيبرانية وتحقيق الأمن السيبراني من خلال هيكلة بنية تحتية للمؤسسات وتبنيها استراتيجيات وطنية، وأبرمت اتفاقيات عديدة لتبادل الخبرات الفنية والعملية ونشر ثقافة الوعى بالأمن السيبراني من خلال تبنيها سياسات وطنبة، وكذلك أقامت المبادرات والملتقيات والمنتديات وعقدت مؤتمرات وأبرمت اتفاقات دولية وإقليمية في مجال الأمن السيبراني، وقد تخطت مصر بذلك أزمات الثقة التي تهدد انتشار ثقافةً الأمن السيبراني محلياً وعالمياً من خلال خمسة معايير حددها مؤشّر قياس ITU هي: (التقنية – التنظيمية – القانونية – التعاون – إمكانات النمو).

وفي عام 2017 وقعت مصر على اتفاقية التعاون والشراكة بين المعهد القومي للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيكو العالمية وذلك لإطلاق أول أكاديمية مصرية للأمن السيبراني بهدف تثقيف وتطبيق كافة المهارات اللازمة لمواجهة تحديات الأمن السيبراني وشاركت في مؤتمر المنطقة المركزية للاتصالات بالعاصمة واشنطن عن سبل الاستجابة للحوادث التي تهدد الأمن السيبراني، وشاركت مصر في المنتدى الإقليمي للاتحاد الدولي للاتصالات ومنظمة فرست، وورشة عمل لتقييم الجاهزية للاستجابة للطوارئ المعلوماتية للمنطقة العربية والأفريقية، وشاركت مصر في المؤتمر الإقليمي السادس للأمن السيبراني بعمان والذى نظمه الإتحاد الدولي للاتصالات.

وفي عام 2018 صدر القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات والذي أشار في المادة الرابعة إلى التعاون بين السلطات المصرية والدول الأجنبية بناء على مبدأ المعاملة بالمثل في ضوء الاتفاقيات والمعاهدات الدولية والإقليمية والثنائية أيضاً التي تم التصديق عليها لتبادل المعلومات والمساعدة في إجراءات التحقيق وضبط مرتكبي هذه الجرائم للحد منها (المصري، 2018)، وشاركت مصر في مؤتمر اختراقات الأمن السيبراني ومؤتمر قمة إفريقيا للدفاع السيبراني، وكذلك مؤتمر اجتماع لجنة الدراسات ١٧ التابعة للاتحاد الدولي للاتصالات والمؤتمر الإقليمي السابع للأمن السيبراني وكذلك نظم مركز المعلومات ودعم القرار بمجلس الوزراء حلقة نقاشية بعنوان: الأمن السيبراني وحماية الهوية المصرية في البيئة الرقمية الحديثة وكذلك أطلق المجلس الأعلى للأمن السيبراني الإستراتيجية الوطنية للأمن السيبراني (2017–2021).

وفي 2019 نظمت ماستر كارد أول منتدى حول الأمن السيبراني في القاهرة وكذلك قامت غرفة تكنولوجيا المعلومات والاتصالات بتنظيم المؤتمر السنوي الخامس للأمن السيبراني (فوزي، 2019).

وفي عام 2023 تم إصدار الإستراتيجية الوطنية للأمن السيبراني (2023–2027) وتتجلى أهمية هذه الإستراتيجية في نقطتين رئيسيتين وهما:

- التصدي ومكافحة الجرائم السيبرانية المتزايدة والمستمرة بشكل مطرد من حيث أهدافها ومنبعها ومصدرها.
- تزويد السوق المصرية عن طريق بناء القدرات المتمثل في الكوادر البشرية وتنمية الصناعات المحلية مما يزيد من الناتج القومي للبلاد.

وهناك هدف أسمى من هذه الإستراتيجية ألا وهو تقييم حالة الأمن السيبراني في مصر في هذه الفترة والوقوف على مدى مواجهته للحوادث السيبرانية بكافة صورها وأشكالها.

وتضمنت الإستراتيجية أن تزايد الهجمات السيبرانية نتيجة لتعدد مصادرها ومنها الجرائم السيبرانية والحرب السيبرانية والارهاب السيبراني ومن التحديات الأساسية للأمن السيبراني عدم مواكبة البحث العلمي في هذا المجال مما يحتاج إلى بناء بنية تحتية للبحث العلمي فيه ودمج برامج الامن السيبراني في مراحل التعليم المختلفة وكذلك أقرت العديد من الوسائل لتطوير الإستراتيجية منها تجارب الدول الرائدة والبحث العلمي والاستعانة بالخبراء الأكاديميين في هذا المجال، والنص صراحة على إنشاء إطار تشريعي كامل قائم على تجريم هذه الجرائم وما المسؤولية التي تقع عل مرتكبيها من خلال قانون 175 لسنة 2018 وفرض المعايير والضوابط لحماية البيانات والمعلومات من خلال قانون حماية البيانات الشخصية رقم 151 لسنة 2020 ومحاولة الوصول لتشريع قانون خاص بالأمن السيبراني وسوف نتناول ذلك بالتفصيل في موقف المشرع المصري لاحقاً، وأيضاً تضمنت التعاون بين الجهات الحكومية ومؤسسات القطاع الخاص والخبراء في تنفيذ الإستراتيجية لتعزيز الشراكة الوطنية في المشروعات الوطنية والبنية التحتية الحرجة وبرامج للقطاع الخاص وغيرها من سبل التعاون وأيضاً برامج توعوية تثقيفية وبرامج تدريب متخصصة وبرامج إعلامية لتوعية المواطنين في مجال الأمن السيبراني وكذلك الحث على البحث العلمي والابتكار (السيبراني، 2023).

الفرع الثاني: موقف المشرع المصري من الجرائم السيبرانية

تناول الدستور المصري لعام 2014 في مواده بعض الأحكام والمواد الخاصة بالأمن السيبراني وأمن المعلومات حيث تناولت المادة 31 من هذا الدستور على أن أمن الفضاء السيبراني المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه وعلى النحو الذي ينظمه القانون وكذا ما تناولته أيضاً المادة 57 منه على عدم المساس بحرمة الحياة الخاصة من المراسلات البريدية والإلكترونية والمحادثات الهاتفية وكفالة سريتها ولا يجور مراقبتها أو الاطلاع عليها أو مصادرتها إلا بإذن قضائي محدد المدة ومسبب، ولا يجوز تعطيل أو حرمان المواطنين منها أو تعطيلها تعسفياً.

وكذلك تناول المشرع المصري في القانون رقم 94 لسنة 2015 لمكافحة الإرهاب الذي استمد أحكامه من قرارات مجلس الأمن والاتفاقيات الدولية والإقليمية تجريم الإرهاب بكافة صوره ومنها الإرهاب الرقمي أو الإلكتروني ومنها المادة الأولى الخاصة بالأصول المادية والافتراضية وعائداتها أيّاً كان شكلها بما فيها الرقمية أو الإلكترونية والائتمان المصرفي بكافة صوره، وفي المادة الثالثة جرمت مصادر تمويل الإرهاب الرقمية أو الإلكترونية، وعاقب القانون بالسجن المؤبد أو المشدد الذي لا تقل مدته عن عشر سنين في مادته الخامسة عشر كل من قام بارتكاب جريمة إرهابية عن طريق الوسائل السلكية أو اللاسلكية أو الإلكترونية، وكذلك بالسجن المشدد مدة لا تقل عن خمس سنين لمن أنشأ أو استخدم موقعا إلكترونياً بغرض الترويج للأفكار والمعتقدات الإرهابية والعقوبة بمدة لا تقل عن عشر سنوات لكل من دخل بغير حق أو بطريقة غير مشروعة موقعا إلكترونياً تابعاً لأية جهة حكومية للحصول على البيانات أو المعلومات الموجودة عليها أو محوها أو إتلافها أو تزوير محتواها ونحن نرى أن هذا القانون قد واجه بشكل كبير جرائم الإرهاب بكافة صوره ومنها الإرهاب السيبراني.

كما أصدر المشرع المصري القانون رقم 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات والذي تناول في الباب الأول منه الأحكام العامة من تعريفات والتزامات وواجبات مقدمي الخدمة ونطاق تطبيق القانون من حيث المكان وكذلك التعاون الدولي لمكافحة هذه الجرائم، وتناول في الباب الثاني منه الأحكام والقواعد الإجرائية الخاصة بمأموري الضبط القضائي في هذه الجرائم والأوامر القضائية المؤقتة

والإجراءات والقرارات التي تصدر لحجب المواقع والتظلم من هذه القرارات والمنع من السفر والاستعانة بالخبراء والفنيين وحجية الأدلة الرقمية في الإثبات، وكذلك تناول في الباب الثالث الجرائم وعقوباتها في فصله الأول مثل جرائم الاعتداء على سلامة شبكات وأنظمة المعلومات مثل جريمة الانتفاع بدون وجه حق بخدمات الاتصالات وتقنياتها والدخول غير المشروع وتجاوز الحق في الدخول والاعتراض غير المشروع والاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية والاعتداء على البريد الإلكتروني والاعتداء على تصميم موقع والاعتداء على الأنظمة المعلوماتية الخاصة بالدولة والاعتداء على سلامة الشبكة المعلوماتية واستخدام البرامج والأجهزة والمعدات المستخدمة في هذه الجرائم، وفي فصله الثاني الجرائم التي ترتكب بواسطة أنظمة وتقنية المعلومات مثل جرائم الاحتيال والاعتداء على بطاقات البنوك وأدوات الدفع الإلكتروني والمتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني، وفي فصله الثالث الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع، وفي فصله الرابع الجرائم التي ترتكب بواسطة مدير الموقع، وفي فصله الخامس أحكام المسؤولية الجنائية لمقدمي الخدمات، وفي فصله السادس الظروف المشددة للجريمة، وفي فصله السابع المسؤولية الجنائية للأشخاص الاعتبارية، وفي فصله الثامن العقوبات التبعية، وفي فصله التاسع الشروع وأحكام الإعفاء من العقوبة، وأخيراً في الباب الرابع الأحكام الانتقالية والختامية وتنوعت العقوبات حسب كل صورة من صور الجرائم ما بين الحبس بحد أدني شهر وحد أقصى خمس سنوات أو الغرامة بحد أدنى عشرة آلاف جنيها وحد أقصى خمسة ملايين جنيها أو كليهما أو السجن المشدد في حالة إذا ما كانت الجريمة تخل بالنظام العام والأمن القومي وسلامة المجتمع (المصري، 2018).

وكذلك التشريع رقم 15 لسنة 2004 المتعلق بالتوقيع الإلكتروني الذي جرم التزوير الإلكتروني بكافة صوره للمحررات الإلكترونية واستعمالها وإتلافها أو تعديلها، وأيضاً عدة قوانين مثل قانون العقوبات كحماية الحق في الحياة الخاصة، وقانون تنظيم الاتصالات رقم 10 لسنة 2003 الذي جرم تعطيل شبكات الاتصالات وإحداث الضرر بها والتصنت على الاتصالات وذلك من أجل سلامة وأمن نظم وشبكات الاتصالات (عسكر، وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسة التجسّس وقت السلم، 2021).

وكذلك أصدر المشرع المصري القانون رقم 151 لسنة 2020 والمحدث حتى عام 2023 في شأن حماية البيانات الشخصية المعالجة إلكترونياً جزئياً أو كلياً لدى أي حائز أو متحكم أو معالج لها لهذه البيانات الخاصة بالأشخاص الاعتباريين.

وتسري أحكام هذا القانون على كل من ارتكب إحدى هذه الجرائم المنصوص عليها في القانون المرافق في حالة إذا كان الجاني من المصريين داخل الجمهورية أو خارجها أو من غير المسلمين والمقيمين داخل جمهورية مصر العربية أو غير المسلمين خارجها إذا كان هذا الفعل معاقب عليه وحدد في المادة الثالثة الحالات التي لا تسري فيها احكام القانون ومنها البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والبيانات الشخصية التي تم معالجتها حصراً للأغراض الاعلامية وكذلك البيانات الشخصية التي تخص جهات الأمن القومي وما تقدره لاعتبارات اخرى وكذلك البيانات الشخصية لدى البنك المركزي المصري والجهاز المصرفي والجهات الخاضعة لرقابته واشرافه وكذلك الزم السيد الوزير المعني بشؤون الاتصالات وتكنولوجيا المعلومات بإصداره لائحة للعمل بهذا القانون وقد حدد اختصاص المحاكم الاقتصادية وقد وكذلك أسند الاختصاص للمحاكم الاقتصادية بنظر الجرائم التي ترتكب مخالفه لهذا القانون وتناول في الفصل الاول المادة الأولى إلى جانب بعض التعريفات العامة مثل البيانات الشخصية والمعالجة والبيانات الشخصية الحسابية والحائز والمتحكم وغيرها من البيانات التي تخص وغيرها من البيانات الشخصية وفي الفصل الثاني تناول حقوق الشخص المعني بالبيانات وشروط معالجة هذه البيانات أنهم لا يجوز جمع هذه البيانات شخصية أو معالجتها أو الافصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة أو إذن قانوني في الأحوال المصرح بها قانوناً وكذلك في المادة الثالثة حدد شروط جمع البيانات الشخصية والاحتفاظ بها ومعالجتها ومنها أن يكون جمع هذه البيانات لأغراض مشروعة ومحددة

وتكون صحيحة وسليمة وغيرها وأيضاً في الفصل الثالث حدد الالتزامات الخاصة بالمتحكم والمعالج بإلزام المتحكم بالحصول على البيانات الشخصية من الجهات المختصة التي تزوده بها بعد موافقة الشخص المعني بالبيانات والتأكد من صحة هذه البيانات ووضع أسلوب ومعايير لمعالجة هذه البيانات واتخاذ الاجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها للحفاظ على سريتها وعدم اتلافها أو تدميرها أو تغييرها أو اختراقها لاي اجراء غير مشروع وكذلك تصحيح الأخطاء بالبيانات الشخصية والحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية وأيضاً حدد التزامات المعالج بان يلتزم معالج البيانات الشخصية بإجراء المعالجة والقيام بها وتنفيذها للقاعدة المنظمة في هذا القانون وأن يكون من أغراض المعالجة وممارستها ان تكون مشروعة ولا تخالف النظام والآداب العامة وعدم تجاوز الغرض المحدد والمعين لهذه المعالجة والمدة المسموح بها ومحو هذه البيانات خلال مدة الانقضاء وتضمن أيضاً شروط المعالجة الالكترونية بان تكون مشروعة وقانونية في حالة موافقة الشخص المعني بالمعالجة وان تكون لازمة وضرورية وان ينظم القانون من خلال جهات التحقيق هذه المعالجة وأيضاً الالتزام بالإخطار والابلاغ ان يلتزم المتحكم والمعالج بحسب الاحوال حالة علمه بوجود خرق أو اتلاف للبيانات الشخصية بأن يقوم بإبلاغ المركز خلال 72 ساعة وكذلك شروط تعيين مسؤول حماية البيانات الشخصية والتزاماته التي يلتزم بها طبقاً لنصوص القانون وأيضاً حدد اجراءات إتاحة البيانات الشخصية ومنها ~~ان يكونها~~ ان تكون بناء على طلب كتابي يقدم اليه من ذي صفة والتحقق من توفر المستندات اللازمة لتنفيذ الإتاحة وغيرها وأيضاً البيانات الشخصية الحساسة يحظر على المتحكم أو المعالج سواء كان شخصاً طبيعياً أو اعتبارياً جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز وأيضاً تناول في الفصل السابع البيانات الشخصية عبر الحدود وكذلك في إتاحة البيانات الشخصية المتحكم أو معالج اخر خارج جمهورية مصر العربية وذلك يكون طبقاً لاتفاق عمل بين كل من المتحكمين أو المعالجين وتوافر المصلحة المشروعة والتسويق الالكتروني المباشر الخاص بالبيانات وأيضاً تشكيل المركز الخاص بحماية البيانات الشخصية وتشكيل مجلس إدارة لإدارة المركز وتحديد مسؤولياته وواجباته واختصاصاته وحدد أيضاً أنواع التراخيص والتصاريح والاعتمادات الخاصة للمجلس أو المصرح بها واجراءاتها وشروط هذه التراخيص والتصاريح ومدى تعديلها وإلغائها وأيضاً حدد الجزيئات الادارية الخاصة بالمسؤولية المدنية ومنها الانذار وايقاف الترخيص وسحبه وحدد موازنة المركز وموارده المالية وأيضاً تضمن الطلبات والشكاوي والصيغة القانونية لها وتناول في الفصل الرابع عشر الجرائم والعقوبات ومنها عقوبة الغرامة التي لا تقل عن 100,000 جنيه ولا تتجاوز مليون جنيه لكل حائز أو متحكم أو معالج أو إتاحة البيانات الشخصية أو تداولها باي وسيلة من الوسائل وتكون العقوبة مدة لا تقل عن ستة اشهر وغرامة لا تقل عن 200,000 جنيه ولا تتجاوز هاتين العقوبتين إذا ارتكب هذا الفعل مقابل الحصول على منفعة أو تحقيق منفعة مادية أو معنوية أو أدبية وأيضاً عقوبة الغرامة التي لا تقل عن 100,000 جنيه ولا تتجاوز مليون جنيه لكل حائز أو متحكم امتنع عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المواد السالفة وتنوعت العقوبات ما بين الغرامة وما بين الحبس لكل من يخالف احكام هذا القانون وحدد صور هذه الجرائم في والافعال الإجرامية في عدة مواد من القانون وحدد أيضاً حالات الصلح والتصالح (المصري، قانون حماية البيانات الشخصية رقم 151 لسنة 2020 محدثاً حتى عام 2023، 2020).

وكذلك قد أورد المشرع المصري بعض الحماية من خلال نصوص قانون حق المؤلف ولو كان من خلال تقنية المعلومات فقط قرر في المادة الثانية من قانون حماية حقوق المؤلف أنه تشمل هذه الحماية مؤلفي مصنفات الحاسب الآلي من برامج وقواعد وبيانات وما يماثلها من مصنفات يتم تحديدها بقرار من وزير الثقافة وهي تعد من المصنفات الأدبية واجبة الحماية ثم تناولت المادة الرابعة من ذات القانون أنه مع عدم الإخلال بحكم المادة 19 لا تشمل تلك الحماية الآتي:

المجموعات التي تنظم كل مصنفات عدة مثل مختارات الشعر والنثر ولكن تتمتع تلك المجموعات بالحماية إذا كانت

مميزة لسبب يرجع إلى الابتكار أو الترتيب أو أي مجهود شخصي آخر يستحق الحماية، وقد ثار الخلاف في الفقه حول مدى كون الجرائم سالفة الذكر عمدية.

من منطلق أن المشرع المصري قد قرر عقوبات مناسبة على جرائم تقليد المصنفات الأدبية ومن بينها جرائم الحاسب وقواعد البيانات وفق المادة 47 من قانون حماية حق المؤلف فهل تلك الجرائم يلزم لتوافرها الركن المعنوي أي العمد والإرادة السليمة

الرأي الفقهي الأول ذهب أيضاً أنصار ذلك الرأي إلى وجود توفر القصد الجنائي وأنه يقع على الجاني إثبات حسن النية لأنها جريمة عمدية التي يقوم ركنها المعنوي على القصد الجنائي (لطفي، 2000).

الرأي الفقهي الثاني يرى أنصار ذلك الرأي أن تلك الجريمة يكفي فيها القصد الجنائي العام فقط لاستحقاق العقوبة (فايد، 1991).

الرأي الفقهي الثالث يرى ذلك الرأي أن القصد الجنائي مفترض فإنه يتعارض مع صراحة النص والمبادئ الدستورية الأساسية مثل قرينة البراءة وكذلك مبدأ شخصية المسؤولية الجنائية وعليه فإنه يعد مرتكباً للجريمة المنصوص عليها في المادة 47 من قانون حماية المؤلف من يقوم بتقليد موقع الإنترنت أو التعديل أو التحويل فيه دون علم صاحبه (رمضان، الحماية الجنائية لموقع التجارة الإلكترونية على الإنترنت ومحتوياته، 2001).

المطلب الثاني:

الجانب التطبيقي لجرائم الإرهاب السيبراني الدولي

وفي هذا المطلب سوف نتناول بعض النماذج التطبيقية للجرائم السيبرانية وخاصة جريمة الإرهاب السيبراني الدولي كالآتي:

في العام الحالي 2024، ما حدث في الأيام القليلة الماضية من تفجير ما سمي بأجهزة البيجر (أجهزة اتصال لاسلكية من طراز I C-V82 بديلة عن الهواتف المحمول) للوقاية من الاختراق التي استوردها حزب الله بلبنان من خمسة أشهر تقريباً لمن أبشع صور جرائم الإرهاب السيبراني الدولي التي ارتكبتها إسرائيل ضد أفراد جماعة حزب الله في الآونة الأخيرة حيث أعلنت السلطات اللبنانية أنه تم تفجير هذه الأجهزة عن طريق رسائل إلكترونية تم إرسالها لهذه الأجهزة بصورة جماعية في آن واحد، وتلقت الأجهزة هذه الرسائل وكأنها من عناصر حزب الله قبل تفجيرها مما نتج عنها مقتل ما لا يقل عن 37 شخصاً وإصابة الآلاف (التوقيع الإلكتروني بي بي سي، 2024).

وكذلك حدوث خلل تقني عالمي بسبب طرف ثالث خارج عن السيطرة في نقاط التسجيل وبيانات الركاب تسبب في توقف الطيران العالمي والهبوط الاضطراري لبعض الطائرات مما نتج عنه إثارة الرعب والفزع للمسافرين حول العالم وتكبيد خسائر مالية فادحة لمنظومة الملاحة الجوية على مستوى العالم ومنها أمريكا واسبانيا وفرنسا وايرلندا (الموقع الإلكتروني بي بي سي، 2024).

باشرت محكمة الجنايات في دبي يوم الأربعاء 4-3 عام 2020 محاكمة ثلاثة متهمين من جنسيات آسيوية وغربية شاركوا في تدمير نظام إلكتروني لإحدى الشركات في الدولة مسببين لها خسائر مالية بنحو مليون درهم ونفذ عملية القرصنة وتدمير النظام أحدهم وهو موظف سابق في الشركة المجني عليها بعد حصوله على الرقم السري واسم المستخدم من زميله المتهم الأول موظف بالشركة بتحريض من المتهم الثاني وهو موظف سابق كذلك وعرض عليهما رشوة لتنفيذ الجريمة بعد إغرائهما بتوظيفهما وبراتب أعلى في الشركة الجديدة التي يعمل فيها وذلك لأغراض إنتقامية.

وكذلك من أخطر الجرائم السيبرانية المتوقع زيادتها في السنوات القادمة، هجوم الفدية الذى وصفته وزارة العدل الأمريكية بأنه صورة من صور الجرائم السيبرانية، وقدر المبلغ الإجمالي من مدفوعات الفدية بما يقرب من مليار دولار سنوياً وفقاً لما جاء بتقرير مكتب التحقيقات الفيدرالي، وجاءت التوقعات بأن الشركات التجارية سوف تقع ضحية لهجوم الفدية كل 14 ثانية بحلول عام 2019 (الغامدي، 2018) وتشير التقارير الدولية إلى أن هجوم الفدية تسبب في خسائر مالية فادحة فاقت الخمسة مليارات دولار أثناء عام 2017 وهو معدل مرتفع جداً خلال عام واحد.

ومن أمثلة جريمة الإرهاب السيبراني الدولي ما حدث لشبكة الكهرباء الأوكرانية والذي تسبّب في انقطاع الكهرباء وبقاء

أوكرانيا لساعات في الظلام وبذلك تخطّت الجرائم والهجمات السيبرانية نطاق البيانات والمعلومات والمعلومات والمواقع الإلكترونية وصولاً للبنية التحتية والأنظمة الحيوية مثل المفاعلات وأنظمة الكهرباء والقطاعات الصحية والنقل وغيرها من المؤسسات التي تعد ركائز أساسية للدول، مما زاد مستوى الخطورة على الدول (العجمي، 2018).

وقد بين تقرير "Council Advisory Security Overscan" عام 2016، أن الهجوم السيبراني على شركة أرامكو السعودية تحملت تكلفة تغيير 50 ألف قرص صلب لأجهزة الكمبيوتر مما يمثل عبئاً مالياً ضخماً عليها، ولم تستطع استخدام الإنترنت لقرابة خمسة أشهر، وأيضاً في نفس العام أفاد تقرير شركة نورتون الأمريكية (سمنتك) إلى أن هناك عدد كبير من المواطنين في المملكة كانوا ضحايا هجمات سيبرانية أو تأثروا بالجرائم السيبرانية، وكذلك ذكر التقرير أن نسبة 85٪ من السكان تعرضوا لهجمات واختراقات سيبرانية وهذه النسبة تخطت النسبة العالمية بما يعادل 10% (العالم، 2018) ومن أشهر الهجمات والاختراقات السيبرانية ما حدث من سرقة حسابات شركة ياهو (Yahoo) حيث بلغ عدد الحسابات التي تم اختراقها وسرقتها ثلاثة مليارات حساب، وكذلك اختراق إكيفاكس (Equifax) حيث تأثّر أكثر من خمسة مليون عميل (فوزي، 2019).

وفي عام 2014م، تم رصد هجمات سيبرانية في العراق بواسطة شركات أمنية مختصة بالأمن السيبراني باستخدام وسائل التواصل الاجتماعي لحشد المؤيدين ونشر الدعاية ولجمع المعلومات الأمنية عن طريق مجموعة من قراصنة الإنترنت الذين يعملون على خداع الناس بإرسال رسائل تحوي شفرات وبرامج ضارة عبر وسائل التواصل الاجتماعي، وما أن يتم فتحها حتى يبدأ المهاجمون على الفور بالتحكم الكامل بالجهاز وسرقة الملفات أو استخدام كاميرا الكومبيوتر أو الميكرفون لمراقبة ما يجري للشخص المستهدف (صالح، 2023).

وما تم رصده في الانتخابات العراقية لعام 2018م، من انتشار الكثير من التسجيلات الصوتية لعمليات شراء مقاعد في مجلس النواب كذلك في عام 2019م تعرض نحو 30 موقع إلكتروني للحكومة العراقية لحالة من الاختراق منها جهاز الأمن الوطني العراقي ووزارة الداخلية والصحة والدفاع، مما نتج عنه عطل بالصفحات الرسمية الخاصة بالوزارات الأمنية مثل وزارة الداخلية ومستشارية الأمن الوطني وجهاز مكافحة الإرهاب، وتم اختراق قاعدة البيانات وتسريب معلومات وبيعها تتعلق بالأمن الوطني العراقي (هيثم كريم صيوان ومهنّد جبار عباس، 2022).

وكذلك أيضاً اختراق الموقع الرسمي لجهاز مكافحة الإرهاب والإعلان عن انقلاب ضد الحكومة تلبية لرغبة المتظاهرين، إلا أنه أعلن عبر موقعه الرسمي في وقت لاحق عن تعرض الموقع لاختراق وأن ما نشر فيه عارٍ تماماً من الصحة (صالح، 2023).

وذلك كما حدث أيضاً في حرب الخليج الثانية حيث تم ضرب مولدات الطاقة الكهربائية العراقية مما أدى إلى وفاة حوالي 8000 مواطن عراقي كنتيجة مباشرة لعدم توافر الطاقة الكهربائية.

وفي عام 2008 قامت روسيا بالاستيلاء على 54 موقعاً اخبارياً لجورجيا وموقعاً رسمياً لوزارة الدفاع وموقعاً مالياً لأحد البنوك وتم قطع خدمة الإنترنت عن جورجيا لبضع ساعات ونتج عن ذلك توقف نسبة 35% من مؤسسات جورجيا التي تعتمد على الإنترنت ومنها توقف جميع الخدمات الإلكترونية للبنك الوطني وقد كان ذلك معاصراً لشن عمليات عسكرية تقليدية.

وفي عام 2010 تم شن هجوم سيبراني على المرافق النووية الإيرانية حيث تم اختراق النظام السيبراني المختص بتشغيل أجهزة الطرد المركزي المختصة بتخصيب اليورانيوم عن طريق إدخال برامج إلكترونية ضارة مما نتج عنه تلف حوالي ألف جهاز طرد مركزي وحرمانها واستبعادها من الخدمة مع عدم وجود أي أثر للفيروس الذي تم استخدامه في الهجوم السيبراني عقب تحقق الضرر مباشرة.

وخلال الفترة من عام 2011 حتى عام 2013 كانت هناك سلسلة من الهجمات السيبرانية من قبل مجموعة من المبرمجين الإيرانيين استهدفت عدد 47 بنكاً ومؤسسة مالية أمريكية مثل البنوك وغيرها من هذه المؤسسات المالية والمصرفية وتسببت هذه الهجمات السيبرانية في إعاقة الآلاف من عملاء البنوك من الدخول والولوج الى حساباتهم البنكية ومعاملتهم المصرفية

وتحملت هذه المؤسسات الخسائر المالية الفادحة نظير إصلاح هذه الأضرار التي لحقت بالأنظمة الإلكترونية الخاصة بالبنوك.

وفي الفترة من عام 2013 حتى عام 2017 نشطت مجموعة من مجموعات إيرانية في القيام بالعديد من الهجمات السيبرانية المكثفة على الجامعات والمؤسسات الأمريكية واستهدفت عدداً كبيراً ما يقرب من 144 من الجامعات والمؤسسات العلمية الأمريكية وقاموا بالاستيلاء على ما يقدر به 31 تيرا من الوثائق والبيانات والمعلومات الهامة وهاجمت هذه المجموعة خلال هذه الفترة 176 جامعة في 21 دولة ومهاجمة 47 نظام خاص بشركات داخل وخارج الولايات المتحدة الأمريكية والمؤسسات الرسمية الأمريكية ومنظمة الأمم المتحدة وغيرها (الميموني، 2020).

وأيضا الهجوم الأمريكي على أجهزة إطلاق الصواريخ الإيرانية في عام 2019 حيث كان هناك هجوماً سيبرانياً على الحواسيب والأجهزة التي تتحكم في إطلاق الصواريخ الإيرانية باستغلال العديد من الثغرات في الشبكة الإيرانية التي وصفت بأنها تخضع لحراسة مشددة ~~والخراء~~ وأكد الخبراء والسياسيون على أن هذا الهجوم جاء بموافقة الرئيس الأمريكي دونالد ترامب رداً على عمليات سابقة من إيران ضد أمريكا منها اسقاط الطائرة الأمريكية المسيرة جلوبال التي قامت بها إيران بدعوة أنها اخترقت المجال الجوي الإيراني ورداً على استهداف إيران لنقلات النفط في الخليج في عمان.

وأيضاً استهداف وهجوم سيبراني إسرائيلي استهدف ميناء الشهيد رجاء الإيراني الذي يطل على مضيق هرمز وتسبب هذا الهجوم في تعطيل الحركة الملاحية عبر الممرات المؤدية للميناء وأن الهجوم تم تنفيذه بدقة عالية وتسبب في حدوث أضرار وخسائر فادحة لحقت بالميناء الإيراني إلا أن نظام الحماية السيبراني الإيراني (الحصن الرقمي) لم يكن فعالاً وتم اختراقه أكثر من مرة وفقاً لما جاء بالتقارير الإسرائيلية (إسرائيل وراء الهجوم السيبراني عالي الدّقة على ميناء إيراني، 2020).

وفي نهاية عام 2009 تعرضت شركة جوجل لهجوم سيبراني والتي انتهت التحقيقات فيه إلى أنه كان الغرض الرئيسي من الهجوم سرقة معلومات من البريد الإلكتروني تخص مواطنين صينيين من العاملين في مجال حقوق الإنسان ووصف المجتمع الدولي هذا الهجوم السيبراني آنذاك بأنه جريمة دولية ومنهم وزيرة الخارجية الأمريكية كلينتون التي أدانت هذا الاعتداء واستنكرته.

ولقد عرف عام 2016 في الإعلام الدولي بأنه عام الهجمات السيبرانية وكان الحدث الأبرز هو إتهام روسيا بالتدخل السيبراني وبالتلاعب في نتائج الانتخابات الأمريكية حيث أعلن مدير الاستخبارات الأمريكية أن المخابرات واثقة تماماً بأن الحكومة الروسية متورطة في هذا الاختراق لتؤثر على نتائج الانتخابات لصالح المرشح دونالد ترامب وأن عملاء روس اخترقوا أنظمة المعلومات وقواعد البيانات الخاصة باللجنة الوطنية الديمقراطية وحصلوا على كل تقاريرها ورسائل البريد الإلكتروني المتبادلة بين أعضائها وتم التلاعب في البيانات والمعلومات الخاصة باللجنة لصالحه (الرشيدي، 2021).

وفي عام 2017 أشارت تقارير المختصين بالتسليح إلى أن نسبة فشل اختبارات الصواريخ الباليستية لكوريا الشمالية بلغت 88% وذلك لأن الولايات المتحدة الأمريكية كانت تقوم بهجمات وعمليات سيبرانية ضد برامج تطوير هذه الصواريخ تنفيذاً لإستراتيجية الأمن القومي الأمريكي التي تقضي إلى فرض عقوبات عاجلة على الدول والجهات الأخرى التي تمارس عمليات سيبرانية عدائية مع تكبيدها خسائر فادحة (عسكر، وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسات التجسّس وقت السلم، 2021).

وفي عام 2023 تعرضت مصر للعديد من الهجمات والتهديدات السيبرانية بكافة أشكالها وأنواعها وذلك في كل ما ورد بتقرير فريق البحث والتحليل العالمي في الشرق الأوسط وإفريقيا وتركيا في شركة (كاسبر سكاي) وهذه الشركة متخصصة في خدمات الأمن السيبراني وقد واجهت وتصدت هذه الشركة وكشفت عن حوالي 13 مليون هجمة سيبرانية على مصر في مطلع عام 2023 ونجد ان هذه الهجمات قد تركزت على الحسابات المصرفية في البنوك الخاصة ببيانات العملاء في القطاع المصرفي بنسبة 186% خلال الربع الاول من عام 2023 مقارنة بالربع الاول من عام 2022 ووفقا لذلك فان الهجمات السيبرانية المتمثلة في هجمات

القرصنة تتزايد بشكل مطرد مستهدفة نظام المعلومات في القطاعات المصرفية في مصر وكذلك زيادة هجمات التصيد الاحتيالي عن طريق البريد الالكتروني والرسائل النصية ووفقا لهذا التقرير أيضاً فقد تعرض حوالي 75,000 مستخدم في مصر خلال بداية عام 2023 لهجمات التصيد الاحتيالي وكذلك بعض المؤسسات الحكومية المصرفية تعرضت لهجمات تم شنها من عصابات دولية في القرصنة في عام 2022 وذلك بهدف سرقة بيانات ومعلومات العملاء والتجسس عليهم (البهي، 2023).

وبالإضافة الى ذلك واجهت مصر الخطر العظيم المتمثل في الإرهاب السيبراني في ظل توظيف وتفعيل التنظيمات الإرهابية للجان الإلكترونية التي تنشر الفوضى في المجتمع وتقوض الاستقرار وتنشر الشائعات والتأثير على وعي المواطنين في المجتمع والنيل من النظام السياسي والتشكيك في إمكانيات ومسارات الدولة ومشروعاتها وذلك من خلال نشر معلومات مزيفة وغير مطابقة للواقع وهذه اللجان تتبع أقسام الرصد والمتابعة الخاصة باللجان الإعلامية في التنظيمات الإرهابية وتتولى مهمة رصد وتتبع كل الأخبار والشائعات التي تعرض على الشاشات في مختلف منصات التواصل الاجتماعي ومتابعة الباحثين المتخصصين في جرائم الارهاب وذلك أيضاً متابعة الإعلاميين والوسائل الإعلامية التي تؤيد الدولة وسياستها وتتخذ القرارات بملاحقة الخصوم وتشويه سمعتهم وأفكارهم واغتيالهم معنوياً (فتحي، 2023).

الخاتمة:

بعد العرض آنف البيان انتهينا بما لا يدع مجالاً للشك إلى أهمية وضع تعريف محدد ودقيق لجريمة الإرهاب السيبراني وتحديد صوره وأركانه ومسؤولية مرتكبي هذه الجرائم وتعزيز ومضاعفة الجهود الدولية في مكافحة الجرائم السيبرانية التي تتم عبر الفضاء السيبراني والإنترنت لأنها بطبيعتها جريمة عابرة للحدود والقيود، والتي أفرزت جملة من التحديات على المجتمع الدولي ليست خياراً إنما هي ضرورة لا مناصة منها في الوقوف صفا كالبنيان المرصوص من جانب كافة الدول في سبيل المكافحة والمواجهة القائمة على أسس علمية سليمة ومدروسة لا سيما أن عمليات الإثبات في الجرائم السيبرانية تحيطها الصعوبة الشديدة بل والاستحالة في بعض الجرائم والحالات وبالرغم من كل الجهود التي بذلها العالم في هذا الشأن وفي سبيل تلك التحديات تبقى القضية صعبة وشبه مستحيلة لإيجاد الحلول الكاملة في غالب الحالات خاصة في تلك الدول التي لم تبادر بعد إلى تعديل تشريعاتها الداخلية بما يضمن تجاوز القوالب القانونية التقليدية العتيقة بما يتواكب مع مناهضة هذا النوع من الجرائم السيبرانية ولذلك فإن العمل على إرساء قواعد التعاون الإقليمي الدولي في مجال التكنولوجيا ومكافحة الجرائم السيبرانية التي تتم عبر الفضاء السيبراني وكذلك السعي نحو إيجاد إطار قانوني للتعاون الدولي الجنائي قضائيا وأمنياً بات أمراً ضرورياً ولزاماً للغاية وندعو الله أن نكون قد تناولنا الموضوع من كافة جوانبه مما يسهم ولو بقليل في تعزيز الثقافة القانونية خاصة في مجال القانون الدولي الجنائي بهذا النمط الجديد من الجرائم السيبرانية التي بات الاعتراف بوجودها أمراً حتمياً كما نعترف بمخاطرها أمراً لا فكاك منه في ظل التطور التكنولوجي المتلاحق في أساليب تلك الجرائم بما يجعل من صعوبة مكافحتها دون تكاتف وتلاحم الجهود الدولية أمراً يجب الوقوف عليه كما أنه لا يمكن توقع تبعات تغير أنماط وأشكال الجرائم السيبرانية وخاصة الإرهاب السيبراني الدولي في المستقبل بما يضع المجتمع الدولي في مأزق شديد من حصار ويلاتها ويجب أن يعمل المجتمع الدولي من الآن على قدم وساق من أجل وضع تشريعات جنائية وطنية ودولية لمواجهة هذا النوع من الجرائم وعليه يمكن إجمال أبرز نتائج بحثنا في الآتي:

النتائج:

- اعتماد الدول على وسائل الاتصال الحديثة بات أمراً لا غنى عنه ولا بديل له وهو ما يمثل أرضاً خصبة للإرهابيين في مزاولة نشاطهم وتدمير مخرجات التقنية الحديثة والتي هي في حقيقتها شرعت لخدمة الإنسانية وتيسير سبل الحياة ومن ثم باتت المعلومات المخزنة عرضة للاختراق والتدمير والتغيير بل والحذف أيضاً.
- يمكن القول إن الإرهاب السيبراني الدولي والتخويف أو العدوان أو التهديد باستخدام وسائل التقنية الحديثة من أصحاب المآرب قد يكون مجرماً في كل المبادئ والقيم الإنسانية فهو موضع للمساس سواء الدين أو

النفس أو العرض أو العقل أو المال أو ممتلكات ومرافق الدولة الأساسية وبنيتها التحتية.

- أهم وأخطر مظاهر الإرهاب السيبراني الدولي على الإطلاق وأكثرها شيوعاً هي تبادل المعلومات الإرهابية ونشرها على الشبكة العنكبوتية وكذلك إنشاء مواقع إلكترونية لهم أو تدمير مواقع قائمة وتدمير البنية التحتية لمؤسسات الدولة الخاص.
- عمليات التطور السريع والمتلاحق في تكنولوجيا الاتصالات الحديثة تحتاج لبذل جهد مضاعف لمكافحة أحدث أشكال السلوك غير المشروع للجماعات الإرهابية عبر الفضاء السيبراني في سعيها الدائم نحو تطوير وتغيير وإخفاء نمط عملها للهروب من الملاحقة أو الرصد.
- تعتبر سبل الاتصال الحديثة خاصة الشبكة العنكبوتية هي سلاح ذو حدين فهي نافعة للإنسانية بمجملها وسهلت وصول المعلومات ونقل البيانات إلا أن الوجه الآخر هو استخدامها في أغراض وأهداف مدمرة للإنسانية وتجعل من الأمن الكامل للأفراد أو المؤسسات أو الدول هو درب من دروب الخيال التي بات السيطرة عليها مهمة شبه مستحيلة.
- 6-عدم النص صراحة في كل مادة على مطالبة الدول الأعضاء الموقعين على إيراد أو النص على أعمال الاشتراك أو الشروع الجنائي ضمن العقاب المطالب به في القوانين الوطنية المحلية للدول الأعضاء وعدم افراد مادة منفردة للنص على الشروع والمساهمة الجنائية حتى يضحي الأمر واضحاً لكل الدول الموقعة وينتهي أي خلاف أو جدل أو اختلاف في تفسير بين دولة وأخرى مما قد يجعل من بعض الأفعال أو السلوكيات بمنأى عن التجريم خصوصاً وأن مجال تقنية الاتصالات والمعلومات والشبكة العنكبوتية كل يوم في تطور جديد وحديث ومستمر.

التوصيات:

- يوصى الباحث المجتمع الدولي على النص صراحة على تعريف موحد ودقيق وواضح لجريمة الإرهاب السيبراني في المعاهدات والاتفاقيات الدولية وكذلك في التشريعات الداخلية وتحديد صورها وأركانها والمسؤولية الناشئة عن ارتكاب هذه الجريمة.
- النص صراحة على الاشتراك والشروع والمساهمة في الجرائم السيبرانية وخاصة جريمة الإرهاب السيبراني الدولي من أعمال التحريض والاتفاق والمساعدة في الاتفاقيات والمعاهدات الدولية ضمن العقاب المطالب به في القوانين الوطنية المحلية للدول الأعضاء لكل جريمة على حدها وعدم إفراد مادة منفردة للنص على الشروع والمساهمة الجنائية حتى يضحي يصبح الأمر واضحاً لكل الدول الموقعة وينتهي أي خلاف أو جدل أو اختلاف في تفسير بين دولة وأخرى مما قد يجعل من بعض الأفعال أو السلوكيات بمنأى عن التجريم خصوصاً وأن مجال تقنية الاتصالات والمعلومات والشبكة العنكبوتية كل يوم في تطور جديد وحديث ومستمر.
- مواصلة الدول في سن تشريعات داخلية حديثة تواكب التطورات التكنولوجية المستمرة لمكافحة جريمة الإرهاب السيبراني الدولي بكافة صورها تتضمن المفاهيم التقنية والجوانب الاجرائية من ضبط وتفتيش الأنظمة السيبرانية الواقع عبر الحدود وتحقيق وإحالة ومحاكمة بما لا يخل بضمانات حقوق الإنسان وحرياته.
- إدراج جريمة الإرهاب السيبراني الدولي في النظام الأساسي للمحكمة الجنائية الدولية ضمن الجرائم التي تخضع للاختصاص الموضوعي لها وبيان اركانها وصورها والمسؤولية الناشئة عنها والعقوبات التي تقع على مرتكبيها.
- إنشاء هيئات وأجهزة دولية وإقليمية متخصصة في التحقيق في الجرائم السيبرانية على قدر كافٍ من الخبرة والكفاءة الفنية والقانونية في مجال الأمن السيبراني بما يتيح لها جمع الأدلة والحفاظ عليها وتقديمها للقضاء.
- النص صراحة على تطبيق مبادئ القانون الدولي الإنساني على جريمة الإرهاب السيبراني الدولي التي تستهدف البنية التحتية للمؤسسات الحكومية وذلك

لعدم ملائمة ملاءمة القواعد المطبقة للتطور الهائل والمستمر في تقنية المعلومات.

- التعاون الدولي لسن تشريعات ذات معايير صارمة موحدة في التعاون القضائي وتسليم المجرمين وضبط الأدلة بين الدول وتشديد العقوبات على مرتكبي جريمة الإرهاب السيبراني الدولي بكافة صورها لا تختلف من دولة لأخرى لمنع هروبهم للدول الأقل صرامة في تطبيق العقوبات في قوانينها الداخلية.
- إنشاء مراكز وطنية إرشادية بالشراكة مع مؤسسات الدولة والقطاع الخاص والشركاء العالميين للتوعية لنشر الثقافة الرقمية وتبني إستراتيجيات للتوعية بمخاطر جرائم الإرهاب السيبراني الدولي وكيفية مواجهتها من خلال البرامج التدريبية والمنح الاحترافية المتخصصة في مجال الأمن السيبراني.
- استخدام تقنيات الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية (الإرهاب السيبراني الدولي) وتطوير البنية الرقمية وإجراء برامج قياس الجاهزية ومنع الاختراقات وأجهزة ووكالات للرصد والإنذار المبكر بحدوثها لتحقيق الأمن السيبراني.
- إلزام الدول بالتعاون الدولي والإقليمي بتكثيف الجهود لتوفير التدريب والتأهيل المناسب والكافي للتحقيق في مجال العدالة الجنائية في كافة مراحله لتطوير التحقيقات والإثبات الجنائي والأدلة الرقمية في الجرائم السيبرانية.
- تكثيف الجهود للتوعية الأمنية بالإرهاب السيبراني الدولي عن طريق إضافة برامج تعليمية وتدريبية متخصصة وتشجيع البحث العلمي في مراحل التعليم المختلفة وخاصة المؤسسات الشرطية.
- إنشاء نظام أمني دولي به قواعد بيانات خاصة بجريمة الإرهاب السيبراني الدولي من حيث صورها وأساليب ارتكابها ومرتكبي هذه الجرائم لسهولة الإثبات في هذه الجرائم وسرعة التوصل لمرتكبيها.

قائمة المصادر والمراجع:

- فاقية (2000). مكافحة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم 63/55. منظمة الأمم المتحدة.
- أحمد بن عل علي الميموني. (2020). تداعيات المواجهة السيبرانية بين إيران وإسرائيل. مجلة الدراسات الإيرانية، السنة الرابعة، العدد الثاني عشر، ص67- 85.
- أحمد جلال محمود. (2020). أثر التهديدات الغير غير التقليدية للأمن على العلاقات الدولية المعاصرة. مركز بحوث الشرق الأوسط والدراسات المستقبلية، جامعة عين شمس، ص 70، 71.
- أحمد فتحي. (2023). خطة مسمومة.. كيف ينشر الإخوان الارهاب الالكتروني بمصر. العين الإخبارية.
- سامه عبد الله فايد. (1991). الحماية الجنائية لحق المؤلف دراسة مقارنة. القاهرة: دار النهضة العربية، ص73.
- إسلام فوزي. (2019). الأمن السيبراني الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي. المجلة الاجتماعية القومية، ص 99-139.
- الجمعية الدولية للقانون العقوبات جهة استشارية للأمم المتحدة. (1989).
- المادة 5. (2001). اتفاقية بودابست لمكافحة الجرائم المعلوماتية.
- المادة الرابعة. (2001). اتفاقية بودابست لمكافحة الجرائم المعلوماتية.
- المشرع المصري. (2020). قانون حماية البيانات الشخصية رقم 151 لسنة 2020 محدثاً حتى عام 2023. الجريدة الرسمية المصرية.
- أيسر محمد عطية. (2014). دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهتها.
- إيهاب السنباطي. (2009). الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة السيبرانية بودابست 2001 والبروتوكول الملحق بها. القاهرة: دار النهضة العربية، ص 80.

- إيهاب خليفة. (ديسمبر, 2021). الحالة السيبرانية في نظريات العلاقات الدولية، بقلم خبير. مركز المعلومات ودعم اتخاذ القرار، الصفحات العدد 23، ص 8-11.
- بندر عقاب الدرويش. (2017). الإثبات في جرائم الإرهاب السيبراني دراسة مقارنة (الإصدار رسالة ماجستير). عمان: جامعة العلوم الإسلامية العالمية.
- تقرير اجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية. (2017). فيينا: مكتب الأمم المتحدة المعني بالمخدرات والجريمة.
- حسن بن علي العجمي. (2018). الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، الأمن السيبراني حروب الأرقام الصماء. المجلة العربية، 16.
- حسن حسنين بوادي. (2006). الإرهاب. الرياض: مكتبة العبيكان.
- حسنين بوادي. (2006). الارهاب. الرياض: مكتبة العبيكان.
- خالد ممدوح إبراهيم. (2009). الجرائم المعلوماتية. مصر: دار الفكر الجامعي ص 277ن.
- خالد ممدوح إبراهيم. (2009). الجرائم المعلوماتية. مصر: دار الفكر الجامعي ص278،277.
- ربيع حسن وسيد رفاعي. (2001). مبادئ علم الإجرام والعقاب. القاهرة: المؤسسة الفنية للنشر والطباعة.
- رغدة البهي. (2023). التجربة المصرية في مكافحة الإرهاب السيبراني: رؤية تحليلية. مركز الدراسات السياسية والإستراتيجية الأهرام، ص1 – ص22.
- سامر محي عبد الحمزة. (2022). مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، كلية القانون جامعة واسط، عدد 67، ج1، ص331.
- سامر مؤيد عبد اللطيف ونوري رشيد الشافعي. (2016). دور المنظمات الدولية في مكافحة الإرهاب الرقمي. العراق: جامعة كربلاء، ص65.
- سمية مزغيش. (2014). جرائم المساس بالأنظمة المعلوماتية. الجزائر: رسالة ماجستير كلية الحقوق والعلوم السياسية جامعة بسكرة.
- شيماء تركان صالح. (2023). الأمن الوطني العراقي والتهديدات السيبرانية الإرهاب السيبراني نموذجاً. مجلة تكريت للعلوم السياسية، ص 230.
- لاح الفتلاوي. (2004). الخطورة الإجرامية وأثرها في تحديد الجزاء الجنائي. العراق بغداد: كلية الحقوق رسالة دكتوراه.
- عامر محمود ناجي. (2008). الحماية الجنائية لوسائل الاتصال دراسة مقارنة. العراق: رسالة دكتوراه كلية القانون جامعة بابل ص41.
- عامر محمود ناجي. (2008). الحماية الجنائية لوسائل الاتصال دراسة مقارنة. العراق: رسالة دكتوراه، كلية القانون، جامعة بابل.
- عبد الله شرف الغامدي. (2018). الجرائم السيبرانية والتحديات المستقبلية، الأمن السيبراني حروب الأرقام الصماء. المجلة العربية، ص7.
- عبد الله علي عبد الله القحطاني. (2017). إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني. جامعة الملك عبد العزيز جده: جامعة الملك نايف للعلوم الأمنية.
- علي يوسف الشكري. (2012). المنظمات الدولية. عمان: دار صفاء للطباعة والنشر والتوزيع، ط1، ص 97 و98.
- عمر محمد أبو بكرين يونس. (2014). الجرائم الناشئة عن استخدام الإنترنت. مصر: دار النهضة العربية الطبعة الأولى.
- عميد شرطة عبد المجيد الحلاوي. (2006). أهمية التعاون العربي والدولي في مكافحة جرائم الإرهاب المعلوماتي. القنيطرة المغرب.
- كريمة غلاف وزهوره جلال. (2020). جريمة الإرهاب السيبراني. الجزائر: كلية الحقوق جامعة عبد الرحمن ميرة.

- ليلى الجنابي. (2017). فاعلية القوانين الوطنية والدولية لمكافحة الجرائم السيبرانية. بغداد: قناة الحوار المتمدن.
- لينا محمد متعب الأسدي. (2012). مدى فاعلية أحكام القانون الجنائي في مكافحة الجرائم المعلوماتية. العراق: رسالة ماجستير ن.
- لينا محمد متعب الأسدي. (2012). مدى فاعلية أحكام القانون الجنائي في مكافحة الجرائم المعلوماتية. العراق: رسالة ماجستير، كلية الحقوق، جامعة النهرين.
- مجلس الوزراء، وزارة الاتصالات وتكنولوجيا المعلومات المجلس الأعلى للأمن السيبراني. (يناير, 2023). وزارة الاتصالات وتكنولوجيا المعلومات. تم الاسترداد من الموقع الرسمي لوزارة الاتصالات وتكنولوجيا المعلومات: http://andp.unescwa.org.
- محمد أسعد العالم. (2018). الهدم والتخريب تقنياً، الأمن السيبراني وحروب الأرقام الصماء. المجلة العربية الرياض السعودية، ع 498، ص13.
- محمد حسام محمود لطفي. (2000). حقوق المؤلف في ضوء آراء الفقه وأحكام القضاء دراسة تحليلية للقانون المصري. القاهرة: بدون ناشر.
- محمد طارق عبد الرؤوف الخن. (2011). جريمة الاحتيال عبر الإنترنت والأحكام الموضوعية والأحكام الإجرائية. بيروت: منشورات الحلبي الحقوقية ط1.
- محمد عادل عسكر. (2021). وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسات التجسس وقت السلم. مجلة البحوث القانونية والفقهية، كلية الحقوق جامعة بني سويف، ص 303.
- محمد عادل عسكر. (2021). وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسات التجسس وقت السلم. مجلة البحوث القانونية والفقهية، كلية الحقوق جامعة بني سويف، مج33، ع1، ص263.
- محمد عادل عسكر. (2021). وضع العمليات السيبرانية في القانون الدولي العام مع التطبيق على ممارسة التجسس وقت السلم. مجلة البحوث الفقهية والقانونية، كلية الحقوق جامعة بني سويف ص314 مرجع سابق.
- محمد علي العريان. (2011). الجرائم المعلوماتية. دار الجامعة الجديدة، ص 32ن 33.
- محمد كمال محمود الدسوقي. (2017). الحماية الجنائية لسرية المعلومات السيبرانية. مصر: دار الفكر والقانون، ص 55.
- مود حجازي محمود. (2001). النظام القانوني الدولي للاتصالات بالأقمار الصناعية. القاهرة: دار النهضة العربية، ص131.
- مداوي سعيد مداوي القحطاني. (2016). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها. الأمانة العامة لمجلس التعاون لدول الخليج العربية، ص77.
- مدحت رمضان. (2001). الحماية الجنائية لموقع التجارة الإلكترونية على الإنترنت ومحتوياته. القاهرة: دار النهضة العربية، ص19.
- مدحت رمضان. (بلا تاريخ). الحماية الجنائية لموقع التجارة السيبرانية على الإنترنت.
- معنوي مختار المشرف. (2004). علاقة جريمة الإرهاب السيبراني بغيرها من الجرائم. الرياض: جامعة نايف العربية للعلوم الأمنية.
- مكافحة جرائم الانترنت. (2015). مؤتمر الرياض الإقليمي. الرياض.
- ملياني عبد الوهاب. (2017). أمن المعلومات في بيئة الأعمال السيبرانية. الجزائر: كلية الحقوق والعلوم السياسية جامعة تلمسان.
- مؤتمر الرياض. (2017). تجريم الارهاب السيبراني. وكالة أنباء الإمارات.
- مؤتمر مسقط الإقليمي الثالث للأمن السيبراني. (2014).

http://www.regionalcybersecuritysumm it.com. شبكة الانترنت.

- مؤتمر منظمة الامم المتحدة الثامن. (1990). منع الجريمة ومعاملة المجرمين. تقرير أعدته الأمانة العامة. مشورات منظمة الأمم المتحدة رقم (A-91-IV-2).
- هالة أحمد الرشيدي. (2021). هل من حرب سيبرانية بين الولايات المتحدة وروسيا. جريدة الأهرام.
- هبة جمال الدين. (2023). الأمن السيبراني والتحول الرقمي في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية كلية الاقتصاد والعلوم السياسية جامعة القاهرة، مجلد 24، ص94.
- هلالي عبد الله أحمد. (2011). اتفاقية بودابست لمكافحة الجرائم المعلوماتية معلقاً عليها. القاهرة: ط8، دار النهضة العربية.
- هيثم كريم صيوان ومهند جبار عباس. (2022). الحرب السيبرانية بين التحديات واستراتيجيات المواجهة العراق نموذجاً. مجلة قضايا سياسية، كلية العلوم السياسية، ص 159، 160.
- وفاء لطفي. (يناير, 2022). الجهود الدولية في مجال مكافحة الإرهاب السيبراني، التجربة الماليزية نموذجاً. مجلة كلية الاقتصاد والعلوم السياسية جامعة القاهرة، الصفحات مج13، ع 1، ص159-178.
- وفاء لطفي. (يناير, 2022). الجهود الدولية في مجال مكافحة الإرهاب السيبراني التجربة الماليزية نموذجاً. مجلة كلية الاقتصاد والعلوم السياسية جامعة القاهرة، الصفحات مج13، ع1، ص159-178.

References:

- ttp://www.sharjah.ac.ae.com. (n.d.).
- SCHJIBERG., S. (2008). The HISTORY of global Harmonication on cyber crime legislation. :http://www.cybercrimelaw.net.
- إسرائيل وراء الهجوم السيبراني عالي الدقة على ميناء إيراني (19-5-2020) Retrieved from https://www.defense-arabic.com
- صادق، ع. ع .(2009) .الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة. مركز الدراسات السياسية والإستراتيجية، ص109.
- القرار رقم 12 لعام 2024 على الموقع الإلكتروني للموقع الرسمي لوزارة الاتصالات (7-4-2024)، Retrieved from http://www.moct.gov.sy .
- المصري، ا .(2018) .قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 .الجريدة الرسمية المصرية- المطابع الأميرية.
- الموقع الإلكتروني بي بي سي (21 – 9 – 2024) Retrieved from .http://www.bbc.com/Arabic/articles
- الموقع الإلكتروني بي بي سي (20 9 2024) .Retrieved from http://.skynewsarabia
- الموقع الرسمي للاتحاد الدولي للاتصالات (www.it.int/or/action/pages).
- الموقع الرسمي لوزارة الاتصالات المصرية (27 9 2024)، Retrieved from mcit.gov.eg/ar/telecommunications/ind .ustry/Cyber-ecurity
- ملتقى تقنية المعلومات كلية تقنية المعلومات جامعة البحرين (14 9 2024)، Retrieved from: الموقع السيبراني: http://www.oub-.bh.com/forum/threads/2777